

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.



Yasinthorn (Not) Khemprakhon

Penetration Tester
Siam Thanat Hack Co., Ltd.



Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างโค้ด และรูปในการบรรยาย 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	ส่วนน่าสนใจในเส้นทางอาชีพ

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)

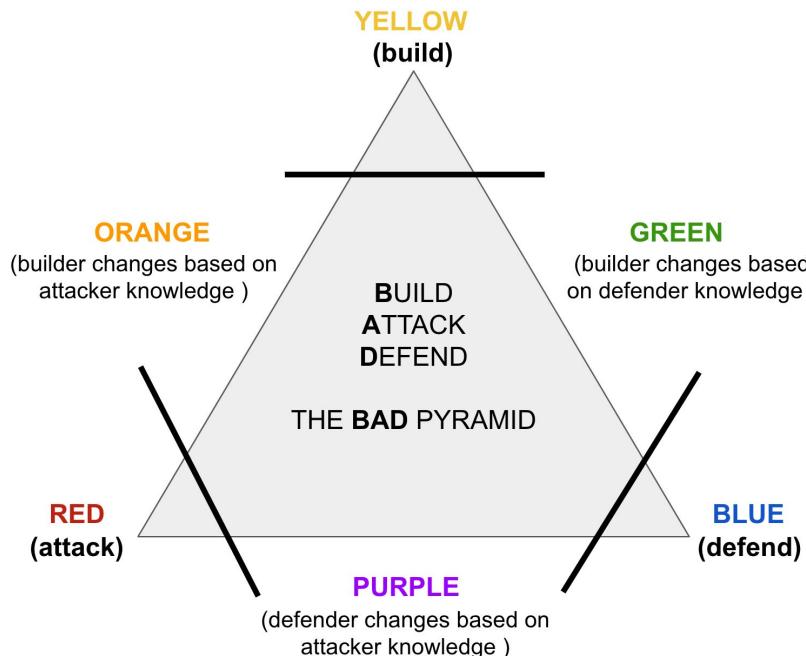
3. TryHackMe Platform

- Room
- Learning Path
- AttackBox & VPN
- Blue Team Rooms

4. Capture The Flag (CTF)



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

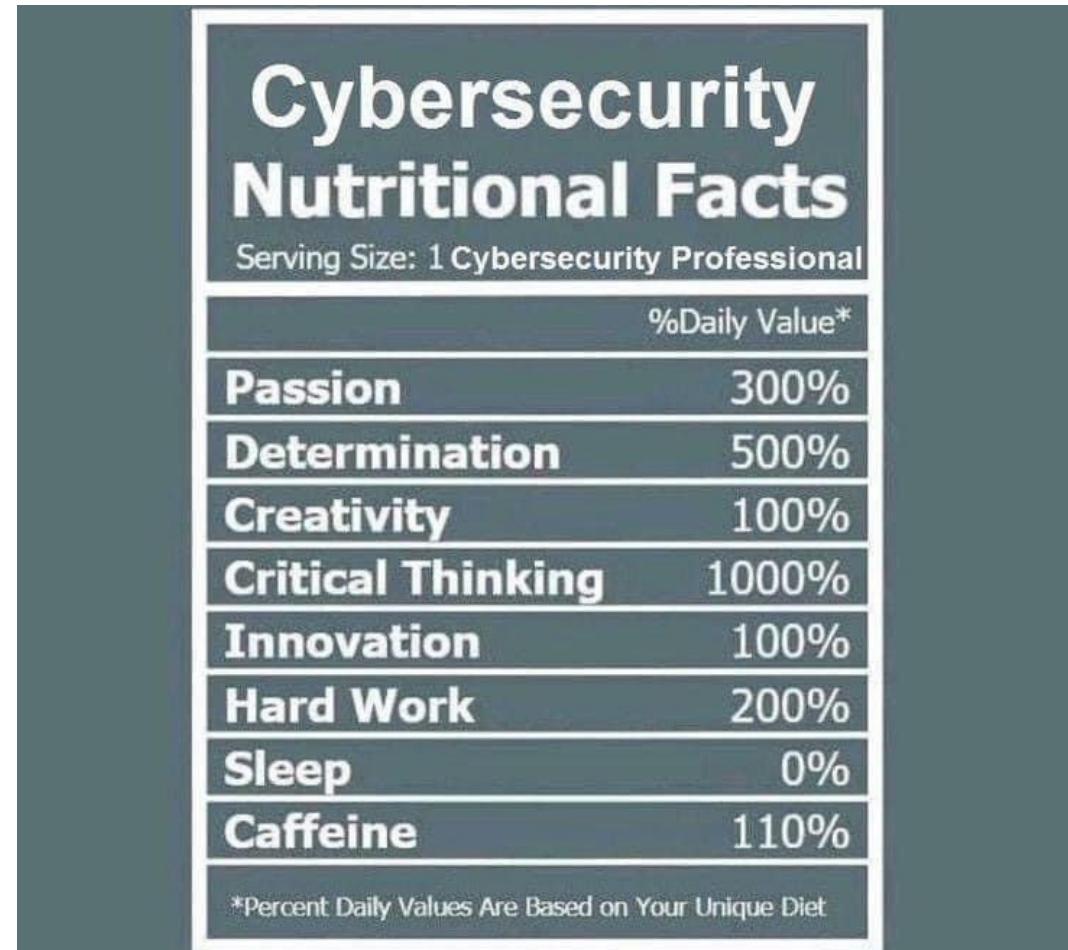
Purple Teams

- 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



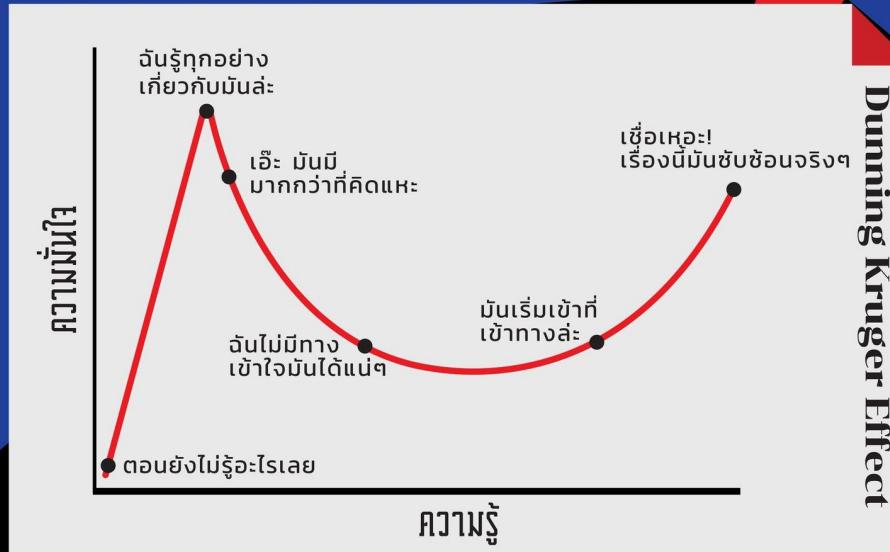
Dunning Kruger Effect

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

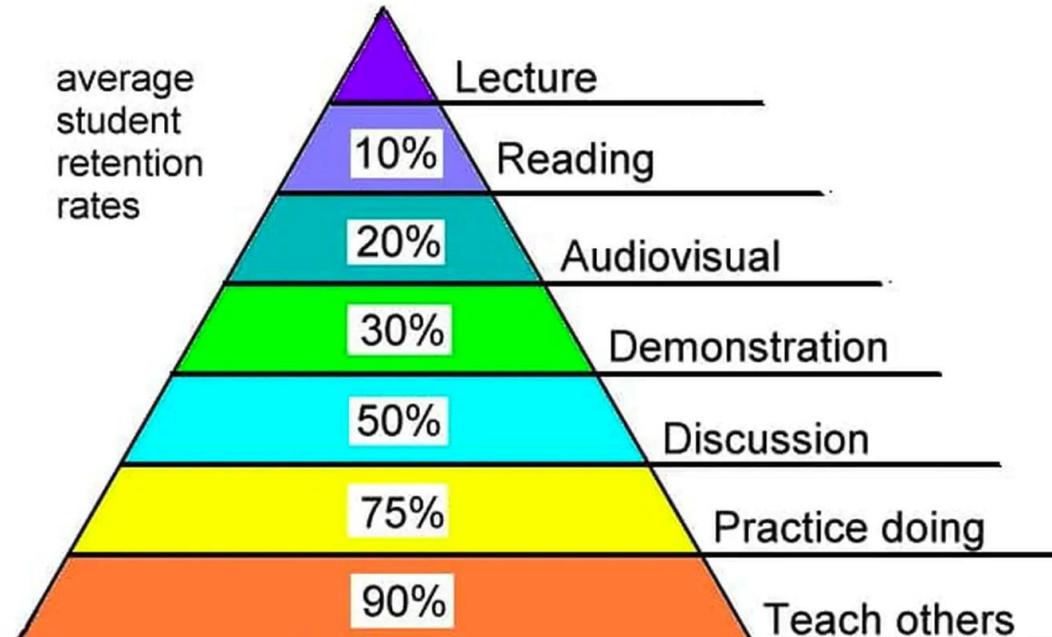
Source: BrandThink

<https://www.facebook.com/brandthink.me/posts/2471666556492215/>

ทำไมบางครั้งคนที่รู้น้อย
ถึงคิดว่าตัวเองฉลาดนักหนา



Learning Pyramid



Source: National Training Laboratories, Bethel, Maine

ความรู้พื้นฐาน IT Security สำคัญกว่า “เครื่องมือ”



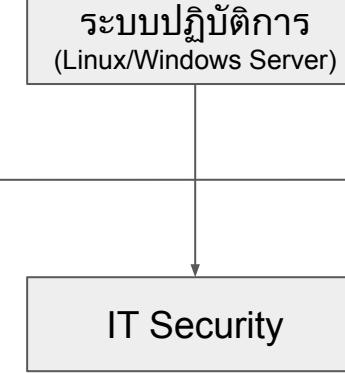
เขียนโปรแกรม



ระบบปฏิบัติการ
(Linux/Windows Server)



ระบบเครือข่าย
คอมพิวเตอร์



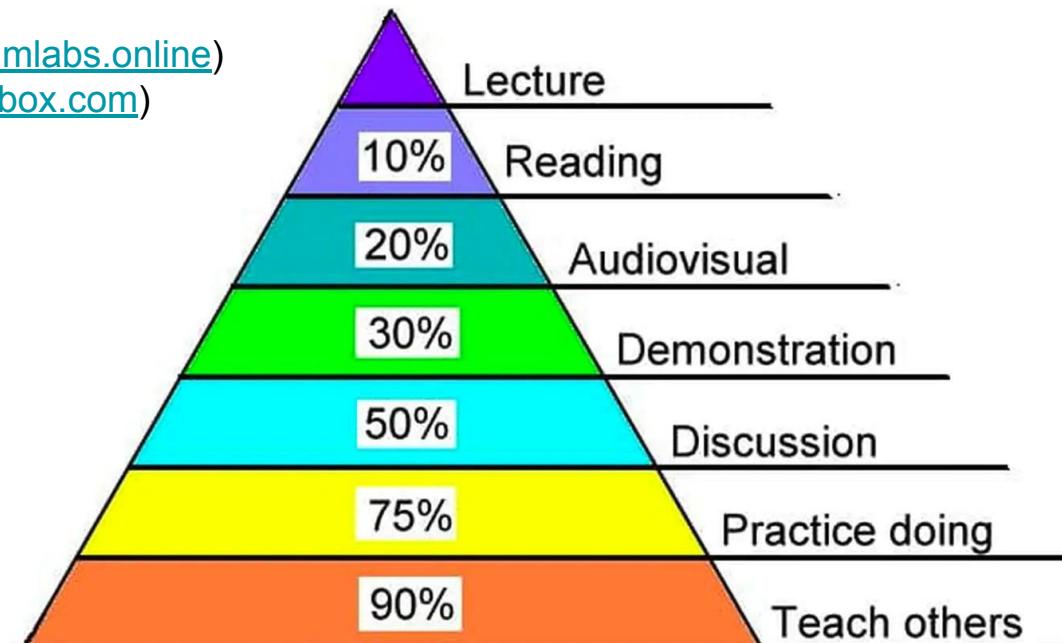
Platform แนะนำสำหรับการพัฒนาบุคลากร

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

ในแล็บนี้ให้ทำการสแกน ip เครื่องเป้าหมายและบอกว่ามี port อะไรบ้าง ด้วยโปรแกรม nmap รูปแบบ คำตอบ
พอร์ท,พอร์ท,พอร์ท

Machine LAB



[Open Machine LAB](#)

[VPN Access](#)

? How to use VPN DropCTF

อ่านเพิ่มเติม vpn และรับ ^^

ส่งคำตอบ



QUESTION 1

10 point

ใส่รหัสผ่าน

คำตอบมีจำนวน 8 อักษร



The live feed displays several user profiles with their names, titles, and descriptions of their challenges:

