A Development of Cybersecurity Techniques and Law Enforcements for Royal Police Cadet Academy

Pol.Capt.Chiawchan Chodhirat and Pol.Capt.Dr.Wongyos Keardsri
Royal Police Cadet Academy, Thailand
E-mal: chiawchan2014@gmail.com and wongyos@gmail.com
Facebook: facebook.com/ThomChodhirat and facebook.com/wongyos

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Contents

ROYAL POLICE CADET ACADEMY (RPCA)

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1 The ACADEMIC PROGRAM & CYBERSECURITY

Administrative Divisions of RPCA

THREE FACULTIES

Faculty of
Police Science

Faculty of
Social Science

Faculty of
Forensic Science

RPCA BACHELOR DEGREE

PUBLIC ADMINISTRATION

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

ROYAL POLICE CADET ACADEMY

POLICE CADETS

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

ROYAL POLICE CADET ACADEMY

TRAINING OFFICERS

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Law Enforcement Training

INTERNATIONAL LAW ENFORCEMENT ACADEMY

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

CYBERSECURITY COURSES IN RPCA

(1) DIGITAL TECHNOLOGY:

the 1st year cadet

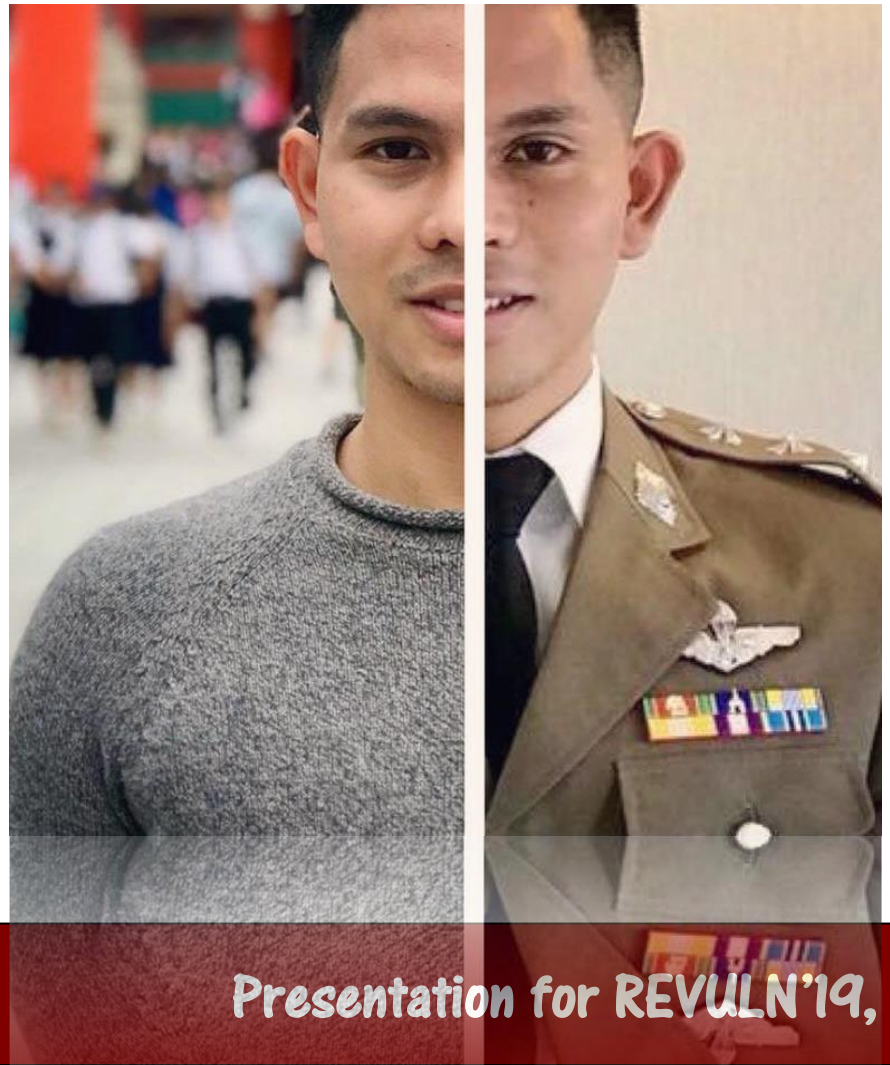
Not Enough

(2) CYBERCRIME:

the 3rd year cadet

LAW ENFORCEMENT IN CYBERSECURITY

(CYBER)CRIME PREVENTION



Harvard Kennedy School
(Cybersecurity) 2018

Boston University
(Cybercrime Investigation) 2017

Royal Police Cadet Academy
(Public Administration) 2013

Email: CHIAWCHAN2014@gamil.com

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

2 CYBERCRIME & THE ROYAL THAI POLICE

CYBERCRIME

Thailand second worst for cybercrime

Posted June 8, 2016 by Lei Lo Leave a comment

Thailand second worst for cybercrime says Allianz Global Corporate and Specialty SE (AGCS). Furthermore, Nearly 20% of Thailand's cybercrime victims reported losses of over US 100,000 in 2015. Furthermore, 4% of the country's cybercrime victims reported losses of between $1 million and $100 million last year, said Paul Davis, regional chief financial officer Asia for AGCS, the specialty insurance service arm of Germany's Allianz SE. "The local cybercrime rate has risen sharply over the past two years, resulting in a jump from fourth to second place [globally]," he said. Thailand is one of the world's top 25 targets for malware attacks, while Bangkok is a prime mark for hackers in Asia-Pacific.

THE CHALLENGES

1. Thailand ranked the 5th of the highest risk for cybersecurity threats in Asia and is the 11th in the world.

2. The local cybercrime rate has risen rapidly. The computer crime damaged many big companies from fraud external hacking to internal employee.

3. The official websites of Thai government have been hacked.

TECHNOLOGY CRIME SUPPRESION DIVISION (TCSD)

The law enforcement officers who are sufficiently trained to deal with the sudden spike in technology-based crime.

The main problem is that the Technology Crime Suppression Division does not have enough personnel to keep up with the changing nature of criminal behaviour.

THE STRATEGIC CHALLENGES

Police officers do not know how to contribute to security breaches.

Police officers do not have the sense of the cybersecurity and information security policies and procedures.

ROUTINE ACTIVITY THEORY: Cohen & Felson

CYBER-ROUTINE ACTIVITIES THEORY (C-RAT)

1. C-RAT embraces RAT as a new theoretical application for primarily explaining computer crime victimization concerning three main tenets: MOTIVATED OFFENDERS, SUITABLE TARGETS, AND ABSENCE OF CAPABLE GUARDIANS.

2. The motivated offender tenet suggests that there will always be an infinite amount of crime motivation. Most of the Cybercrime attacks have proven to be a successful monetary opportunity for cybercriminals.

CYBER-ROUTINE ACTIVITIES THEORY (C-RAT)

3 Cybercrime allows cybercriminals to withhold valuable data from users' and agencies' computers until a ransom has been paid with relative ease and anonymity. Thus, C-RAT (2008) also crosses parallels with RAT argumet in highlighting motivated offenders as a given situational factor.

4 The suitable target tenet in respect to cyberspace is also a given situational factor. RAT uses four properties (VIVA: value, inertia, visibility, and accessibility) to access the suitable target tenet, commonly.

CYBER-ROUTINE ACTIVITIES THEORY (C-RAT)

5 C-RAT also argues that any user accessing the internet is viewed as a valuable target with a perfectly high vulnerability to a cybercriminal. For exam, when the victims' data are seized from the ransomware, the victims tend to pay the ransom because they are essentially powerless in retrieving important files and data.

6 In terms of capable guardianship, there is a conspicuous lack of capable formal guardianship in cybercrime. The current formal social agents do not provide effective safeguards to protect potential victims in cyberspace since the amount of specialized forces responsible for patrolling cyberspace are limited due to the lack of resources and training.

CYBER-ROUTINE ACTIVITIES THEORY (C-RAT)

7

As a result, the police departments encountering ransomware incidents tend to pay the ransom without making any arrests. This substantially weakens the level of capable guardianship, imposing a negative image of the police departments' capability in handling the cybercrime.

8

Citizens can foster feelings of distrust and fear if the police of their town are unable to stop cybercriminal activities, let alone to criminal by paying them. Collaboration with global nations to provide international cooperation in investigation of cybercrime is extemely challenging. Therefore, the concept of Cohen and a pivotal role in keeping computer system safe from cybercrime attacks.

FUTURE DIRECTIONS ON COMPUTER CRIME

PREVENTION PROGRAM

In order to construct an effective computer crime prevention program, it is imperative to reflect on other theoretical perspectives that would convey positive effects on deterring potential computer crime. Recent criminological literature links illegal computer crime activities to social learning processes.