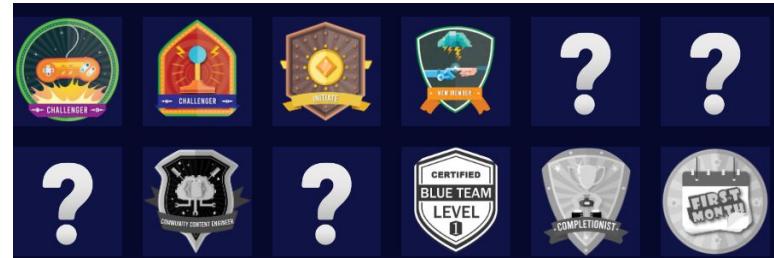
- Kiatisak: 2 ชั่วโมงที่แล้ว brute force #1
- Paramount: 4 ชั่วโมงที่แล้ว vulnerability web application #1
- jammieZnZnZ: 5 ชั่วโมงที่แล้ว WHAT IS HTTP METHOD #1
- jammieZnZnZ: 5 ชั่วโมงที่แล้ว WHAT IS PARAMETER #1
- ro.nyne: 13 ชั่วโมงที่แล้ว Unrestricted File Upload 0x01 #1

Scenario +
Point

Live Feed

Rating	Username	Point	Status
THREAT	bounssp2	25,805	
HACKER	TungGoD	25,255	DropDEFEND
MASTER	bawzazaEz	25,105	DropDEFEND
HARRY	Ar3mus	24,015	DropDEFEND
STAR	XDMAN	23,730	DropDEFEND
DEVIL	ParkerVIRUS	23,540	VIP
PIRATE	Nonthiwat339	23,465	

User Ranking

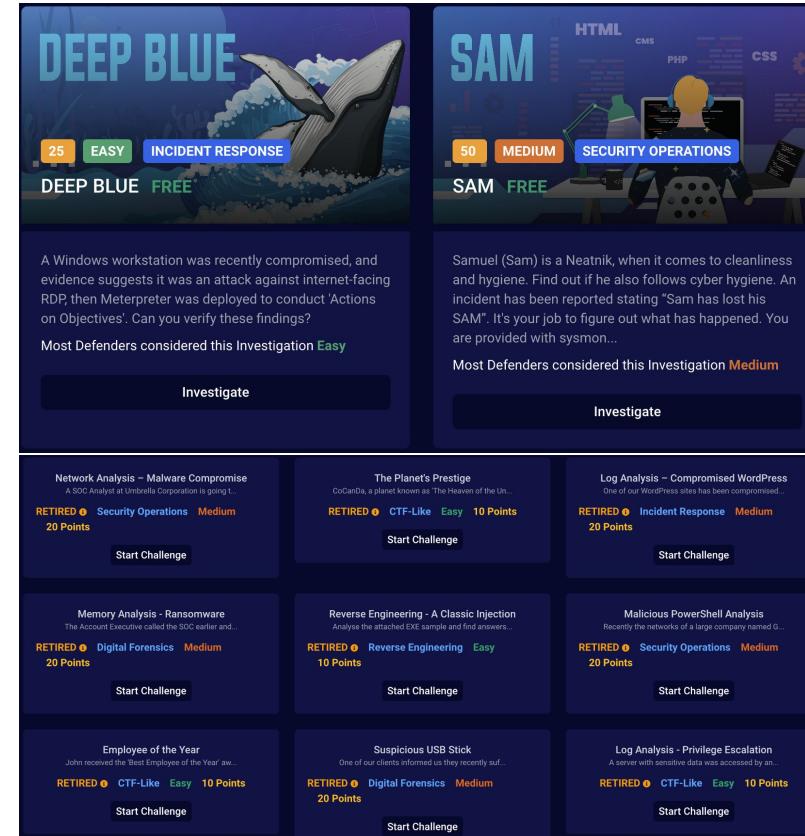


Badge

1 - Blue Team Lab Online (BTLO)

URL: <https://blueteamlabs.online>

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



The screenshot displays a grid of 12 challenge cards from the Blue Team Lab Online platform. Each card includes a title, a brief description, a difficulty level, and a 'Start Challenge' button.

- DEEP BLUE**: 25 EASY INCIDENT RESPONSE. DEEP BLUE FREE. A Windows workstation was recently compromised, and evidence suggests it was an attack against internet-facing RDP, then Meterpreter was deployed to conduct 'Actions on Objectives'. Can you verify these findings? Most Defenders considered this Investigation Easy. **Investigate**.
- SAM**: 50 MEDIUM SECURITY OPERATIONS. SAM FREE. Samuel (Sam) is a Neatnik, when it comes to cleanliness and hygiene. Find out if he also follows cyber hygiene. An incident has been reported stating "Sam has lost his SAM". It's your job to figure out what has happened. You are provided with sysmon... Most Defenders considered this Investigation Medium. **Investigate**.
- Network Analysis - Malware Compromise**: RETIRED. Security Operations. Medium. 20 Points. A SOC Analyst at Umbrella Corporation is going... **Start Challenge**.
- The Planet's Prestige**: RETIRED. CTF-LIKE. Easy. 10 Points. GoCarDi, a planet known as 'The Heaven of the Un...' **Start Challenge**.
- Log Analysis - Compromised WordPress**: RETIRED. Incident Response. Medium. 20 Points. One of our WordPress sites has been compromised... **Start Challenge**.
- Memory Analysis - Ransomware**: RETIRED. Digital Forensics. Medium. 20 Points. The Account Executive called the SOC earlier and... **Start Challenge**.
- Reverse Engineering - A Classic Injection**: RETIRED. Reverse Engineering. Easy. 10 Points. Analyse the attached EXE sample and find answers... **Start Challenge**.
- Malicious PowerShell Analysis**: RETIRED. Security Operations. Medium. 20 Points. Recently the networks of a large company named G... **Start Challenge**.
- Employee of the Year**: RETIRED. CTF-LIKE. Easy. 10 Points. John received the Best Employee of the Year aw... **Start Challenge**.
- Suspicious USB Stick**: RETIRED. Digital Forensics. Medium. 20 Points. One of our clients informed us they recently suf... **Start Challenge**.
- Log Analysis - Privilege Escalation**: RETIRED. CTF-LIKE. Easy. 10 Points. A server with sensitive data was accessed by an... **Start Challenge**.

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	<input type="button" value="Request Quote"/>

1 Month

£15

3 Months- Save 10%!

£40.5

6 Months- Save 15%!

£76.5

Annual- Save 20%!

£144

1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Challenge

หมวด:

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

1 Challenges left to unlock

Challenger I

0%



The Report II

This challenge is an extension for an existing '...'.

FREE Security Operations Medium 20 Points

Start Challenge

Follina

On a Friday evening when you were in a mood to c...

FREE Incident Response Easy 10 Points

Start Challenge

Search by name

Sort By

None

Status

Completed Not Completed Active Retired
 Coming Soon

Content

FREE PRO

Difficulties

Easy Medium Hard

Categories

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

Author

BTLO Community

Reset Filters

The Report

You are working in a newly established SOC where...

FREE Security Operations Easy 10 Points

Start Challenge

Bruteforce

Can you analyze logs from an attempted RDP brute...

FREE Incident Response Medium 20 Points

Start Challenge

Source

A vulnerability was identified in a widely used...

FREE Reverse Engineering Medium 20 Points

Start Challenge

The Package

Authorities are looking for a hacker who is plan...

FREE OSINT Easy 10 Points

Start Challenge

Veriarty

DI Lestrade has intercepted a transmission from...

FREE Digital Forensics Medium 20 Points

Start Challenge

Squid Game

Will you survive the Squid Games?

FREE CTF-Like Medium 20 Points

Start Challenge

Paranoid

I'm not paranoid, you are.

Shiba Insider

Can you uncover the insider?

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

10

Difficulty

Easy

Solves

3064

OS

Windows/Linux



Report.zip

10.4MB

Password

BTLO

Download File



redcanary | 2022 Threat Detection Report

TABLE OF CONTENTS

INTRODUCTION 3

METHODOLOGY 4

TRENDS 8

Introduction 9

Ransomware 11

Supply chain compromise 14

Vulnerabilities 17

Affiliates 21

Crypters-as-a-service 24

Common web shells 26

User-initiated initial access 29

Malicious macOS installers 31

Remote monitoring and management abuse 32

Linux coinminers 33

Abusing remote procedure calls 36

Defence validation and testing 39

THREATS 41

Introduction 42

Top ten threat highlights 44

Cobalt Strike 44

Impacket 47

SocGholish 50

Yellow Cockatoo 53

Gootkit 56

BloodHound 58

New activity clusters 60

Rose Flamingo 60

Silver Sparrow 63

Relevant threats of 2021 65

Bazar 65

Latent threats 66

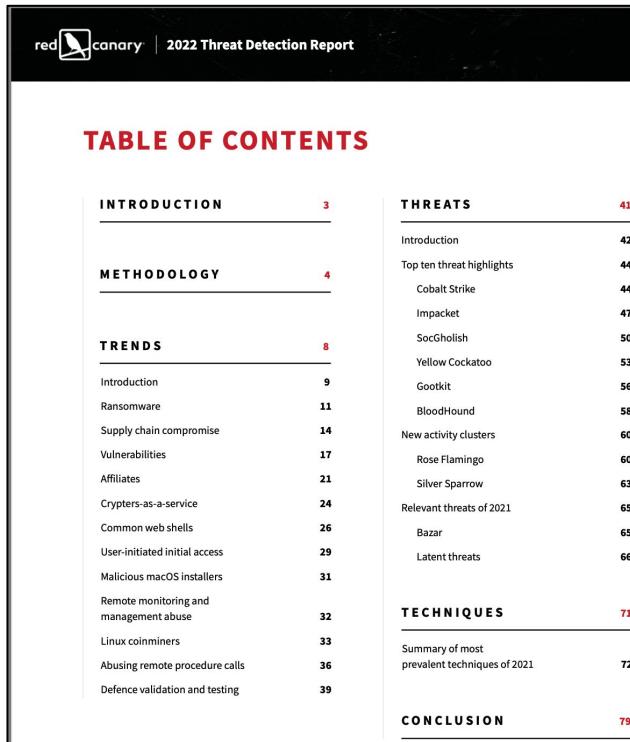
TECHNIQUES 71

Summary of most prevalent techniques of 2021 72

CONCLUSION 79

1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Challenge



redcanary | 2022 Threat Detection Report

TABLE OF CONTENTS

INTRODUCTION	3
METHODOLOGY	4
TRENDS	8
Introduction	9
Ransomware	11
Supply chain compromise	14
Vulnerabilities	17
Affiliates	21
Crypters-as-a-service	24
Common web shells	26
User-initiated initial access	29
Malicious macOS installers	31
Remote monitoring and management abuse	32
Linux coinminers	33
Abusing remote procedure calls	36
Defence validation and testing	39
THREATS	41
Introduction	42
Top ten threat highlights	44
Cobalt Strike	44
Impacket	47
SocGholish	50
Yellow Cockatoo	53
Gootkit	56
BloodHound	58
New activity clusters	60
Rose Flamingo	60
Silver Sparrow	63
Relevant threats of 2021	65
Bazar	65
Latent threats	66
TECHNIQUES	71
Summary of most prevalent techniques of 2021	72
CONCLUSION	79



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-XXXXXX) (1 points)

Format: CVE-XXXX-XXXXXX Submit

1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Challenge

Memory Analysis - Ransomware

The Account Executive called the SOC earlier and sounds very frustrated and angry. He stated he can't access any files on his computer and keeps receiving a pop-up stating that his files have been encrypted. You disconnected the computer from the network and extracted the memory dump of his machine and started analyzing it with Volatility. Continue your investigation to uncover how the ransomware works and how to stop it!

Volatility

Points
20

Difficulty
Medium

Solves
1673

OS
Windows/Linux

 Memory Dump
169 MB

Password
btlo

Download File



Challenge Submission

Run "vol.py -f infected.vmem --profile=Win7SP1x86 psscan" that will list all processes.
What is the name of the suspicious process? (3 points)

Format: @ProcessName

Submit

What is the parent process ID for the suspicious process? (3 points)

Parent Process ID (PPID)

Submit

What is the initial malicious executable that created this process? (3 points)

Format: filename.exe

Submit

1 - Blue Team Lab Online (BTLO)

URL: <https://blueteamlabs.online>

โจทย์แบบ Investigation



DeepBlueCLI PowerShell Event Viewer T1133 T1078.003

T1136.001 T1543.003

Resume Investigation

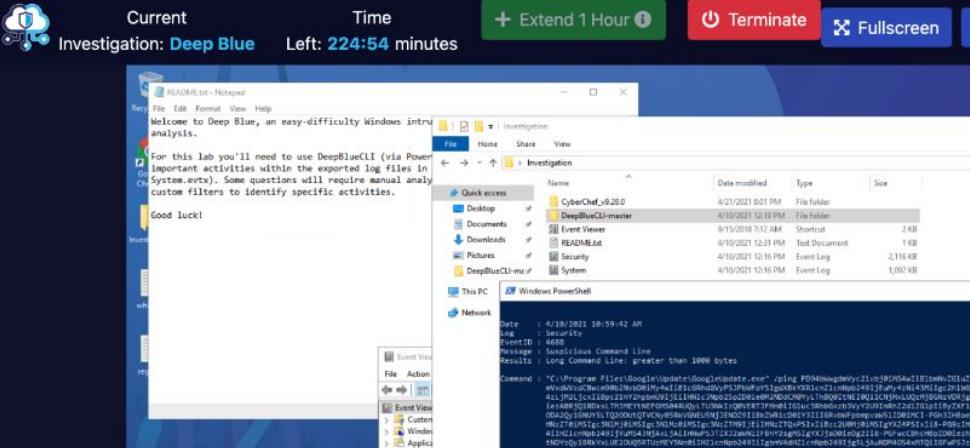


Points
25

Difficulty
Easy

Solves
6449

OS
Windows



The screenshot shows the Deep Blue investigation interface. At the top, it says "Current Investigation: Deep Blue Left: 224:54 minutes". There are buttons for "Extend 1 Hour", "Terminate", and "Fullscreen".