Skinner and Fream (1997) tested the relationship between the theoretical elements of social learning and the behaviours of cyber-criminals. The researchers (1997) posited that the nature of computer crime requires that individuals learn not only how to operate computer equipment, but also to master specific procedures, programming, and techniques for using the computer for illegal activities.

3 Cyber Security Training for Police Cadets

My Short CV

Add profile section | More...

Wongyos Keardsri

Lecturer on Cybersecurity and Digital Forensics at Faculty of Forensic Science, Royal Police Cadet Academy, Thailand

Faculty of Forensic Science, ...

IIC University of Technology

Police Captain Dr.Wongyos Keardsri or Bank (Nickname) is a Thai citizen who received 12 bachelor's degrees, 3 master's degrees and 1 doctor's degree in many areas from many universities, for example Engineering, Science, Business Administration, Economics, Informatics, Arts, Political Science, Laws and Public Health. He received M.Sc. at Department of Computer Engineering, Chulalongkorn University, Thailand and Ph.D. in Business Administration (Marketing) at IIC University of Technology, Cambodia. He works as police lecturer at Faculty of Forensic Science, Royal Police Cadet Academy, Thailand. His researchs focus on Cyber Security, Cyber Privacy, Cybercrime Investigation, Digital Forensics, Digital Technology, Social Media Monitoring, Social Media Data Analytics and Computer Programming. For more information please contact him via wongyos at gmail dot com or mobile phone +66(0)89-599-3490 (WhatsApp) or Line ID: wongyos.

The Current Crimes in Thailand

General Crimes

Cyber Crimes

Cybercrimes Tools in Thailand

Social Media

Cryptocurrency

Dark Web

Cybercrimes Targets in Thailand

Bank

Government Agency

Computer Users

Cyber Security Training

2 Main Parts and Training Teams

Red Team	Blue Team
• Coding/Programming • Reverse Engineering • Digital Forensics • Cryptography • Web Security • Exploitation	• Network Monitoring : Splunk