The main area has three panes:

- File Explorer:** Shows files like "CyberChef_v9.28.0", "DeepBlueCLI-master", "Event Viewer", "README.txt", "System", and "DeepBlueCLI-msf".
- Event Viewer:** Shows a log entry for event ID 4688: "Suspicious Command Line".
- Windows PowerShell:** Displays a command related to the event.

Below the panes, there's a text area with instructions and a "Submit" button.

Instructions: Investigate the Security.evtx log in Event Viewer. Process creation is being audited (event ID 4688). Identify the malicious executable downloaded that was used to gain a Meterpreter reverse shell, between 10:30 and 10:50 AM on the 10th of April 2021. (4 points)

Format: username, filename.exe

Submit

It's also believed that an additional account was created to ensure persistence between 11:25 AM and 11:40 AM on the 10th April 2021. What was the command line used to create this account? (Make sure you've found the right account!) (4 points)

Account Creation Command Line

What two local groups was this new account added to? (4 points)

Format: Group1, Group2

Submit

Submit

Submit

1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Investigation

Screenshot of the Blue Team Lab Online interface showing the investigation process:

Top Bar:
Current Investigation: Deep Blue Left: 224:54 minutes
Buttons: Extend 1 Hour, Terminate, Fullscreen, Clipboard, Details, Questions, Report Issue

Left Panel:
File Explorer showing a folder structure:
Desktop: CyberChef_V9.28.0 (File folder), DeepBlueCLI-master (Shortcut)
Documents: EventView, README.txt
Downloads: EventView
Pictures: Security
DeepBlueCLI-Lab (File folder): System (Event Log)
This PC: Windows PowerShell (Output of command)
Network: Event View, File Action, Custom, Windows, Application, Subscription

Windows PowerShell Output (Left):
Command: "C:\Program Files\Google\Update\GoogleUpdate.exe" /ping P0940wgdmv<21vbj0hs4i181bmhv7GluZz...
Decoded:
Date : 8/10/2021 10:59:42 AM
Log : Security
EventID : 4688
Message : Suspicious Command Line
Results : Long Command Line: greater than 1000 bytes

Right Panel:

Lab Details

OS Username	OS Password (no password)	Reserved to
btlo		183.89.90.91

Scenario



A Windows workstation was recently compromised, and evidence suggests it was an attack against internet-facing RDP, then Meterpreter was deployed to conduct 'Actions on Objectives'. Can you verify these findings?

ข้อควรระวัง 1: วิเคราะห์ไฟล์มัลแวร์

Follina

On a Friday evening when you were on your weekend, your team was alerted that a file was actively being exploited.

VirusTotal Any.Run OSINT

Points 10	Difficulty Easy	Solves 2116	OS Windows/Linux
---------------------	---------------------------	-----------------------	----------------------------

 Challenge.zip
10 KB

 Password infected

[Download File](#)

ไฟล์ติดรหัสผ่าน (infected)



← 43eecf22e8f914d44df3da16c23dcc2e076a8753.zip
✖ Chrome blocked this file because it is dangerous

[Delete](#)

Warning!

This file includes **REAL MALWARE**. Please be careful when interacting with it.

We strongly suggest players create a 'dirty' virtual machine to analyse malicious files in.

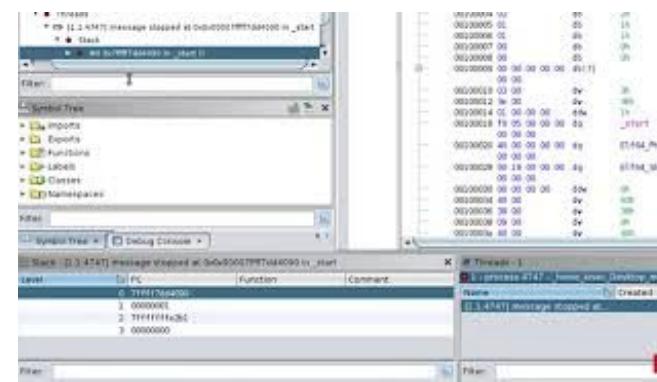
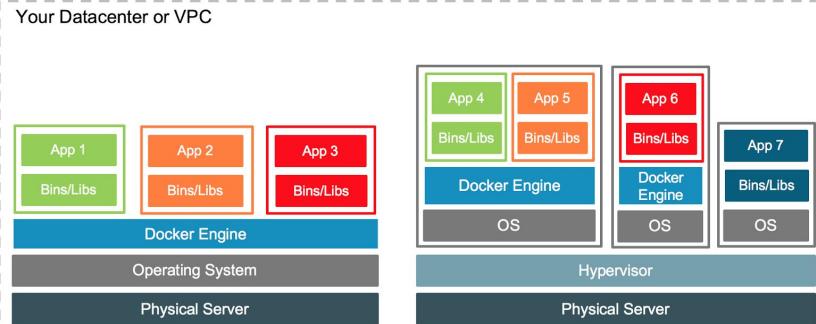
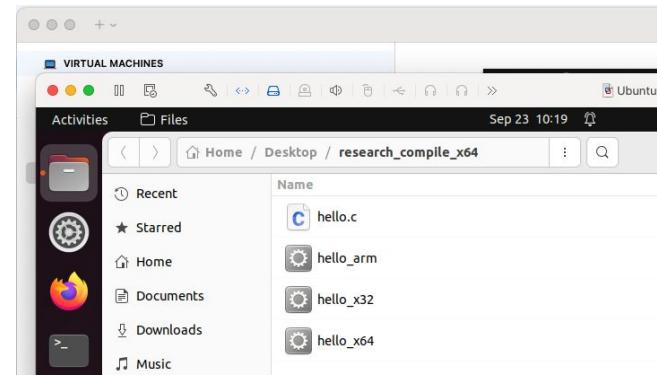
[Understood](#)

มีคำเตือนให้วิเคราะห์ใน VM
ที่สร้างมาเพื่อวิเคราะห์เท่านั้น

Offline Malware Sandbox

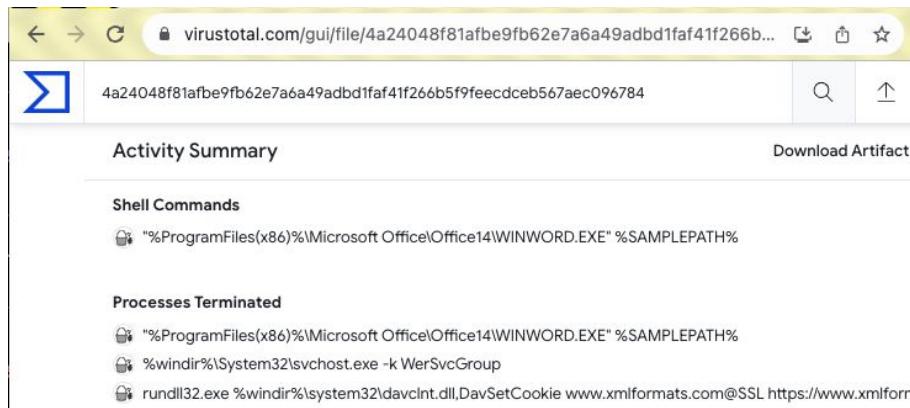
Virtual Machine:

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



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

Online Malware Sandbox



virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b...

4a24048f81afbe9fb62e7a6a49adbd1faf41f266b59feecdceb567aec096784

Activity Summary

Download Artifacts

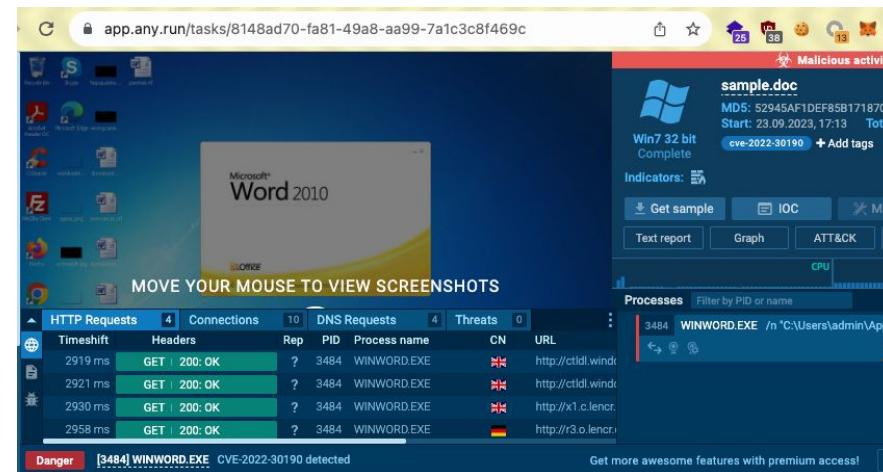
Shell Commands

```
! "%ProgramFiles(x86)%\Microsoft Office\Office14\WINWORD.EXE" %SAMPLEPATH%
```

Processes Terminated

```
! "%ProgramFiles(x86)%\Microsoft Office\Office14\WINWORD.EXE" %SAMPLEPATH%
! %windir%\System32\svchost.exe -k WerSvcGroup
! rundll32.exe %windir%\system32\davclnt.dll,DavSetCookie www.xmlformats.com@SSL https://www.xmlform...
```

<https://www.virustotal.com>



app.any.run/tasks/8148ad70-fa81-49a8-aa99-7a1c3c8f469c

MOVE YOUR MOUSE TO VIEW SCREENSHOTS

HTTP Requests	4	Connections	10	DNS Requests	4	Threats	0
Timeshift	Headers	Rep	PID	Process name	CN	URL	
2919 ms	GET 200: OK	?	3484	WINWORD.EXE	GB	http://ctld.wind...	
2921 ms	GET 200: OK	?	3484	WINWORD.EXE	GB	http://ctld.wind...	
2930 ms	GET 200: OK	?	3484	WINWORD.EXE	GB	http://x1.clenr...	
2958 ms	GET 200: OK	?	3484	WINWORD.EXE	DE	http://r3.o.lencr...	

Danger [3484] WINWORD.EXE CVE-2022-30190 detected

sample.doc
Win7 32 bit Complete
MD5: 52945AF1DEFF85B171870B
Start: 23.09.2023, 17:13 Total: 13
cve-2022-30190 + Add tags

Indicators: 5

Get sample IOC Mal

Text report Graph ATT&CK CPU

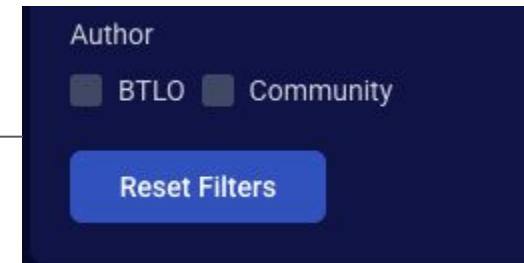
Processes Filter by PID or name

3484 WINWORD.EXE /n 'C:\Users\admin\AppData\Local\Temp\~\$1~.doc'

Get more awesome features with premium access!

<https://app.any.run>

ข้อควรระวัง 2: User-Generated Content



 **Created By**

 **BTLO** 812 days ago

เจ้าของ Platform สร้าง
โจทย์เอง (Official)

Warning!
This external link is going to take you to
<https://smbsid.wordpress.com/2021/04/20/memory-analysis-ransomware>.

Even though these links are verified at the time of publishing them to BTLO, they could be compromised at any time. We do not take responsibility for any damage caused outside of our platform.

Be careful out there defender!