Under Computer Ethics

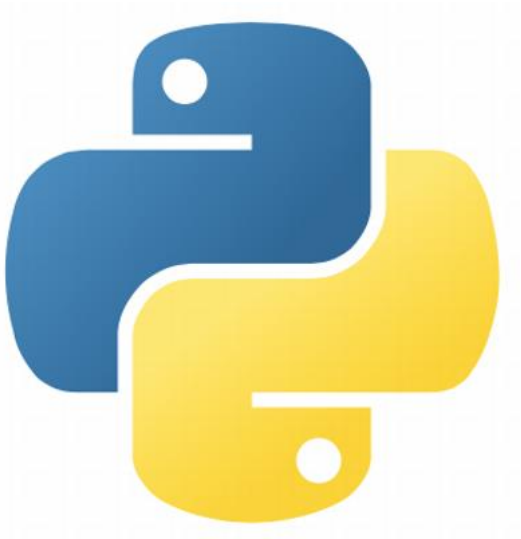
Cyber Security Training Tools

Kali Linux is main tools for this training

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

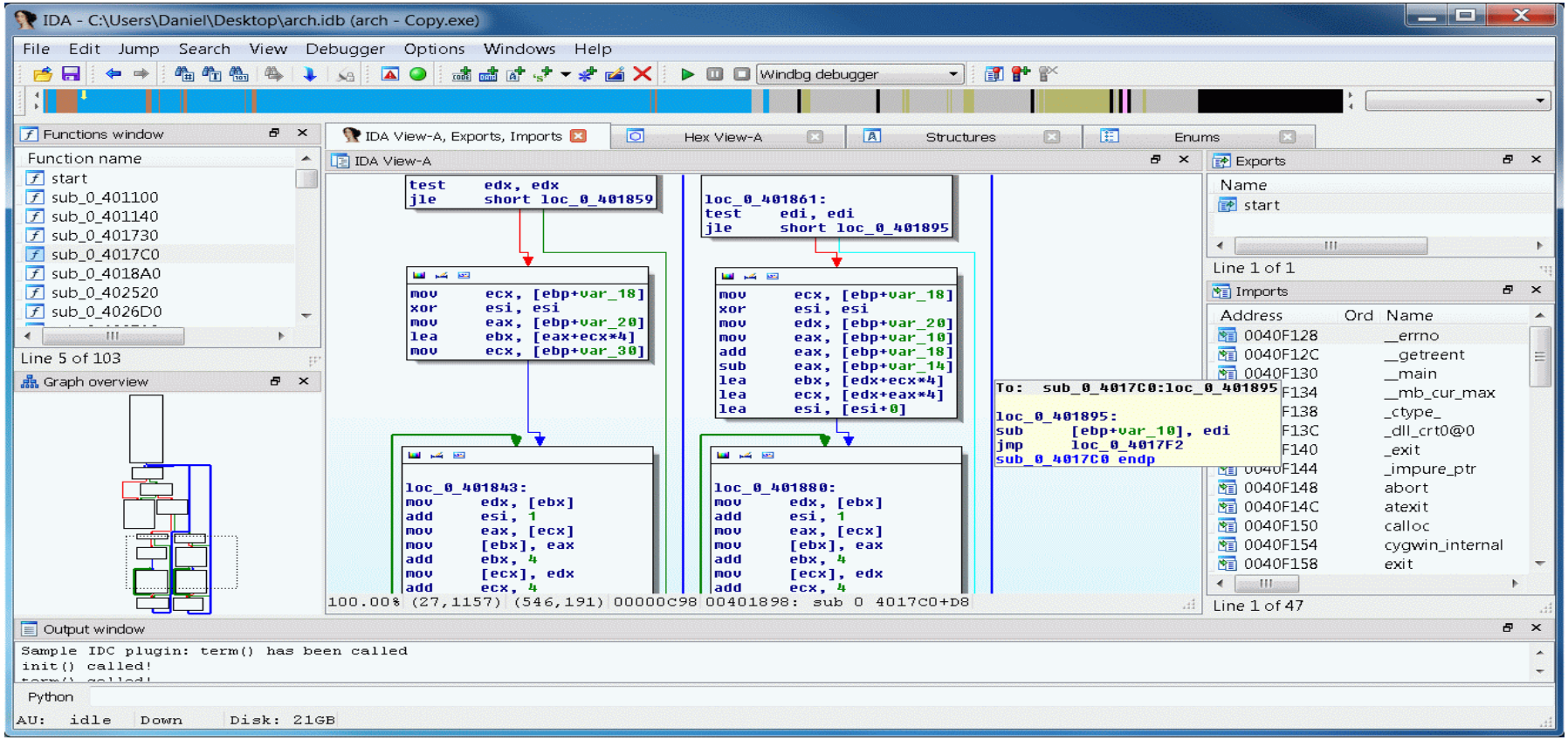
Tools for Computer Programming

Python, Java and C are the main computer languages



Tools for Reverse Engineering

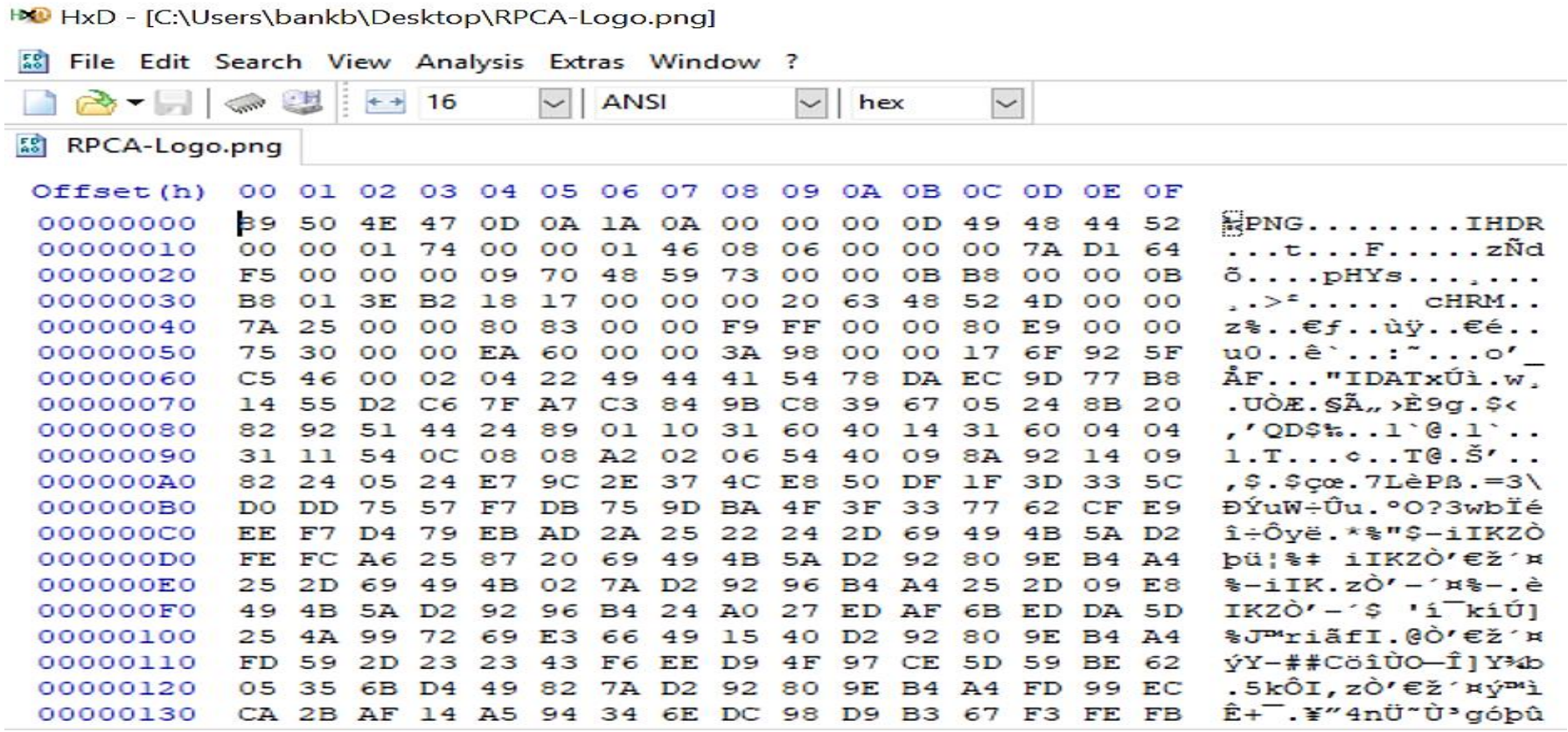
IDA to reverse the executable code to the source code



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Tools for Digital Forensics

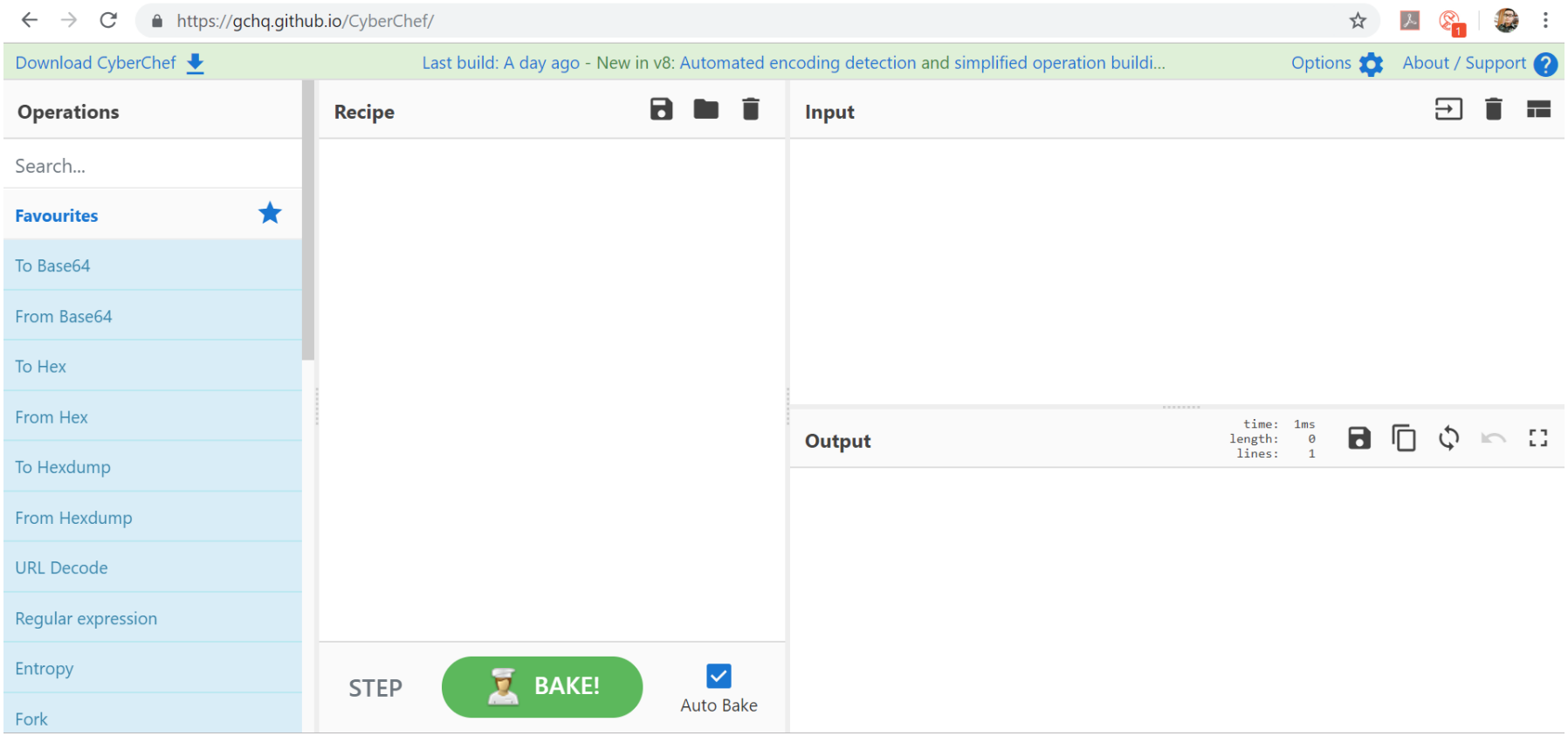
HxD for carving the images



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Tools for Cryptography

CyberChef to encrypt and decrypt the message



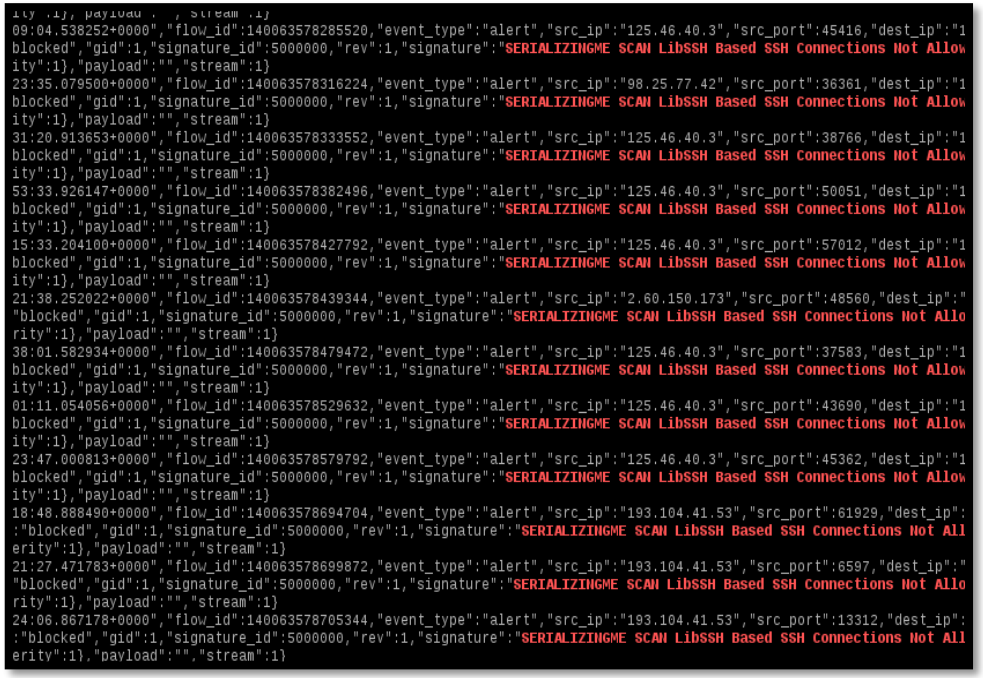
Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Tools for Web Security

SQL Injection and Brute Force to try to access website

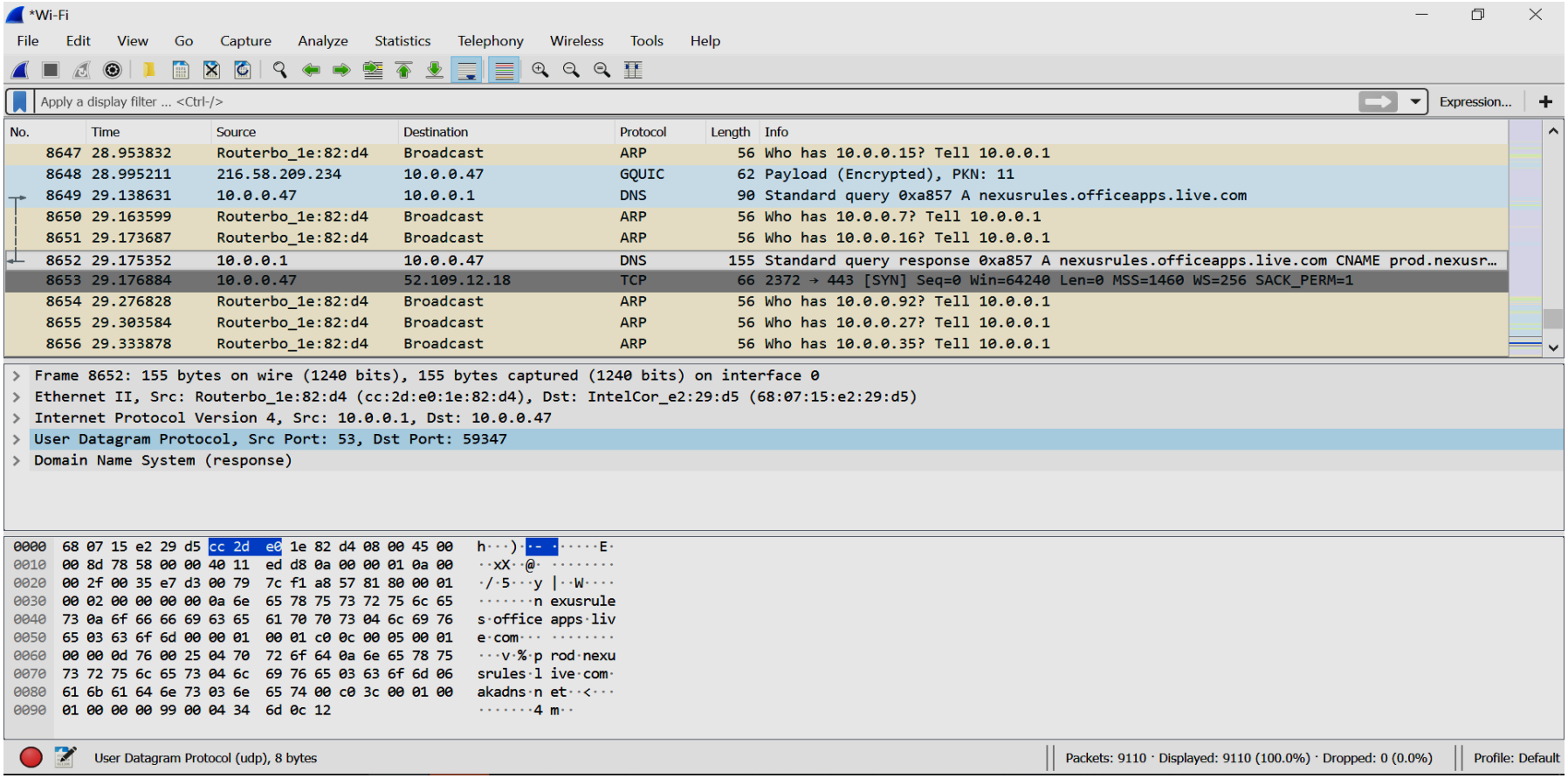
SQL Injection

Brute Force Attack



Tools for Web Security

Wireshark to capture the network traffic



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

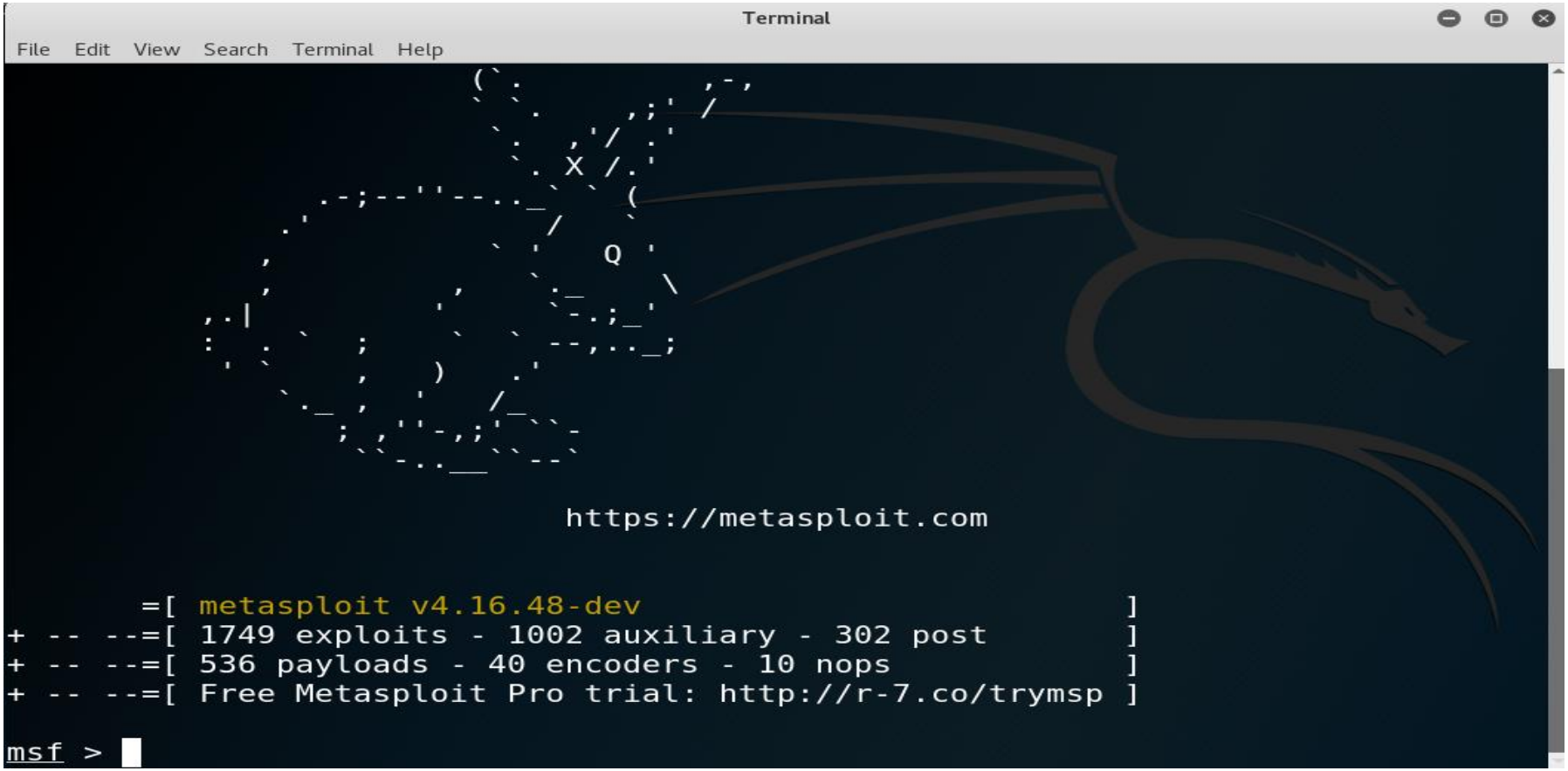
Tools for Exploitation

Nmap to search and find computer target

```
root@kali:~# nmap -sn 192.168.140.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-04 05:44 EDT
Nmap scan report for 192.168.140.1
Host is up (0.00024s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.140.2
Host is up (0.00011s latency).
MAC Address: 00:50:56:E3:F1:8C (VMware)
Nmap scan report for 192.168.140.254
Host is up (0.00040s latency).
MAC Address: 00:50:56:F0:BA:94 (VMware)
Nmap scan report for 192.168.140.131
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.32 seconds
root@kali:~#
```