Understood & Proceed

Unofficial Writeup

 **Created By**

 **chaosmunkey** 693 days ago

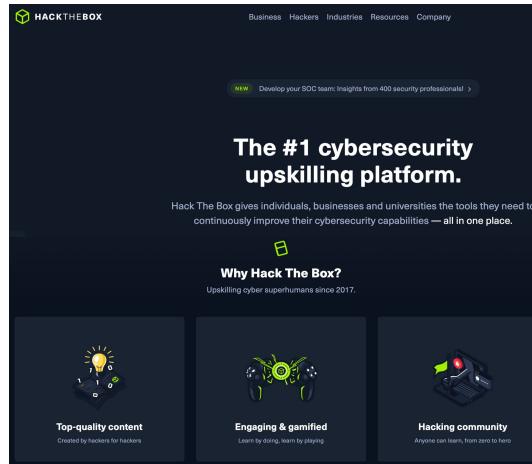
ผู้ใช้งาน (Community)
ช่วยกันสร้างโจทย์

2 - Hack The Box

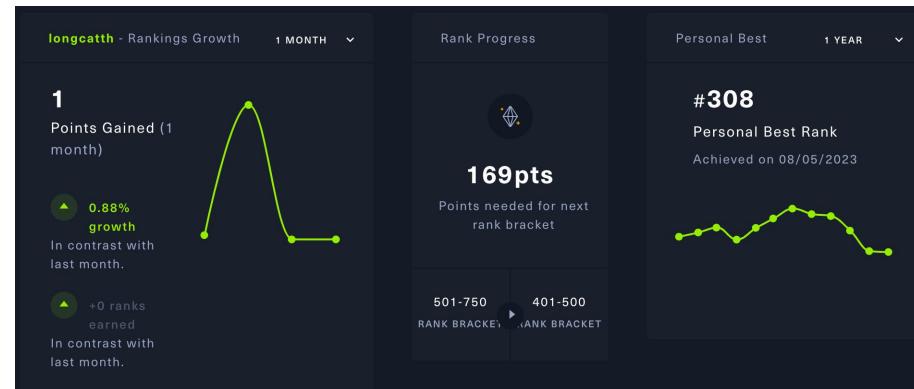
- จำลองการโจมตีระบบ
ที่มีช่องโหว่ เรียกว่า Box
- เน้นสำหรับ Red Team
- รองรับ ภาษาอังกฤษ
- เริ่มตั้งแต่การหาช่องโหว่
ไปจนถึงการลงมือโจมตี

แยกย่อยออกเป็น:

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



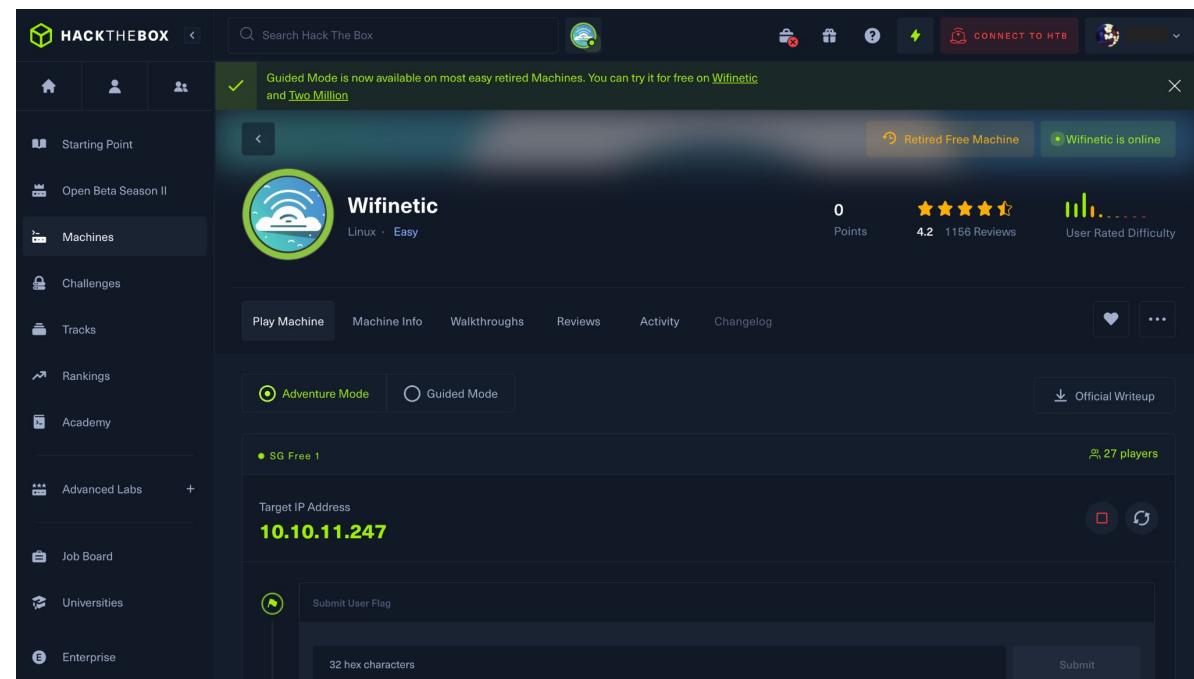
The homepage of HackTheBox features a dark-themed header with the logo and navigation links: Business, Hackers, Industries, Resources, Company. Below the header is a banner with the text "The #1 cybersecurity upskilling platform." and a subtext about providing tools for continuous improvement. A section titled "Why Hack The Box?" highlights "Top-quality content", "Engaging & gamified", and "Hacking community".



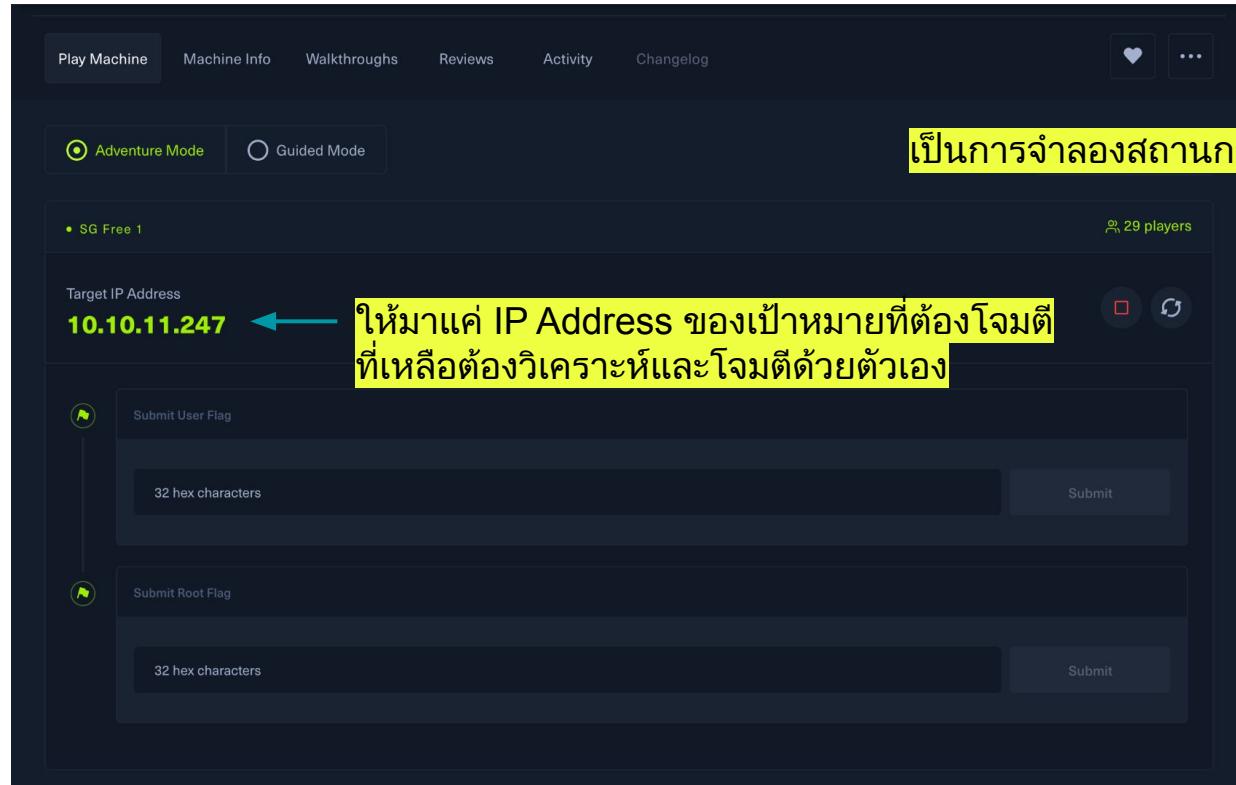
2 - Hack The Box

HTB Machine

- ไม่มีเนื้อหาให้เรียน
- มีแต่แลปให้ลองแฮก
 - เป็นระบบที่มีช่องโหว่
 - ให้ลองแฮกเข้าไป
 - สิทธิ์ต่อ
(user.txt)
 - สิทธิ์สูง
(root.txt)
- สามารถเลือกได้ว่าจะ
 - Adventure mode
 - Guided mode



Adventure Mode ของ Hack The Box



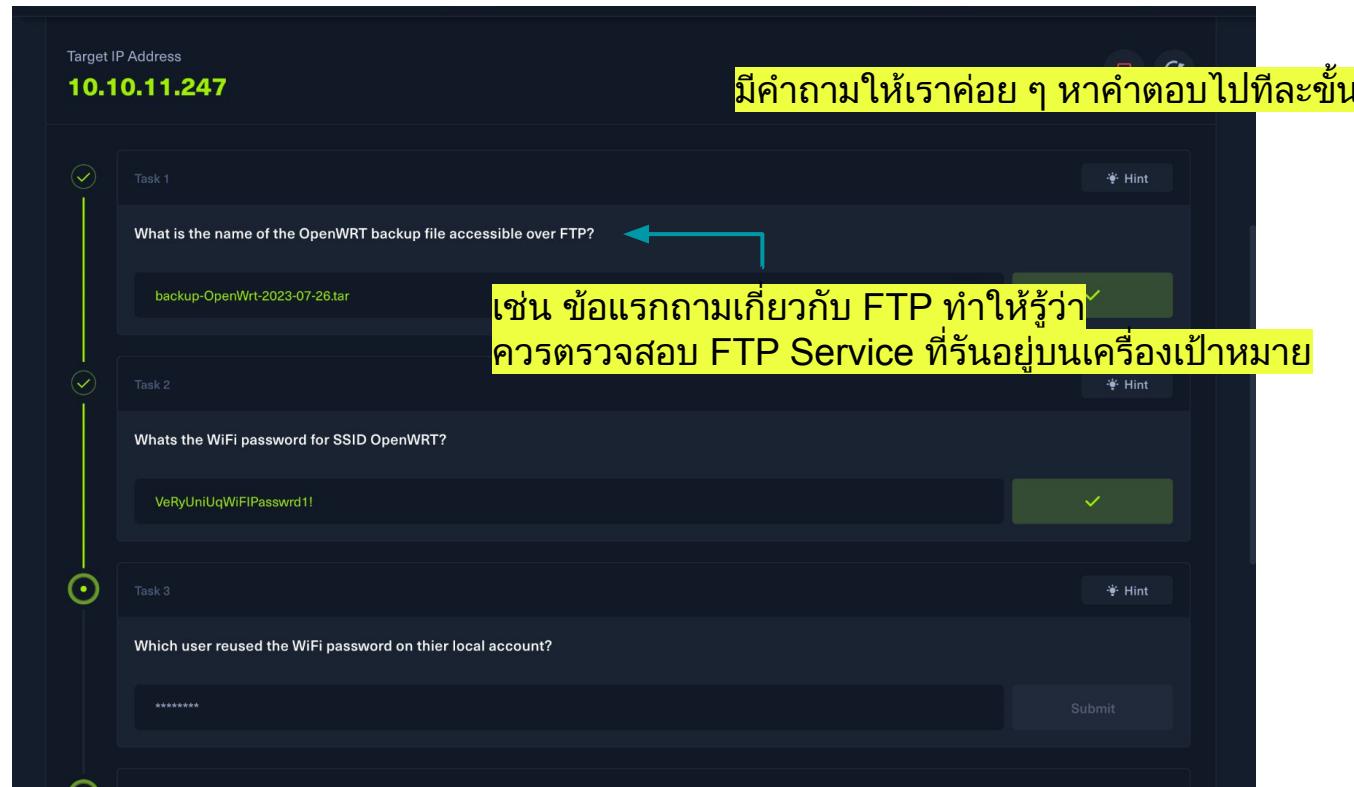
เป็นการจำลองสถานการณ์โจมตีจริง

Target IP Address
10.10.11.247 ← ให้มาแค่ IP Address ของเป้าหมายที่ต้องโจมตีที่เหลืออัตโนมัติและโจมตีด้วยตัวเอง

Submit User Flag
32 hex characters

Submit Root Flag
32 hex characters

Guided Mode ของ Hack The Box



Target IP Address
10.10.11.247

Task 1

What is the name of the OpenWRT backup file accessible over FTP?

backup-OpenWrt-2023-07-26.tar

Task 2

What's the WiFi password for SSID OpenWRT?

VeRyUniUqWiFiPasswrd1!

Task 3

Which user reused the WiFi password on their local account?