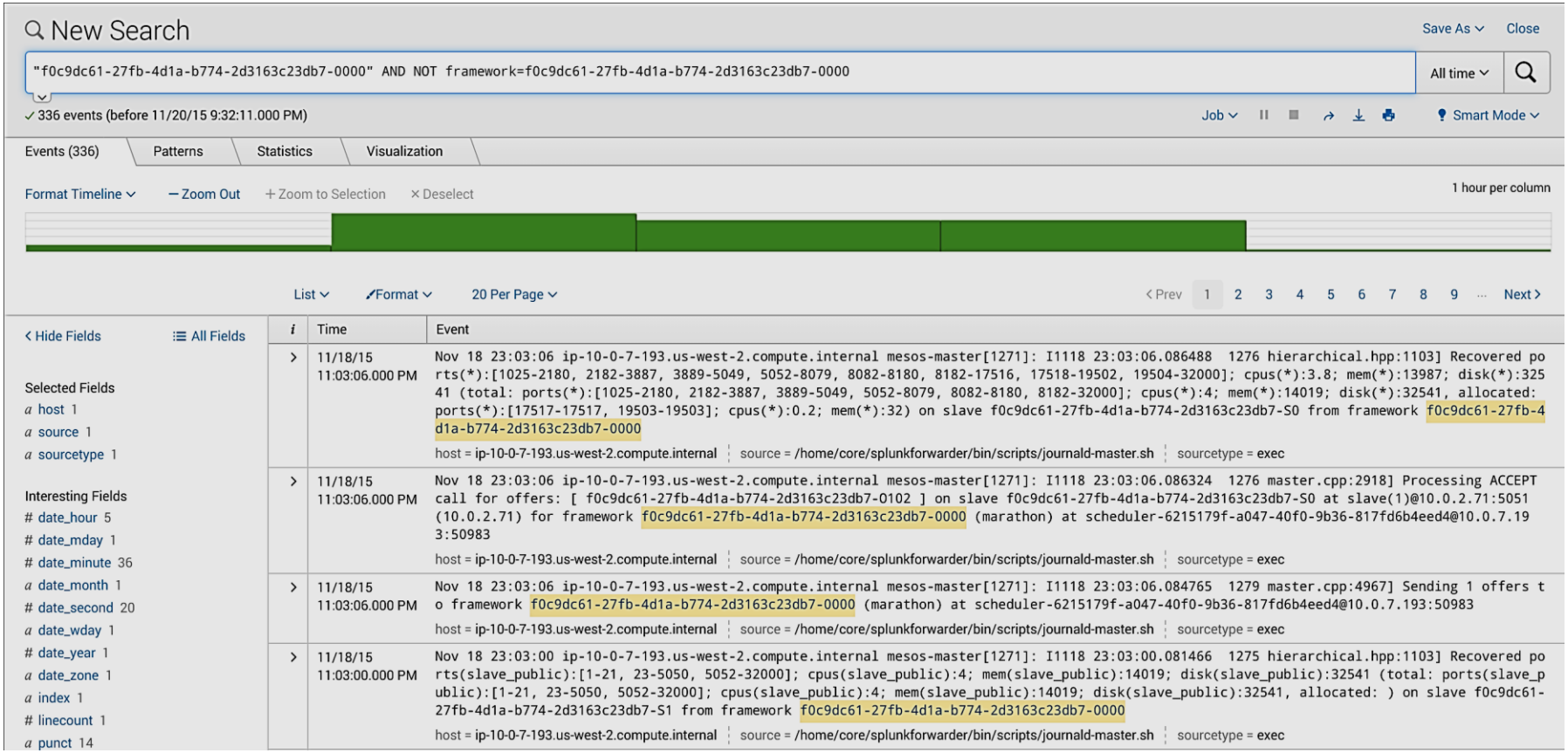
Tools for Exploitation

Metasploit to exploit computer target



Tools for Network Monitoring

Splunk to analyze the computer logs



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Exercise

4 RPCA Cyber Teams and Challenges

RPCA Cyber Teams 2018

FirstHUNTER

SecondHUNTER

ThirdHUNTER

New Blood Cyber Police Officers


ผู้เข้าร่วมแข่งขัน Cyber War ทหาร-ตำรวจ

ตัวแทน รร.นรต. ทีมที่ ๑

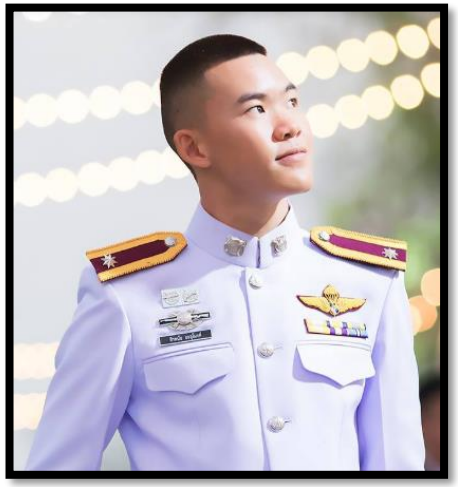
นรต.ณัฐชนน ภูสมตา ชั้นปีที่ ๔

นรต.ภัทราวุธ ดำราษฎร์ ชั้นปีที่ ๔

นรต.สิรดนัย ยะอุโมงค์ ชั้นปีที่ ๔

นรต.อนุสรณ์ ปินใจ ชั้นปีที่ ๔

FirstHUNTER



RPCA Cyber Teams 2019

SecondHUNTER

ThirdHUNTER

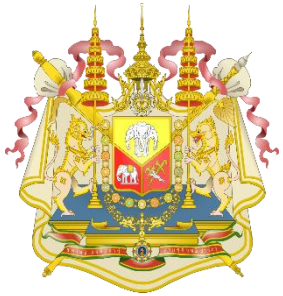
FourthHUNTER

1st Cyber Security Competition for Military and Police Academy

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

Organized by Royal Thai Armed Forces



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

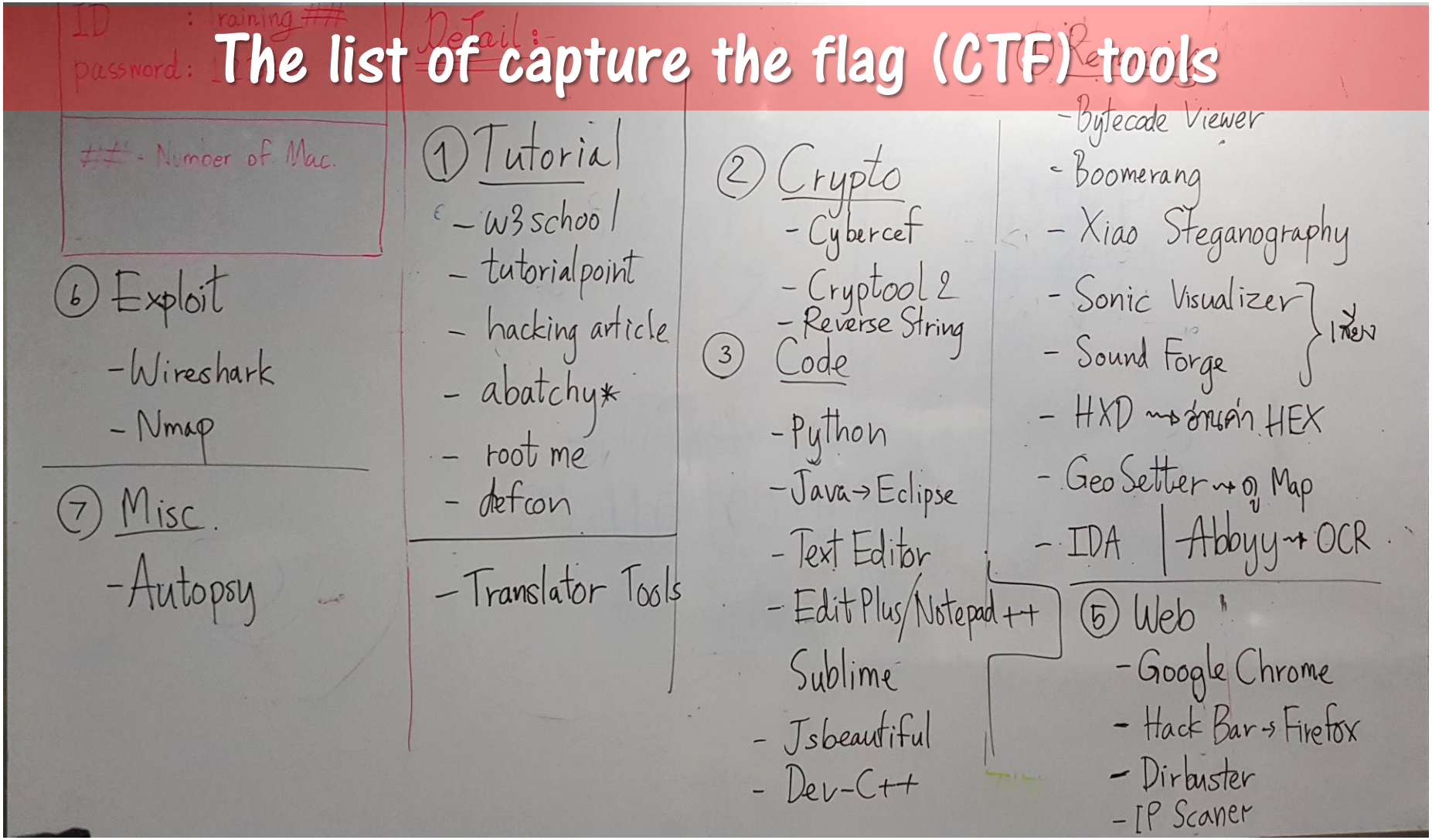
Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