มีคำถามให้เราค่อย ๆ หาคำตอบไปทีละข้อ

เช่น ข้อแรกถามเกี่ยวกับ FTP ทำให้รู้ว่า ควรตรวจสอบ FTP Service ที่รันอยู่บนเครื่องเป้าหมาย

Guided Mode ของ Hack The Box

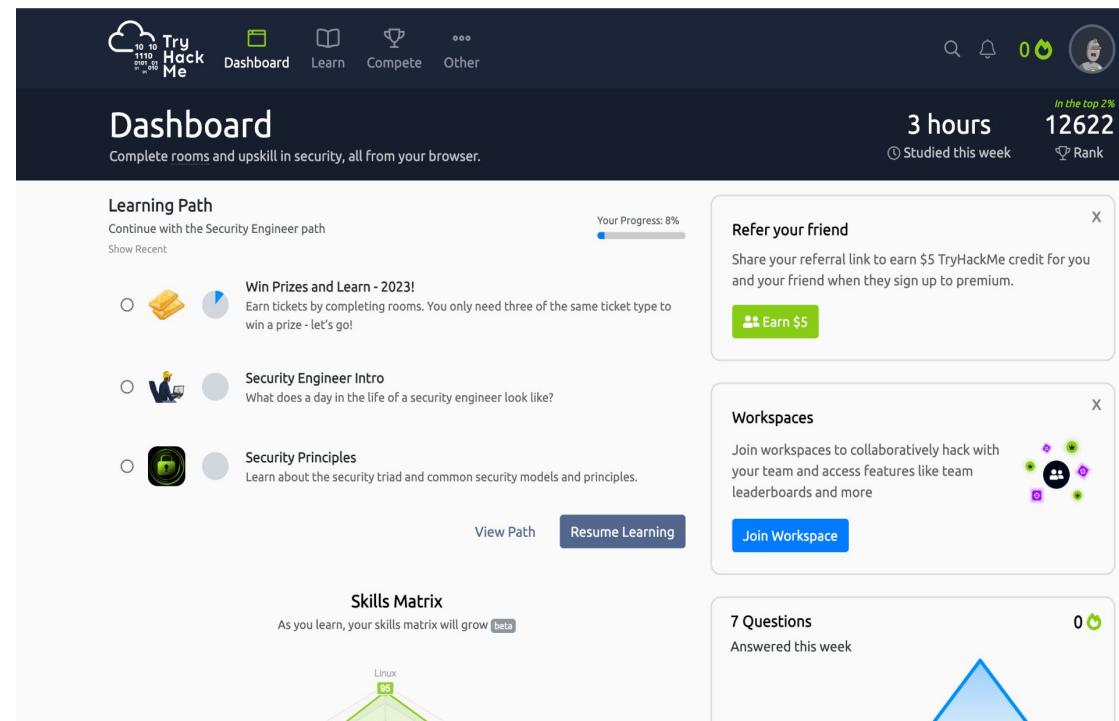
```
└# ftp
ftp> open 10.10.11.247
Connected to 10.10.11.247.
220 (vsFTPD 3.0.3)
Name (10.10.11.247:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||45433|)
150 Here comes the directory listing.
-rw-r--r-- 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

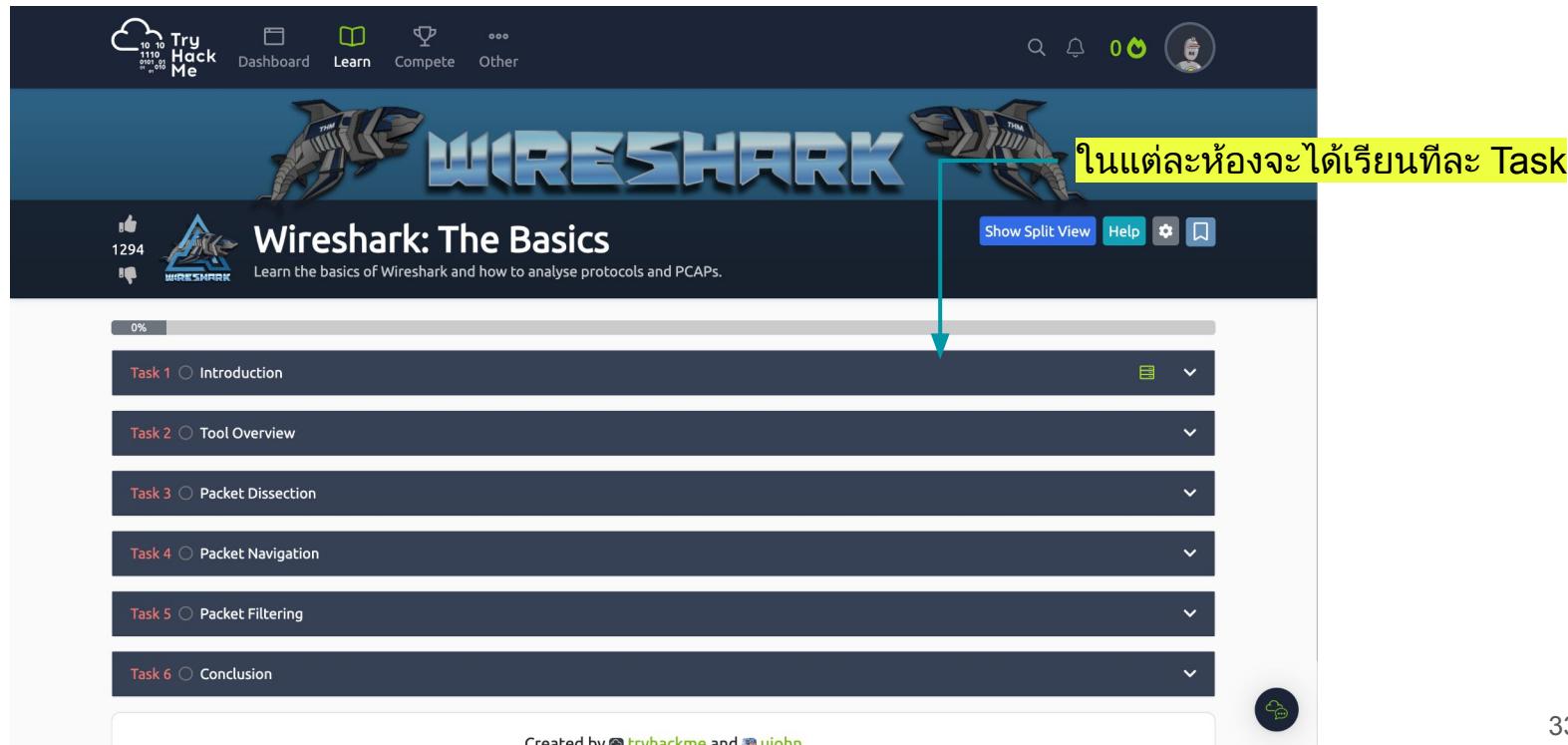
- คอร์สเรียนพร้อม Lab
- อธิบายแบบ Step-by-step
- เน้นไปที่การเรียนรู้
- มีทั้งคอร์สฝึก Red Team และ Blue Team
- เลือกเรียนตาม Path ที่สนใจ
- หรือเลือกเรียนทีละหัวข้อได้
- มีทั้งแบบฟรีและแบบที่ต้องสมัคร Premium
- คอร์สเรียนหลากหลาย



The screenshot shows the TryHackMe dashboard with the following details:

- Header:** TryHackMe logo, navigation menu (Dashboard, Learn, Compete, Other), user stats (0 tickets, In the top 2%, 3 hours studied this week, 12622 rank).
- Dashboard Section:** Complete rooms and upskill in security, all from your browser.
- Learning Path:** Continue with the Security Engineer path. Your Progress: 8%.
- Path Options:**
 - Win Prizes and Learn - 2023! (Earn tickets by completing rooms. You only need three of the same ticket type to win a prize - let's go!)
 - Security Engineer Intro (What does a day in the life of a security engineer look like?)
 - Security Principles (Learn about the security triad and common security models and principles.)
- Buttons:** View Path, Resume Learning.
- Refer your friend:** Share your referral link to earn \$5 TryHackMe credit for you and your friend when they sign up to premium. Earn \$5 button.
- Workspaces:** Join workspaces to collaboratively hack with your team and access features like team leaderboards and more. Join Workspace button.
- Skills Matrix:** As you learn, your skills matrix will grow. Linux icon.
- 7 Questions:** Answered this week. 0 tickets.

ตัวอย่างห้องใน TryHackMe



The screenshot shows the TryHackMe platform interface for a 'Wireshark: The Basics' room. At the top, there's a navigation bar with icons for Dashboard, Learn, Compete, and Other, along with a search bar, notifications, and user profile. Below the header, the room title 'Wireshark: The Basics' is displayed with a Wireshark logo and a count of 1294 likes.

A yellow callout box with the text 'ในแต่ละห้องจะได้เรียนทีละ Task' (In each room, you will learn one task at a time) has an arrow pointing to the first task in the list.

The main content area lists six tasks:

- Task 1 ○ Introduction
- Task 2 ○ Tool Overview
- Task 3 ○ Packet Dissection
- Task 4 ○ Packet Navigation
- Task 5 ○ Packet Filtering
- Task 6 ○ Conclusion

At the bottom of the room view, it says 'Created by trvhackme and uiohn' and features a 'Leave a comment' button.

ตัวอย่างห้องใน TryHackMe

คำถามในแต่ละ Step มีหลายรูปแบบ ได้แก่

- ทำความเข้าใจ เนื้อหา และตอบคำถาม
- ทำความเข้าใจ เนื้อหา และหาคำตอบจาก ไฟล์ที่กำหนดให้
- ทำความเข้าใจ เนื้อหา และหาคำตอบจาก ระบบ Interactive ผ่านหน้าเว็บ
- ทำความเข้าใจ เนื้อหา และหาคำตอบจาก การทำ 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

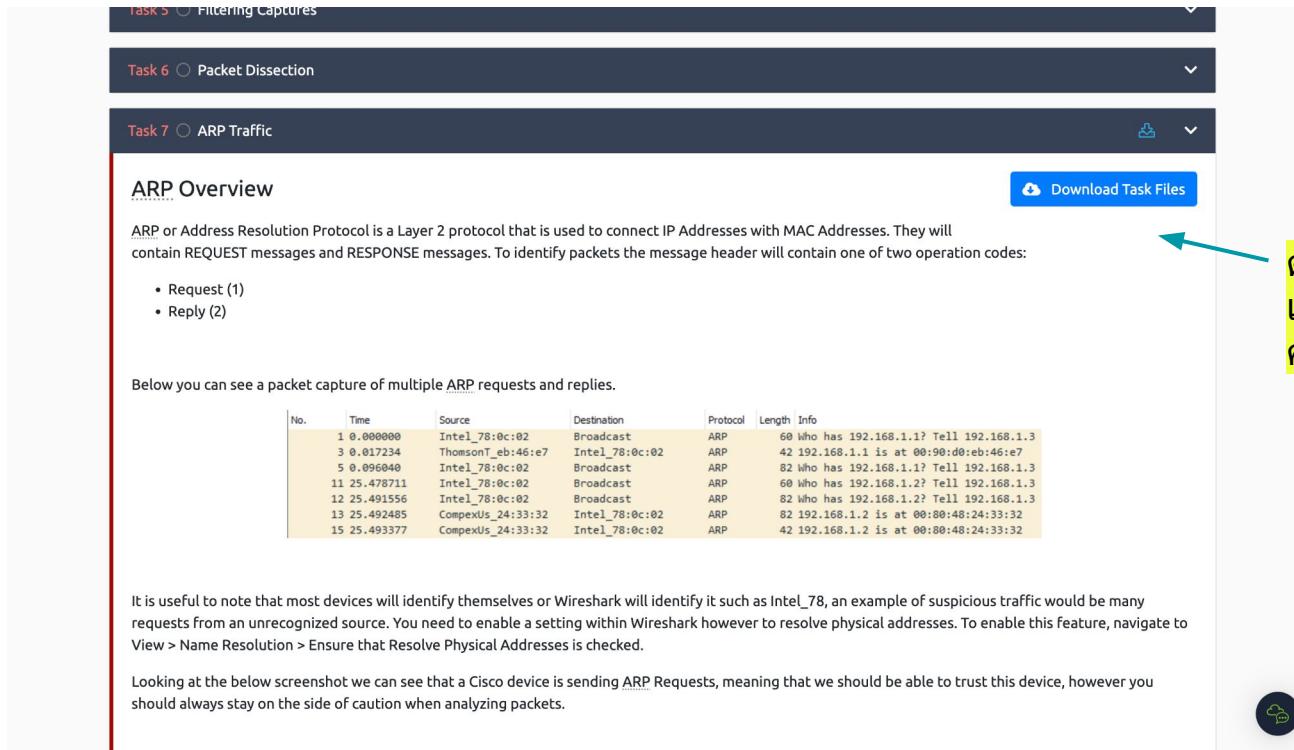
ตอบคำถามตาม
ความเข้าใจ

Task 3 Deploy



ตัวอย่างห้องใน TryHackMe - (2) ดาวน์โหลดไฟล์

ทำความเข้าใจเนื้อหาแล้วหาคำตอบ
จากไฟล์ที่กำหนดให้



The screenshot shows the Wireshark interface with three tabs at the top: Task 5 (Filtering Captures), Task 6 (Packet Dissection), and Task 7 (ARP Traffic). Task 7 is currently selected, displaying an 'ARP Overview' section. The overview explains that ARP is a Layer 2 protocol used to connect IP addresses with MAC addresses, containing REQUEST and RESPONSE messages. It lists two operation codes: Request (1) and Reply (2). Below this, it states: "Below you can see a packet capture of multiple ARP requests and replies." A table of captured ARP packets is shown, with the last few rows highlighted in yellow. An arrow points from the text "ดาวน์โหลดไฟล์ที่เกี่ยวข้องเพื่อหาคำตอบ" to the 'Download Task Files' button in the top right of the ARP Overview section.

Task 5 Filtering Captures

Task 6 Packet Dissection

Task 7 ARP Traffic

ARP Overview

Download Task Files

ARP or Address Resolution Protocol is a Layer 2 protocol that is used to connect IP Addresses with MAC Addresses. They will contain REQUEST messages and RESPONSE messages. To identify packets the message header will contain one of two operation codes:

- Request (1)
- Reply (2)

Below you can see a packet capture of multiple ARP requests and replies.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Intel_78:0c:02	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.3
3	0.017234	ThomsonT_eb:46:e7	Intel_78:0c:02	ARP	42	192.168.1.1 is at 00:90:eb:46:e7
5	0.096040	Intel_78:0c:02	Broadcast	ARP	82	Who has 192.168.1.1? Tell 192.168.1.3
11	25.478711	Intel_78:0c:02	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.3
12	25.491556	Intel_78:0c:02	Broadcast	ARP	82	Who has 192.168.1.2? Tell 192.168.1.3
13	25.492485	Compulex_U_24:33:32	Intel_78:0c:02	ARP	82	192.168.1.2 is at 00:80:48:24:33:32
15	25.493377	Compulex_U_24:33:32	Intel_78:0c:02	ARP	42	192.168.1.2 is at 00:80:48:24:33:32

It is useful to note that most devices will identify themselves or Wireshark will identify it such as Intel_78, an example of suspicious traffic would be many requests from an unrecognized source. You need to enable a setting within Wireshark however to resolve physical addresses. To enable this feature, navigate to View > Name Resolution > Ensure that Resolve Physical Addresses is checked.

Looking at the below screenshot we can see that a Cisco device is sending ARP Requests, meaning that we should be able to trust this device, however you should always stay on the side of caution when analyzing packets.



ตัวอย่างห้องใน TryHackMe - (3) Interactive

ทำความเข้าใจเนื้อหาแล้วหาคำตอบ
จากระบบ Interactive บนหน้าเว็บ

Task 4 Making A Request

Task 5 Practical

Using the website on the right, we can build requests to make DNS queries and view the results. The website will also show you the command you'd need to run on your own computer if you wished to make the requests yourself.

Answer the questions below

What is the CNAME of shop.website.thm?

shops.myshopify.com Correct Answer

What is the value of the TXT record of website.thm?

THM[7012BBA60997F35A9516C2E16D2944FF] Correct Answer Hint

What is the numerical priority value for the MX record?

30 Correct Answer

What is the IP address for the A record of www.website.thm?

10.10.10.10 Correct Answer

Created by tryhackme

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 262172 users are in here and this room is 862 days old.

DNS Type subdomain Send DNS Request

user@thm:~\$ nslookup website.thm

ระบบ Interactive

How DNS Works

ตัวอย่างห้องใน TryHackMe - (3) Interactive

ทำความเข้าใจเนื้อหาแล้วหาคำตอบ
จากระบบ Interactive บนหน้าเว็บ

Task 6 ○ Lab Work

Lab Work

Click on the View Site button, which will display the lab on the right side of the screen.

In the static lab attached, a sample dashboard and events are displayed. When a suspicious activity happens, an Alert is triggered, which means some events match the condition of some rule already configured. Complete the lab and answer the following questions.

Answer the questions below

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

Answer format: *****,*
 Submit Hint

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

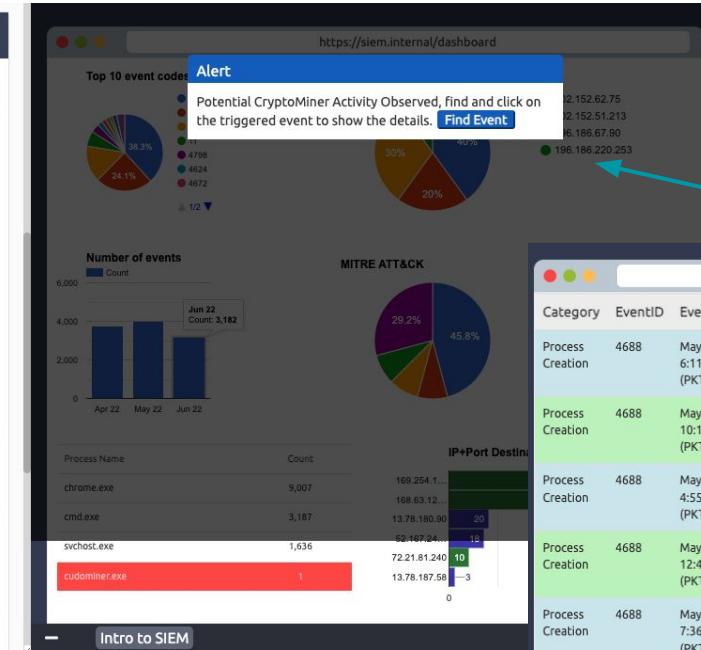
Answer format: ****,*
 Submit

What is the hostname of the suspect user?

Answer format: *****
 Submit

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

Answer format: *****
 Submit

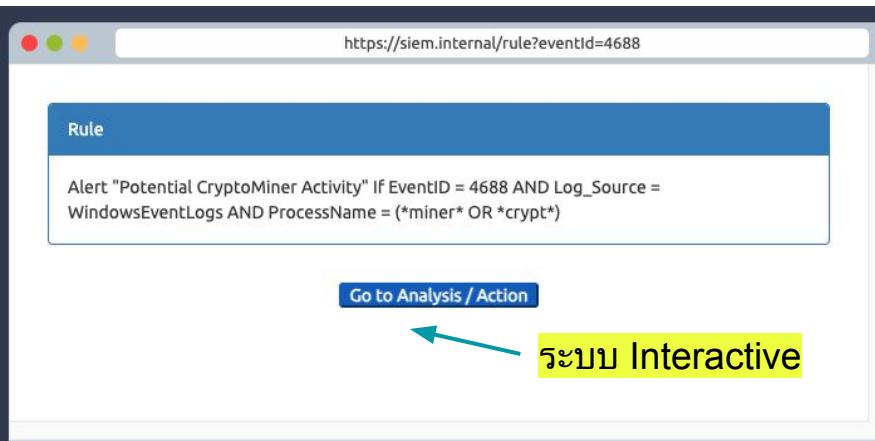


Category	EventID	EventTime	Severity	NewProcessId	ProcessId	Log_Source	EventType
Process Creation	4688	May 7, 2022 6:11 PM (PKT)	INFO	0x5c74eb	1657	WindowsEventLogs	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 10:10 PM (PKT)	INFO	0x0ad4d8	2600	WindowsEventLogs	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 4:55 PM (PKT)	INFO	0x32b4ca	3199	WindowsEventLogs	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 12:40 AM (PKT)	INFO	0xd21aef	1845	WindowsEventLogs	AUDIT_SUCCESS
Process Creation	4688	May 6, 2022 7:36 AM (PKT)	INFO	0xd86ed0	2830	WindowsEventLogs	AUDIT_SUCCESS
Process Creation	4688	May 4, 2022 12:57 PM (PKT)	INFO	0x49957e	1433	WindowsEventLogs	AUDIT_SUCCESS

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

ตัวอย่างห้องใน TryHackMe - (3) Interactive

ทำความเข้าใจเนื้อหาแล้วหาคำตอบ
จากระบบ Interactive บนหน้าเว็บ



A screenshot of a web browser window titled "https://siem.internal/rule?eventId=4688". The page displays a security rule titled "Rule" which states: "Alert "Potential CryptoMiner Activity" If EventID = 4688 AND Log_Source = WindowsEventLogs AND ProcessName = (*miner* OR *crypt*)". Below the rule is a blue button labeled "Go to Analysis / Action". A yellow box highlights the word "ระบบ Interactive" with a blue arrow pointing from it towards the "Go to Analysis / Action" button.

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

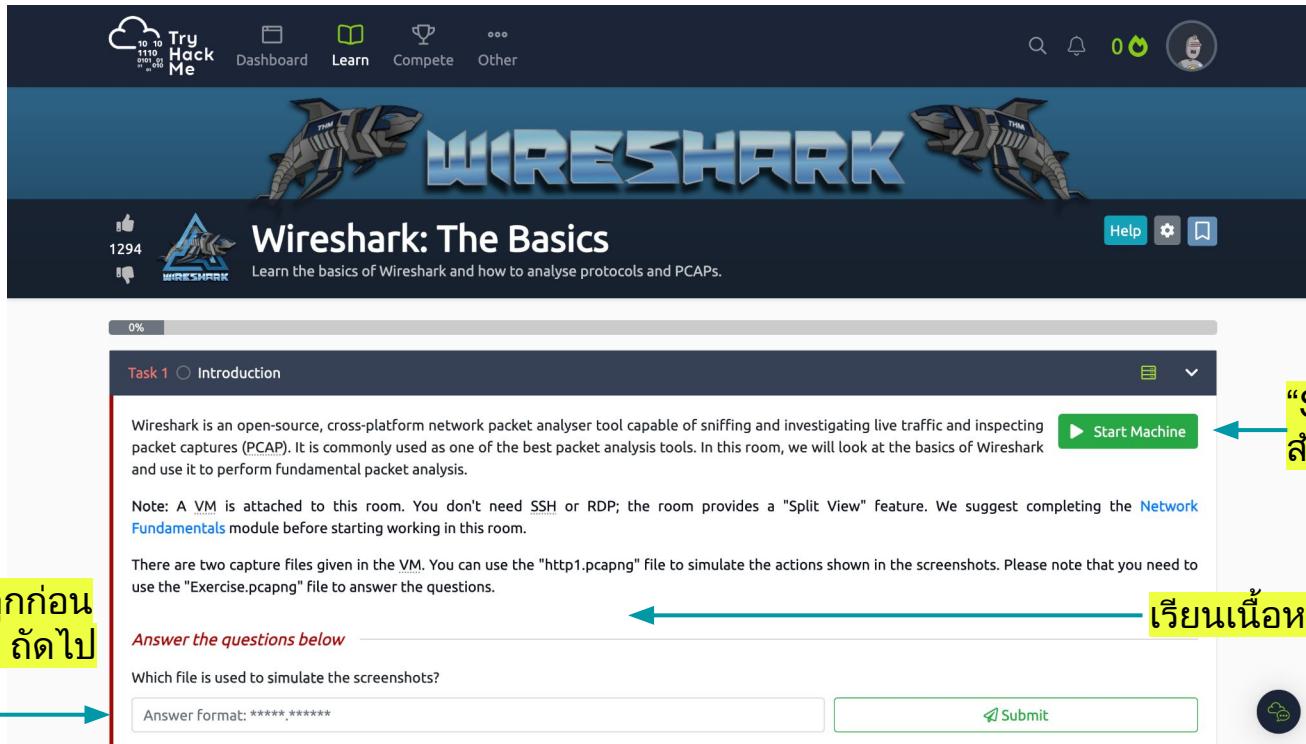
Examine the rule and the suspicious process; which term matched the rule that caused the alert?

miner

Correct Answer

ตัวอย่างห้องใน TryHackMe - (4) Lab

ทำความเข้าใจเนื้อหาแล้วหาคำตอบจากการทำ Lab



The screenshot shows a challenge room titled "Wireshark: The Basics". The room introduction states: "Wireshark is an open-source, cross-platform network packet analyser tool capable of sniffing and investigating live traffic and inspecting packet captures (PCAP). It is commonly used as one of the best packet analysis tools. In this room, we will look at the basics of Wireshark and use it to perform fundamental packet analysis." A green "Start Machine" button is highlighted with a yellow box and an arrow pointing to it from the text "สำหรับทำ Lab". Below the introduction, there is a note about a VM being attached to the room. The challenge instructions ask: "There are two capture files given in the VM. You can use the \"http1.pcapng\" file to simulate the actions shown in the screenshots. Please note that you need to use the \"Exercise.pcapng\" file to answer the questions." A red arrow points from the text "เรียนเนื้อหา ก่อนเริ่มทำ Lab" to the "Answer the questions below" section. At the bottom, there is a question: "Which file is used to simulate the screenshots?" with an input field and a "Submit" button.

ตอบคำถามให้ถูกก่อน
จะผ่านไป Task ถัดไป

"Start Machine"
สำหรับทำ Lab

เรียนเนื้อหา ก่อนเริ่มทำ Lab

Task 1 ○ Introduction

Wireshark is an open-source, cross-platform network packet analyser tool capable of sniffing and investigating live traffic and inspecting packet captures (PCAP). It is commonly used as one of the best packet analysis tools. In this room, we will look at the basics of Wireshark and use it to perform fundamental packet analysis.

▶ Start Machine

Note: A VM is attached to this room. You don't need SSH or RDP; the room provides a "Split View" feature. We suggest completing the Network Fundamentals module before starting working in this room.