The training at Digital Forensic Center (DFC)

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

The competition day, have the relax and lucky

1st Cyber Security Competition for Military and Police Academy

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

Rank	Team	Institutes	Score
1	Hungus	Navaminda Kasatriyadhiraj Royal Thai Air Force Academy	4,480
2	SecondHUNTER	Royal Police Cadet Academy	3,368
3	FirstHUNTER	Royal Police Cadet Academy	3,288
4	Pwnyou	Navaminda Kasatriyadhiraj Royal Thai Air Force Academy	2,918
5	V1p3rRGB	Chulachomklao Royal Military Academy	2,862
6	K0chr04CH	Royal Thai Naval Academy	2,812
7	ThirdHUNTER	Royal Police Cadet Academy	2,760
8	HaCkMeifYoUc@N	Chulachomklao Royal Military Academy	2,716
9	Complex Webster	Navaminda Kasatriyadhiraj Royal Thai Air Force Academy	2,702
10	GetHeinzflyFlag	Chulachomklao Royal Military Academy	2,650
11	ThePaladin.AFAPS2	Armed Forces Academies Preparatory School	2,326
12	p4yl04d	Royal Thai Naval Academy	1,650
13	ThePaladin.AFAPS1	Armed Forces Academies Preparatory School	1,578
14	ThePaladin.AFAPS3	Armed Forces Academies Preparatory School	1,272

1st Cyber Security Competition for Military and Police Academy

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

The second runner up for FirstHUNTER

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

1st Cyber Security Competition for Military and Police Academy

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

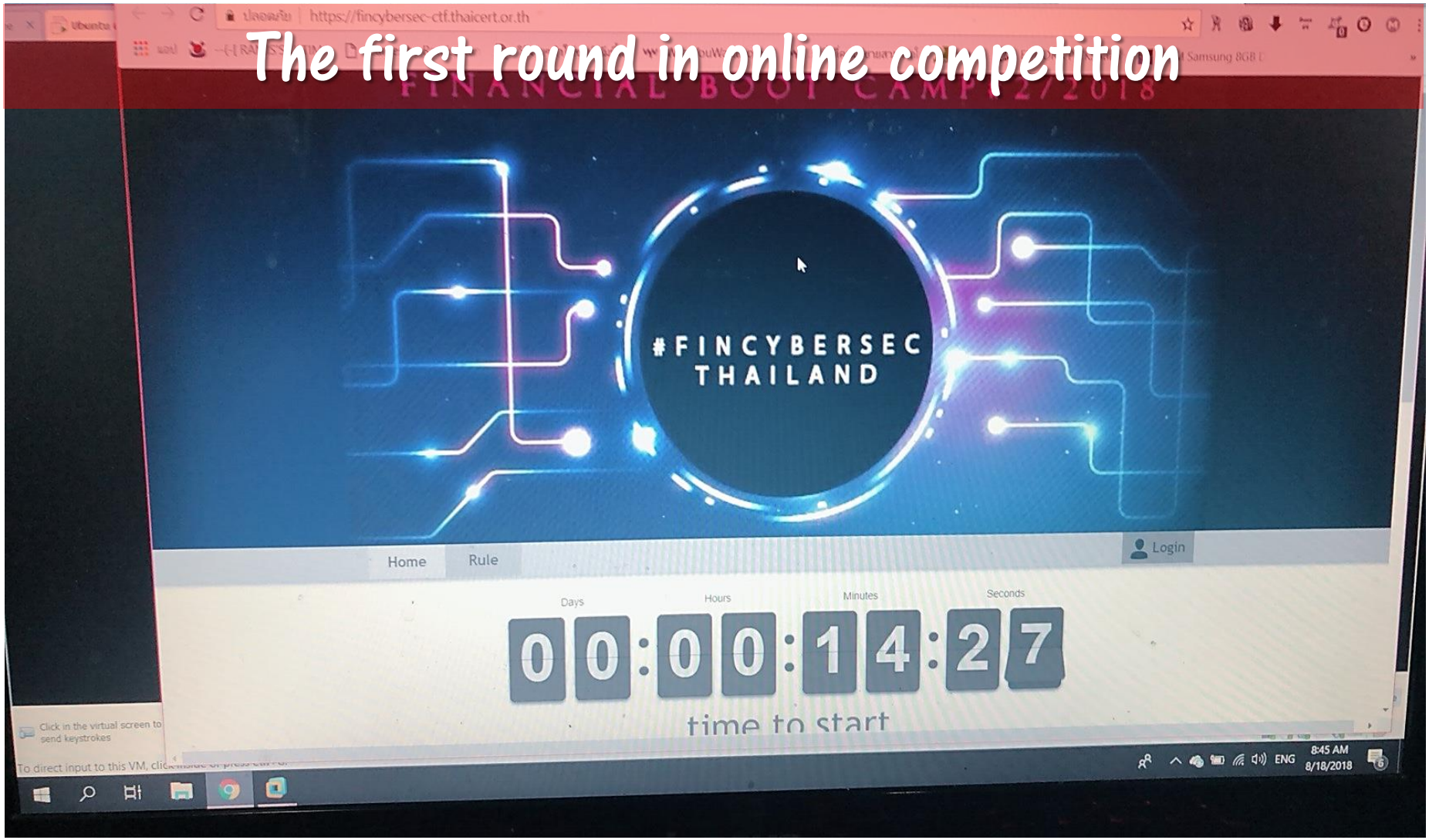
Financial Cyber Security Boot Camp 2018

Financial Cyber Security Boot Camp 2018

Organized by the Bank of Thailand (BOT)

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

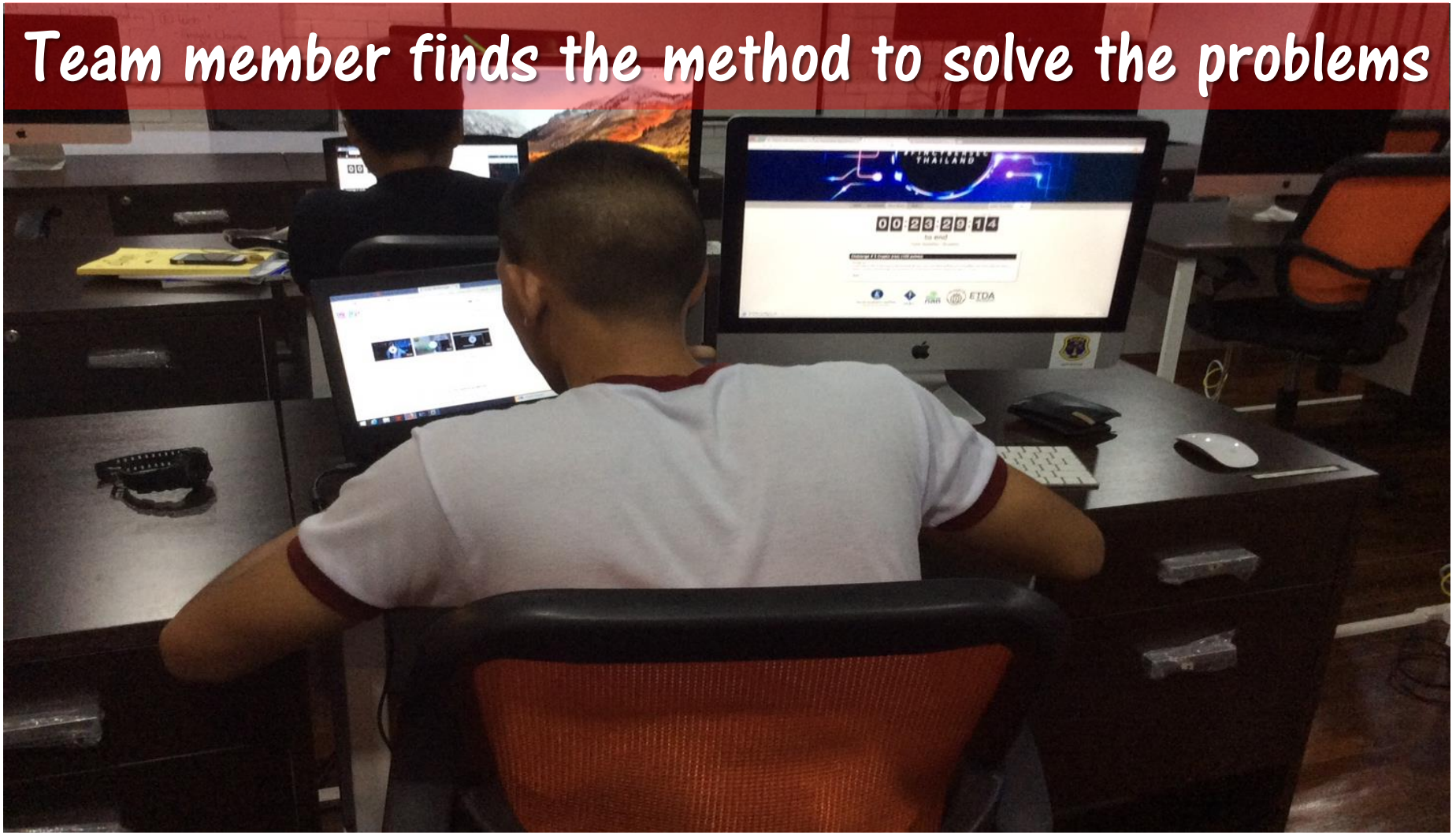
Financial Cyber Security Boot Camp 2018



The first round in online competition

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Financial Cyber Security Boot Camp 2018



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Financial Cyber Security Boot Camp 2018

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Financial Cyber Security Boot Camp 2018

Position	Team Name	Points
1	CPCUCTF	3060.00
2	test	1115.00
3	OLAN	950.00
4	Hamburger	925.00
5	Cyber Guardian	905.00
6	1amN00b	900.00
7	APCR	900.00
8	Maiden	710.00
9	FTTS	700.00
10	MUTAE	500.00
11	cnior	450.00
12	!IsCaptured	400.00

Two of RPCA cyber team go to the final round

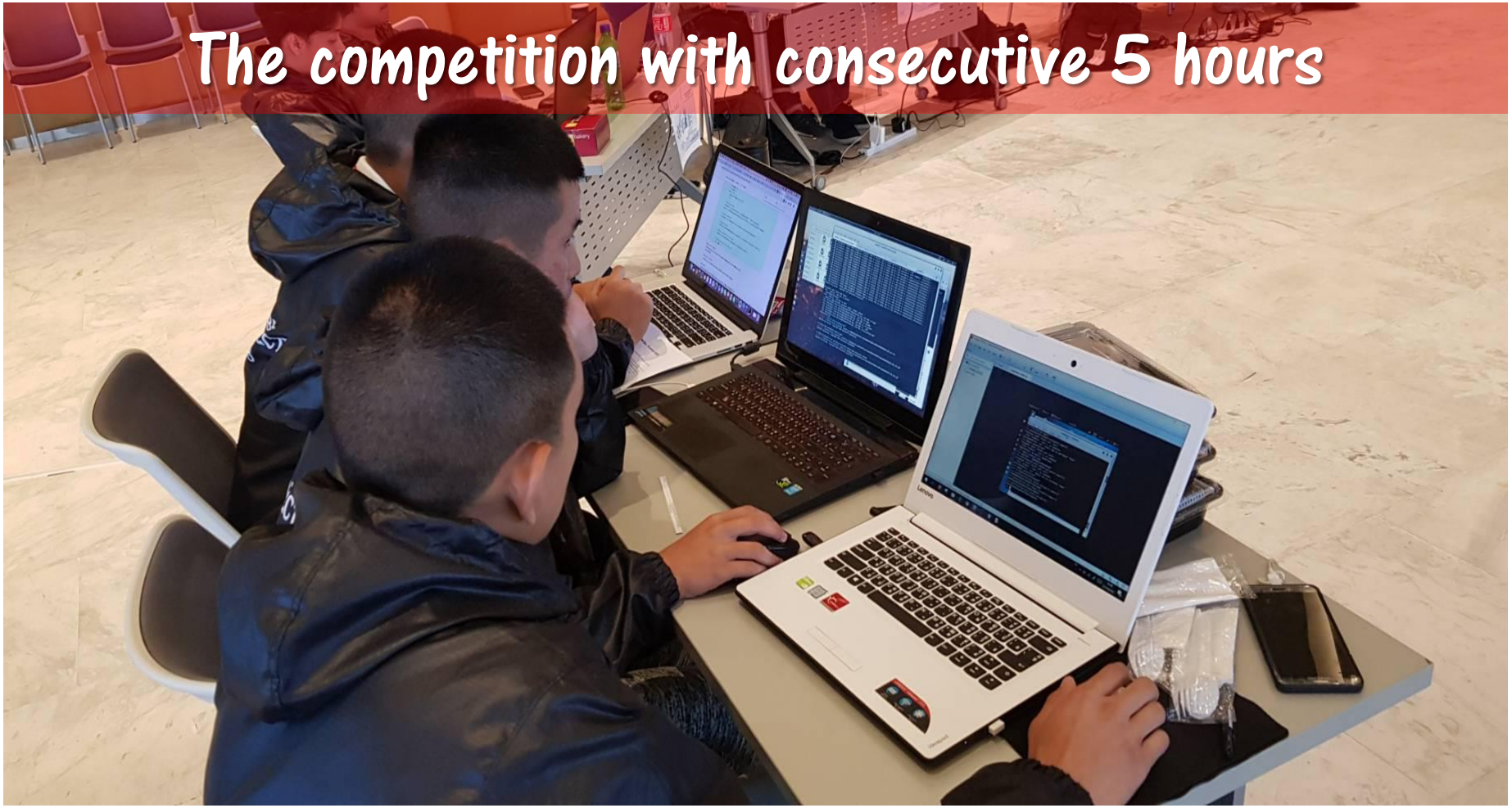
:0{ :|:& };:	Hamburger
!IsCaptured	Maiden
1amN00b	MUTAE
AA K	OLAN
cnior	Omega3
CPCUCTF	Talardlang
Cyber Guardian	test
FTTS	

Financial Cyber Security Boot Camp 2018

The final round at the learning center of BOT

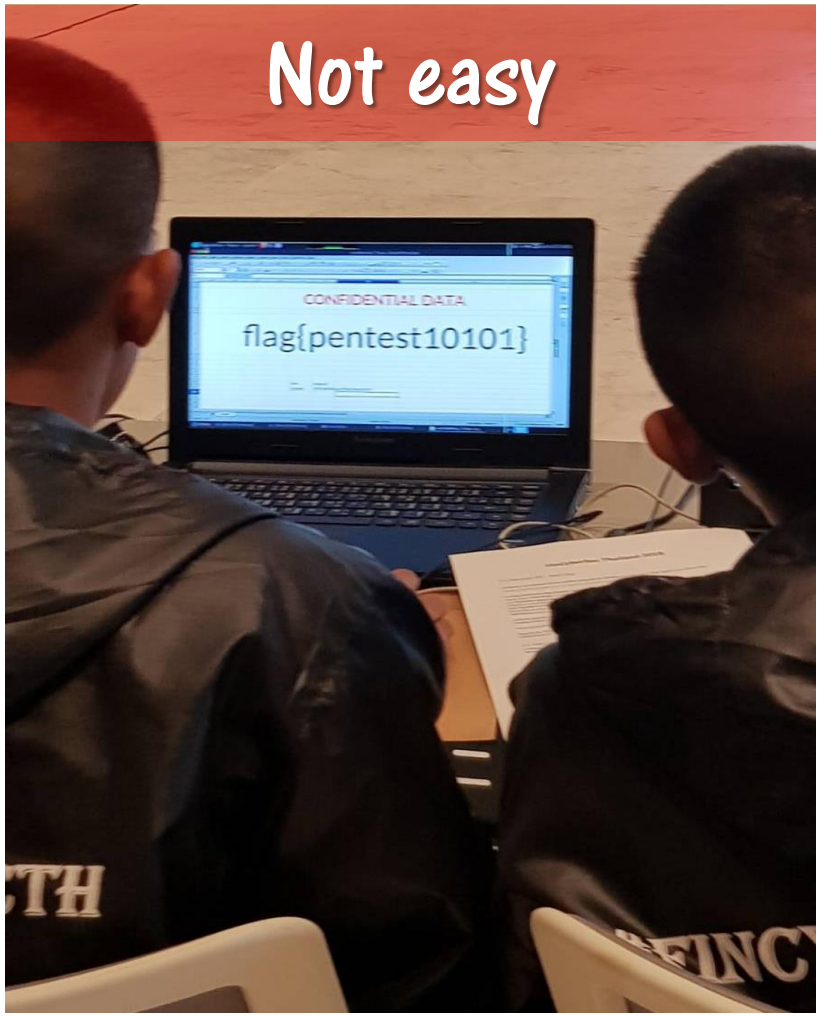
Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Financial Cyber Security Boot Camp 2018



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Financial Cyber Security Boot Camp 2018



Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Financial Cyber Security Boot Camp 2018

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

KPMG Cyber Security Challenge 2018 in Thailand

KPMG Cyber Security Challenge 2018

KPMG Cyber Security Challenge 2018

Test your cyber security skills in this latest Capture The Flag challenge brought to you by KPMG in Thailand.