There are two capture files given in the VM. You can use the "http1.pcapng" file to simulate the actions shown in the screenshots. Please note that you need to use the "Exercise.pcapng" file to answer the questions.

Answer the questions below

Which file is used to simulate the screenshots?

Answer format: *****.*****

Submit

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

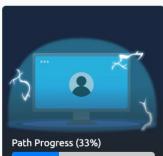


Jr Penetration Tester

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



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

„ Beginner ⓘ 32 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



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



Attacking and Defending AWS

Learn how attackers compromise AWS environments

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

„ Beginner ⓘ 32 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

„ Beginner ⓘ 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...

„ Beginner ⓘ 40 hours

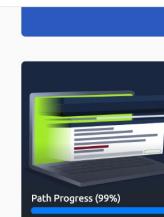


CompTIA Pentest+

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

„ Beginner ⓘ 32 hours



Complete Beginner

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

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

„ Beginner ⓘ 64 hours

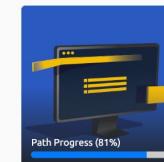


Offensive Pentesting

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

„ Beginner ⓘ 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	ฟรี	4xx ห้อง
Access to Networks	✗	✓	✓	Premium	2xx ห้อง
Faster Machines	✗	✓	✓		
Private OpenVPN Servers	✗	✓	✓	แต่ห้อง Premium จะมีเนื้อหา	
Private King of the Hill Games	✗	✓	✓	ที่ละเอียดและครบถ้วนกว่า	
Custom Learning Paths	✗	✗	✓		
Advanced Reporting	✗	✗	✓		
Transferable Licensing	✗	✗	✓		
Dedicated Customer Success Manager	✗	✗	✓		

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 แล้วหาอันที่มองว่า เหมาะกับตนเอง และคุ้มค่าที่จะใช้เวลา กับมัน
- ระวังความเสี่ยงจากการดาวน์โหลดไฟล์ที่อาจ อันตรายจาก Learning Platform ต่าง ๆ

CTF คืออะไร ?



ย่อมาจาก Capture The Flag

ในฝั่ง Computer Security

- ★ แข่งขันเพื่อชิงชัย
- ★ ชิง 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 หรือชื่อนั้นเอง) เอาไว้ยืนยันเพื่อเก็บคะแนน

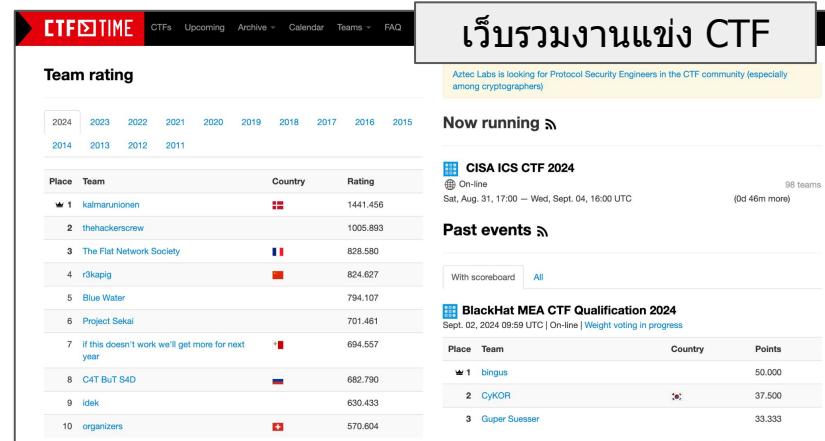
2. Attack-Defence

แต่ละทีมมีคอมพิวเตอร์เป็นฐานของตัวเอง ให้แฮกไปที่เครื่องทีมอื่น โดยทางช่องโหว่ เช่นโคดชิ้นมาโลมตี เพื่อชิงลงมา อาจจะอยู่ในไฟล์ เช่น C:\flag.txt และอาจจะสามารถป้องกันเครื่องของตัวเอง ได้ด้วยโดยจะมี กฎกติกาว่าให้ทำการแก้ไขอะไรได้บ้าง

3. Mixed หรือแบบอื่น ๆ

ตามแต่จะเอาไปดัดแปลงใช้ได้ เช่น wargame ที่เล่นเมื่อไรก็ได้

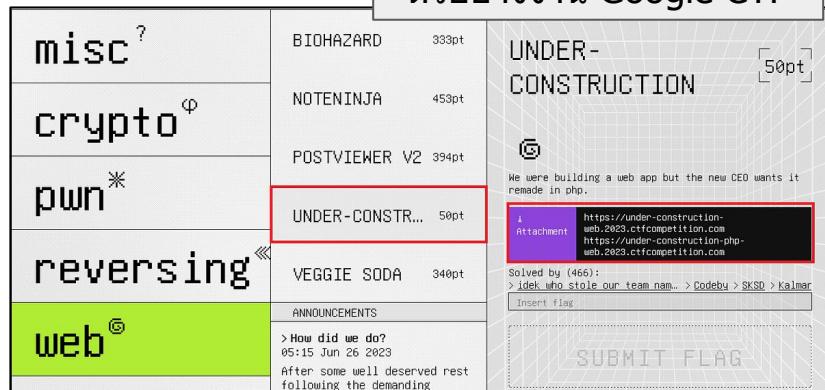
<https://ctftime.org>



The screenshot shows the CTFTIME website's homepage. The top navigation bar includes links for CTFs, Upcoming, Archive, Calendar, Teams, and FAQ. Below the navigation is a "Team rating" section with a table of current standings. The table lists 10 teams with their names, countries, and ratings. A note at the bottom of the table says "If this doesn't work we'll get more for next year". To the right, there are sections for "Now running" (CISA ICS CTF 2024) and "Past events" (BlackHat MEA CTF Qualification 2024).

Place	Team	Country	Rating
1	kalmarunionen	DK	1441.456
2	thehackerscrew	DK	1005.893
3	The Flat Network Society	FR	828.580
4	r3kapig	DK	824.627
5	Blue Water	DK	794.107
6	Project Sekai	DK	701.481
7	If this doesn't work we'll get more for next year	DK	694.557
8	C4T BuT S4D	DK	682.790
9	idek	DK	630.433
10	organizers	DK	570.604

ด้วยผ่าน Google CTF



The screenshot shows the Google CTF competition interface. It features a grid of challenges categorized by color: green (misc, crypto, pwn, reversing, web), red (under-construction), and blue (announcements). Each challenge has a title, points, and a status bar indicating if it's solved or not. A specific challenge in the red row is highlighted with a red border.

Challenge Category	Title	Points	Status
green	misc?	333pt	Solved
green	crypto ^φ	453pt	Solved
green	postviewer v2	394pt	Solved
red	under-constr...	50pt	Solved
blue	VEGGIE SODA	340pt	Solved
blue	ANNOUNCEMENTS	1pt	Solved

Badge ของผู้ชนะ DEFCON CTF
(เข้างานสัมมนาฟรีตตลอดซีพี)

ทำไมถึงควรเล่น CTF

- ★ สนุก มันส์ เมื่อൺความว่าทำไม่ถึง เล่นเกม อ่านการ์ตูน
- ★ งานใหญ่ ๆ จะมีรางวัลให้คนชนะ เป็นเงินบ้าง แล้วไอเท็มบ้าง
- ★ ได้เรียนรู้ Computer Security แบบลงมือทำจริง ได้ลองแฮก ลองแก้ไขโจทย์ปัญหา ยาก ๆ ที่ต้องไปหาอ่านสิ่งใหม่ ๆ อัปเดตความรู้อยู่ตลอดเวลา เทคนิคที่ใช้ในโปรแกรมนี้ เคยปลอดภัยวันนี้ พรุ่งนี้อาจไม่ปลอดภัย เราอ่านข่าว อ่านบทความช่องโหว่งั้นเงี้เหมือนเข้าใจ ลองทำจริง ๆ จากโจทย์ CTF ช่วยยืนยันได้ว่าเข้าใจจริง ๆ
- ★ IT Security Expert ทั่วโลกนิยมเล่นกันอย่างแพร่หลาย คนเล่น CTF ส่วนมากทำงานเกี่ยวกับ IT Security เช่น นักทดสอบระบบ (Penetration Tester) เพราะจะนั่นถ้าอยากรีฝึกหรือวัดความเก่งด้าน IT Security ในระดับโลกการเล่น CTF ก็เป็นอีกตัวเลือกที่ดี เพราะมี Scoreboard ให้ดูด้วยว่าเราอยู่ตรงไหน คนอื่น ๆ เค้ายู่ตรงไหน และช่วยเพิ่มแรงจูงใจในการพัฒนาตนเอง



หมวด: แข่งขันโจทย์มันเป็นยังไง

โจทย์ใน CTF มีหลากหลาย เราอาจไม่ต้องรู้ทุกด้าน ถ้าในทีมมีหลายคน เช่น

- | | |
|----------------------------|---|
| ★ Cryptanalysis | คดครหัส 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 ที่ไม่เข้าพวก เช่นอ่าน QR โค้ดครึ่งอัน |

โจทย์ใน CTF ทุกข้อ จะต้องมีวิธีแก้ไขได้อย่างน้อย 1 วิธีแน่นอน แต่อาจแก้ได้หลายวิธี เช่น กัน ทำไปก็ได้ให้ได้ flag คนตั้งโจทย์ CTF จะต้องไม่สร้างโจทย์ที่วิธีทำไม่ Practical ในการ แก้ไข 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://mronline.com/cyberbiz/detail/9660000099861>

ໃช້ໃນคอร์ส ສອນແຊັກຮາຄາ 2 ແສນ

Authorized Training



Network Penetration Testing and Ethical Hacking -

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 enj