Organized by KPMG Thailand company

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

KPMG Cyber Security Challenge 2018

Cyber team from leading universities in Thailand

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

KPMG Cyber Security Challenge 2018

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

KPMG Cyber Security Challenge 2018

No.	Team	Score
1	KPMG{CPCUCTF_is_back!}	625
2	K0i$uruFortunePr0xy	550
3	squareRoot-1_2^3_sigma_pi	450
4	AA_K	450
5	Jeff	400
6	KU1	400
7	The_BMTH	325
8	Lookchin	325
9	DoubleJelly	325
10	Talardlang	250
11	DDU-DU_DDU-DU	250

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

KPMG Cyber Security Challenge 2018

12	DeadlineIsComing	175
13	Cyber_Script	175
14	KU2	175
15	Cyber_Guardian	175
16	Pid_pid_pewww	175
17	Hamburger	100
18	TryHard	100
19	Theshadow	100
20	newmiracle	100
21	RookieCyber	100
22	ISAG48	100

KPMG Cyber Security Challenge 2018

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Thailand Cyber Security Competition for Military and Police Institutes

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Thailand Cyber Security Competition for Military and Police Institutes

This competition for military and police officer

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Thailand Cyber Security Competition for Military and Police Institutes

Organized by RTARF and IXIA

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Thailand Cyber Security Competition for Military and Police Institutes

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Thailand Cyber Security Competition for Military and Police Institutes

Test.py - D:\Cyber Game\CTF-2018-08-29\Test.py (3.6.5)

File Edit Format Run Options Window Help

```
import codecs
import hashlib
infile = open('data.txt')
for line in infile:
    string = line.strip()
    for i in range(1000):
        string = codecs.encode(string, 'rot_13')
        string = hashlib.md5(string.encode('utf-8')).hexdigest()
    print(string)
```

```
8ced3bf8ae013be3f2eed72e04c5e721
74128fbac2201121f5f2443089ac2a4c
5bcedf3c97b1020cdd4de24f39772b84
c64c8c037fe80214542df3809cedd971
181df0d795e5560fcc146b289199d319
14105f8d44266446457d0e605c993b4a
d12f200f764b4e179ed3c34c79db23b9
2297d27ee8f11286f48412368f752c44
b96a190fcbc75331701fffe29f711fc2
```

```
48e97c43b470117d42c876f3206011b1
deee38ef79054990c08df14f5b7b6499
1a2e2b7f0331920640e4c7c9b83ca823
bcd6c493029480225ec5b2f1e4a4b7a4
4d0656a1e8c0dad5c00ceef3f37485dc
25cdaeda34193d92e09557c7955d7568
0817871bf19ef2e9240551de596d1ca2
9fc28db29586b5220e95d1d088dda537
240258d317020bb416f8da3e1f38e76b
```

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

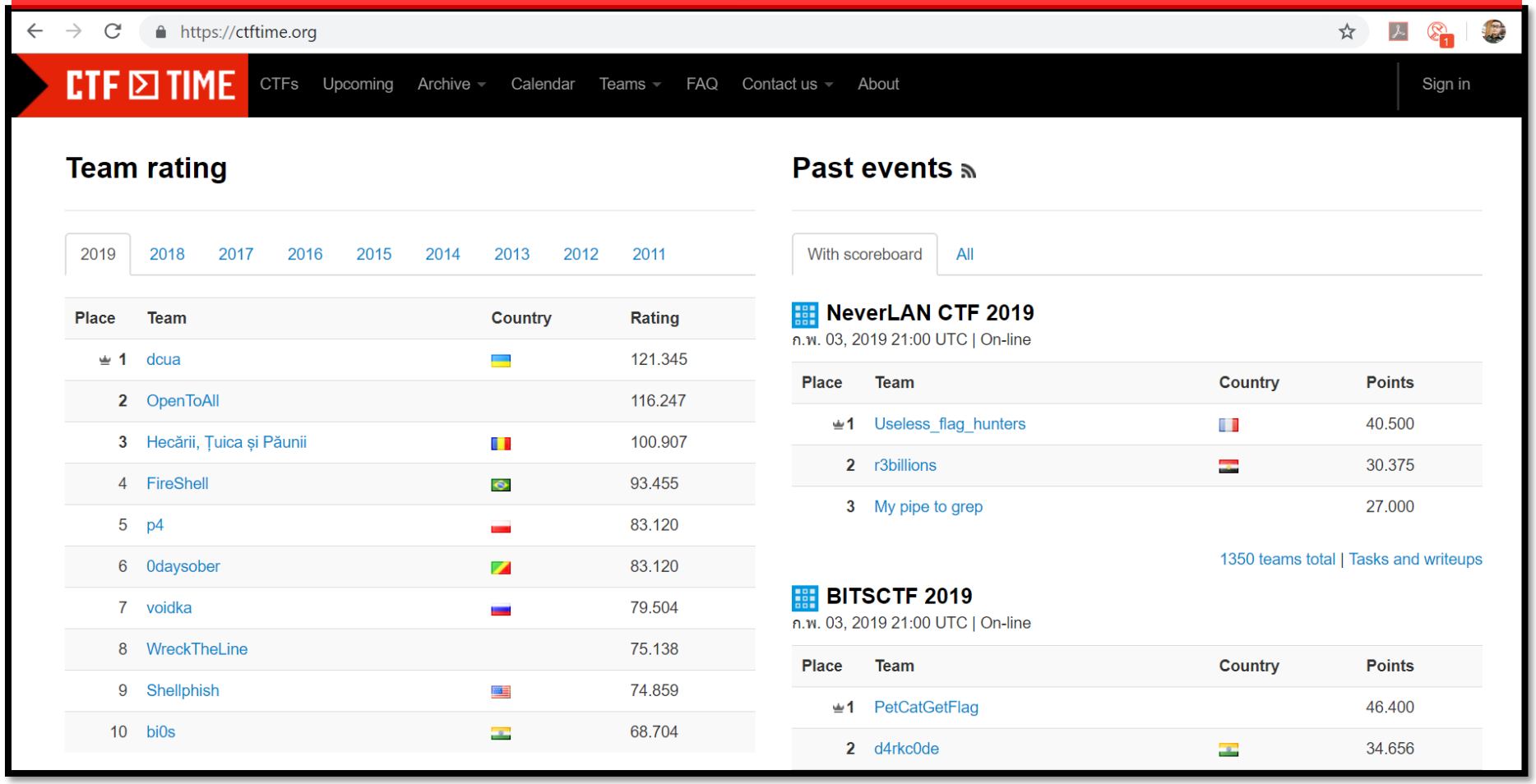
Thailand Cyber Security Competition for Military and Police Institutes

Rank	Team	Institutes	Score
1	NO0P	Ministry of Defence	880
2	Cyber Guardian	Royal Thai Police	820
3	WTF	Royal Thai Armed Forces	740
4	H3x	Royal Thai Armed Forces	740
5	Cyber Ninja	Royal Thai Navy	520
6	0x90	Ministry of Defence	400
7	10 Secs	Royal Thai Navy	390
8	RTAF Cyber Op 1	Royal Thai Air Force	340
9	RTAF Cyber Op 2	Royal Thai Air Force	320
10	B@ckPipe	Royal Thai Army	310
11	Grep * (Grep Star)	Royal Thai Army	300
12	DTI Cyber Team	Defence Technology Institute	210

Online Cyber Security Competition

Online Cyber Challenges

CTF Time at https://ctftime.org/



https://ctftime.org

CTF TIME | CTFs | Upcoming | Archive | Calendar | Teams | FAQ | Contact us | About | Sign in

Team rating

2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	dcua		121.345
2	OpenToAll		116.247
3	Hecării, Țuica și Păunii		100.907
4	FireShell		93.455
5	p4		83.120
6	0daysober		83.120
7	voidka		79.504
8	WreckTheLine		75.138
9	Shellphish		74.859
10	bi0s		68.704

Past events

With scoreboard | All

NeverLAN CTF 2019
ก.พ. 03, 2019 21:00 UTC | On-line

Place	Team	Country	Points
1	Useless_flag_hunters		40.500
2	r3billions		30.375
3	My pipe to grep		27.000

1350 teams total | Tasks and writeups

BITSCTF 2019
ก.พ. 03, 2019 21:00 UTC | On-line

Place	Team	Country	Points
1	PetCatGetFlag		46.400
2	d4rkc0de		34.656

Presentation for REVULN'19, May 15-16, 2019, Hong Kong

Conclusions

1. Briefs for the police cadet program in Royal Police Cadet Academy
2. Explain for the cyber law enforcement courses in Royal Police Cadet Academy
3. Descript the cyber security training for Thailand's police cadets

Conclusions

4

Show the RPCA cyber security teams and the results in the competitions

End of Presentation

Thank You