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

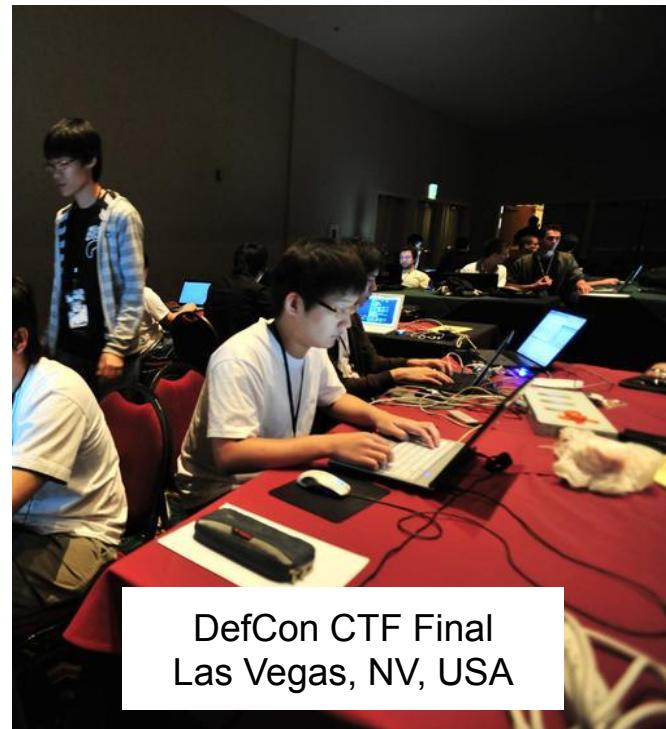
This lively session represents the culmination of the network penetration testing and ethical hacking course, where you'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop. You'll conduct an actual penetration test of a sample target environment. We'll provide the 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

For schedules, cour
or lap

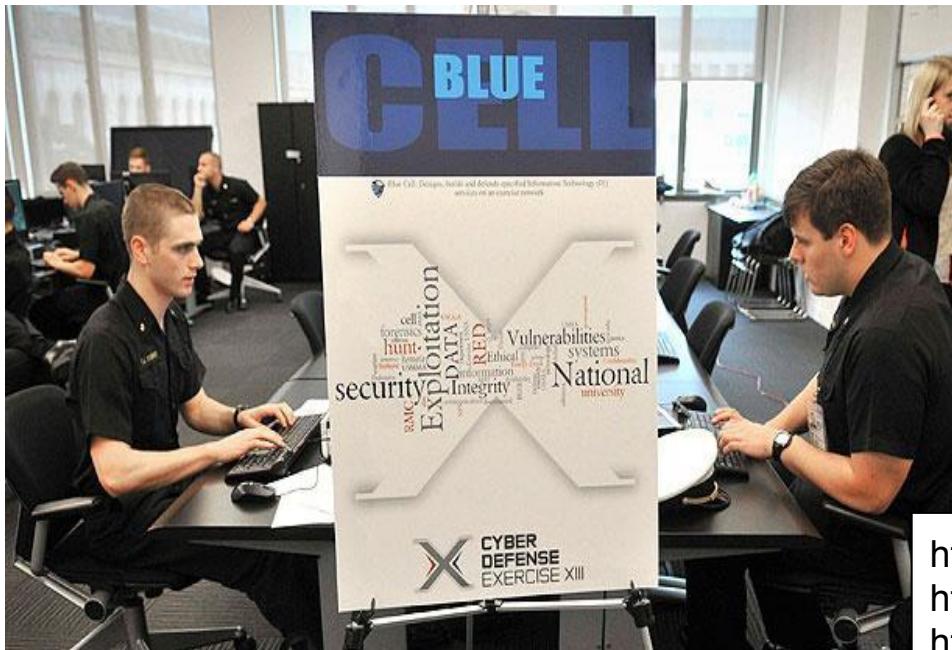
ตัวอย่าง CTF ในต่างประเทศ (1)

งานสัมมนาด้าน Hacking ที่ใหญ่ที่สุดในโลก DEFCON จัด CTF ทุกปี



ตัวอย่าง CTF ในต่างประเทศ (2)

NSA หน่วยงานความมั่นคงอเมริกาใช้การแข่งขันแบบ CTF ช่วยสอน
ทางการทหารใช้เบอร์ 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-S15/187639L-s15-coursedocs>

Wargames

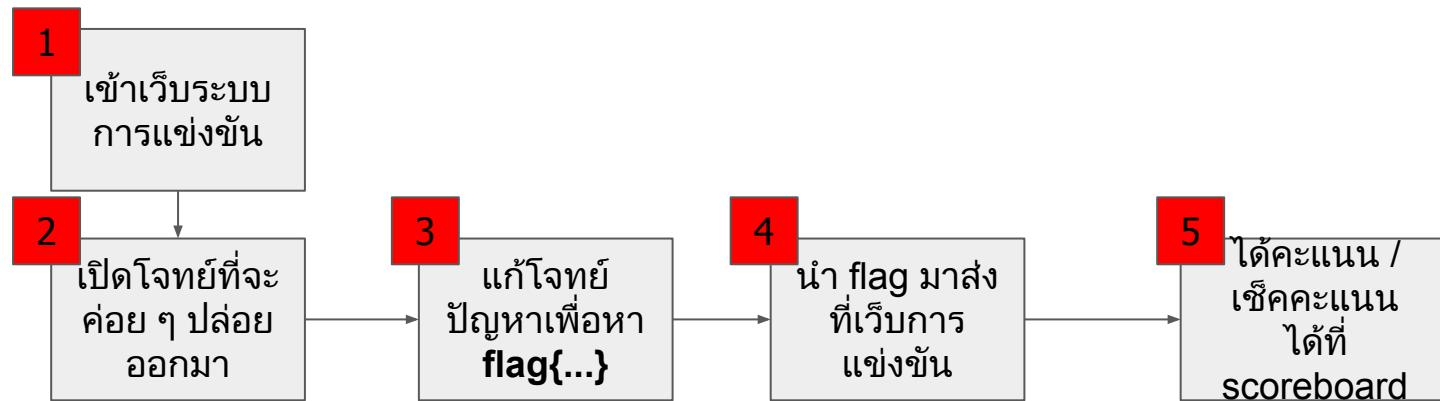
- [picoCTF](#). Grading: 3500 and up: A, 3000 - 3500: B, 2500-3000: C, 2000-2500: D, Fail below, and I will ask you to drop the class.
- [Microcorruption](#). 16 and up: A, 14-16: B, 12-14: C, 11: D, below that: F.
- [IO](#): Level 8 and up: A, Level 7: B, Level 6: C, Level 5: D, Level 4: F. If you have 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



ตัวอย่างเงื่อนไขขึ้นๆ

- ทีมที่แก้โจทย์แต่ละข้อได้เป็นทีมแรกจะได้คะแนน bonus + 10% ของข้อนั้น (first blood)
- กรรมการจัดการแข่งขันจะปล่อยคำใบ้ ถ้าไม่มีทีมใดแก้โจทย์ได้ (hint)
- โจทย์จะทยอยปล่อยออกมาระยะๆ จนครบทุกข้อ
- โจทย์จะมีข้อง่ายให้ทุกทีมร่วมสนุกกับการแข่งขันได้, ข้อยากปานกลางให้ไปศึกษาเพิ่มเติม ก่อนมาทำโจทย์ได้ และข้อยากปริubaheชีyanที่ต้องใช้ความรู้ระดับสูง

ตัวอย่างระบบส่งคำตอบ CTF และ Scoreboard

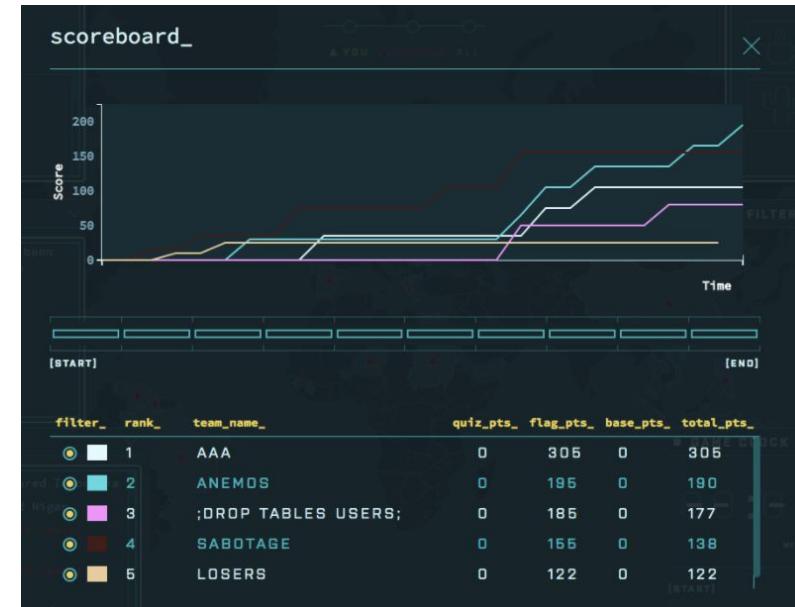
SQL Injection Castle

hack this site: <https://longcat.local>

flag{this_is_flag}

NO HINT **SUBMIT**

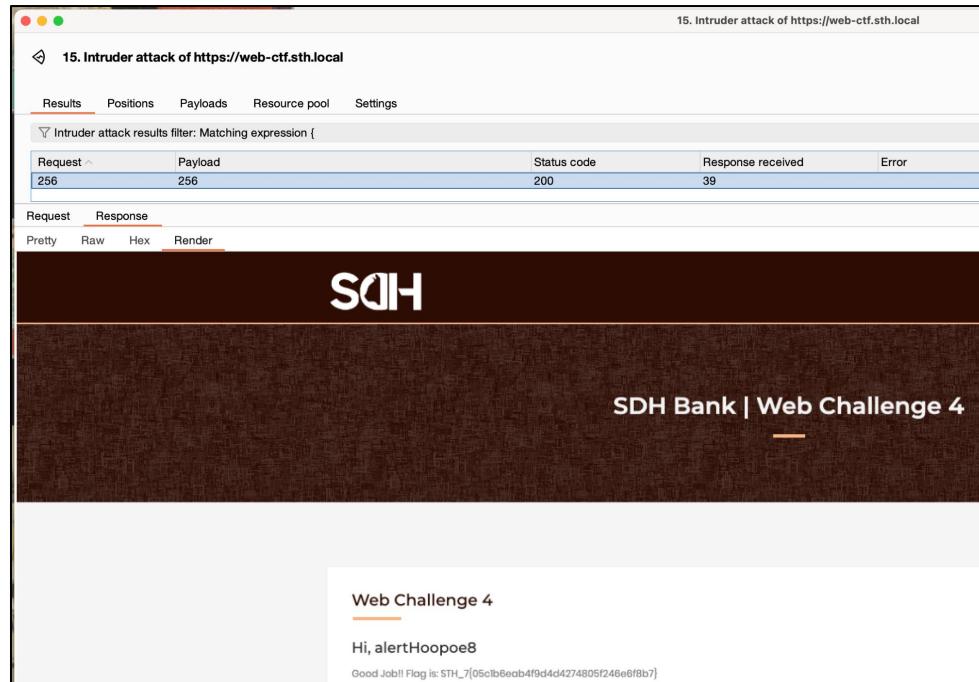
100 PTS	type quiz category Quiz first_capture Uncaptured	completed_by >
------------	---	----------------



โจทย์, คะแนน, ทีมที่ทำได้, ตอบ flag

แสดงและจัดอันดับคะแนน

ตัวอย่างการแก้ไขโจทย์ CTF และได้ Flag



The screenshot shows a browser window with the title "15. Intruder attack of https://web-ctf.sth.local". The tab bar also displays "15. Intruder attack of https://web-ctf.sth.local". The main content area has a header "15. Intruder attack of https://web-ctf.sth.local" and a sub-header "Intruder attack results filter: Matching expression {". Below this is a table with columns "Request", "Payload", "Status code", "Response received", and "Error". A single row is shown with values "256", "256", "200", "39", and an empty error field. Below the table is another header "Request Response" with tabs "Pretty", "Raw", "Hex", and "Render". The "Render" tab is selected, showing a dark brown background with the letters "SDH" in white. At the bottom of the browser window, there is a message box with the title "Web Challenge 4" and the text "Hi, alertHoopoe8". Below this, a smaller message says "Good Job!! Flag is: STH_7[05c1b8eab4f9d4cd4274805f248e8fb7]".

ช่องโหว่ IDOR

Key Takeaway (2/2)

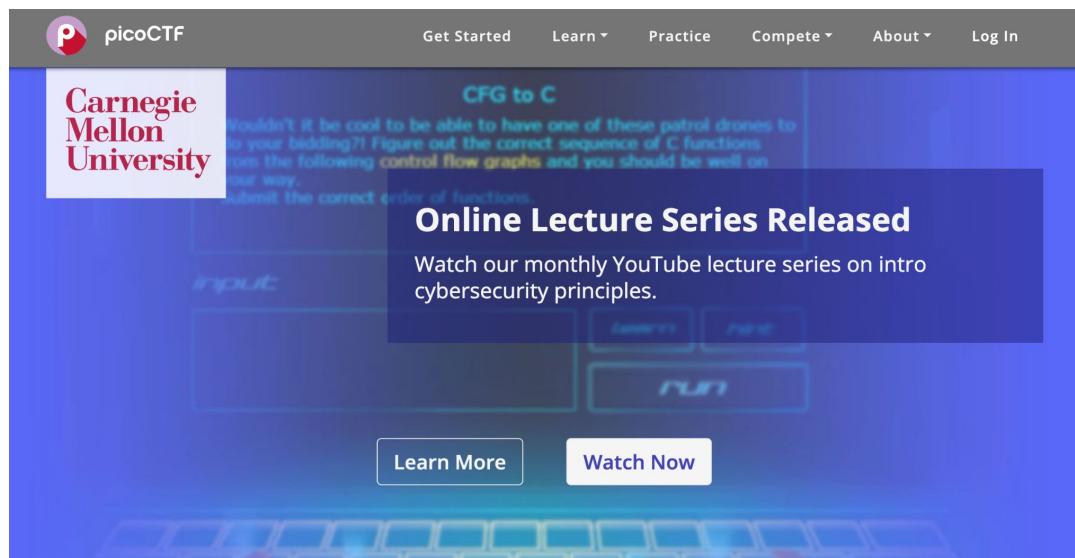
- Learning Platform เช่น TryHackMe หรือ HackTheBox ใช้เรียนรู้ได้ไม่จำกัดเวลา การแก้ไขปัญหาโจทย์ต่าง ๆ
- CTF (Capture The Flag) เป็นงานแข่งขัน มีการกำหนดเวลาแข่งชัดเจน (มีเวลาแข่งจบ) และมักจัดเป็นประจำทุกปีหรือตามรอบ ของงานสัมมนา
- ทั้ง Learning Platform และ CTF ช่วยส่งเสริมการเรียนรู้ทางด้าน Cybersecurity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

CTF Events				
All	Now running	Upcoming	Archive	Format
Name	Date	Format	Location	Restrictions
CSAW CTF Qualification Round 2024	06 Sept., 16:00 UTC — 08 Sept. 2024, 16:00 UTC	Jeopardy	On-line	2024
WMCTF2024	07 Sept., 01:00 UTC — 09 Sept. 2024, 01:00 UTC	Jeopardy	On-line	
HackTheDrone CTF Qualifier	07 Sept., 04:00 UTC — 08 Sept. 2024, 04:00 UTC	Jeopardy	On-line	
snakeCTF 2024 Quals	07 Sept., 08:00 UTC — 08 Sept. 2024, 08:00 UTC	Jeopardy	On-line	
Urmia CTF 2024	07 Sept., 12:00 UTC — 09 Sept. 2024, 12:00 UTC	Jeopardy	On-line	
DFIR Labs CTF by The DFIR Report	07 Sept., 16:00 UTC — 07 Sept. 2024, 20:00 UTC	Jeopardy	On-line	

Agenda (Day 1)

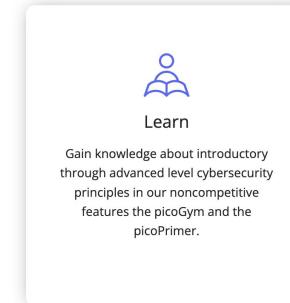
เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00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

Credit for Challenges from PicoCTF



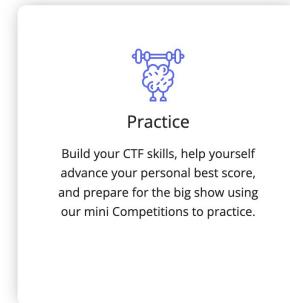
The screenshot shows the picoCTF website homepage. At the top, there's a navigation bar with links for "Get Started", "Learn", "Practice", "Compete", "About", and "Log In". A Carnegie Mellon University logo is visible on the left. The main content area features a large banner for an "Online Lecture Series Released" with a "Learn More" button and a "Watch Now" button. Below this, there's a section titled "CFG to C" with some text and a "Run" button. At the bottom, there are two buttons: "Learn More" and "Watch Now".

<https://picoctf.org>



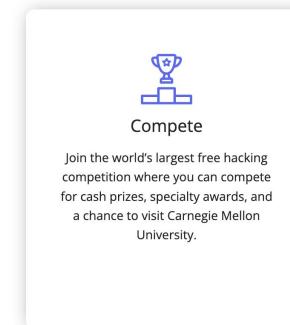
Learn

Gain knowledge about introductory through advanced level cybersecurity principles in our noncompetitive features the picoGym and the picoPrimer.



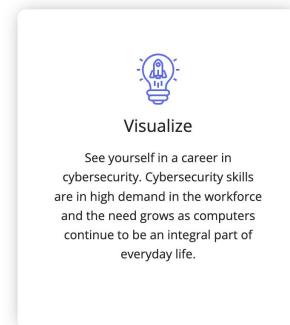
Practice

Build your CTF skills, help yourself advance your personal best score, and prepare for the big show using our mini Competitions to practice.



Compete

Join the world's largest free hacking competition where you can compete for cash prizes, specialty awards, and a chance to visit Carnegie Mellon University.



Visualize

See yourself in a career in cybersecurity. Cybersecurity skills are in high demand in the workforce and the need grows as computers continue to be an integral part of everyday life.



Thank you !!