



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

1

The Academic Program and Cybersecurity

2

Cybercrime and Police Cadets

3

Cyber Security Training for Police Cadets

4

RPCA Cyber Teams and Challenges

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



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

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

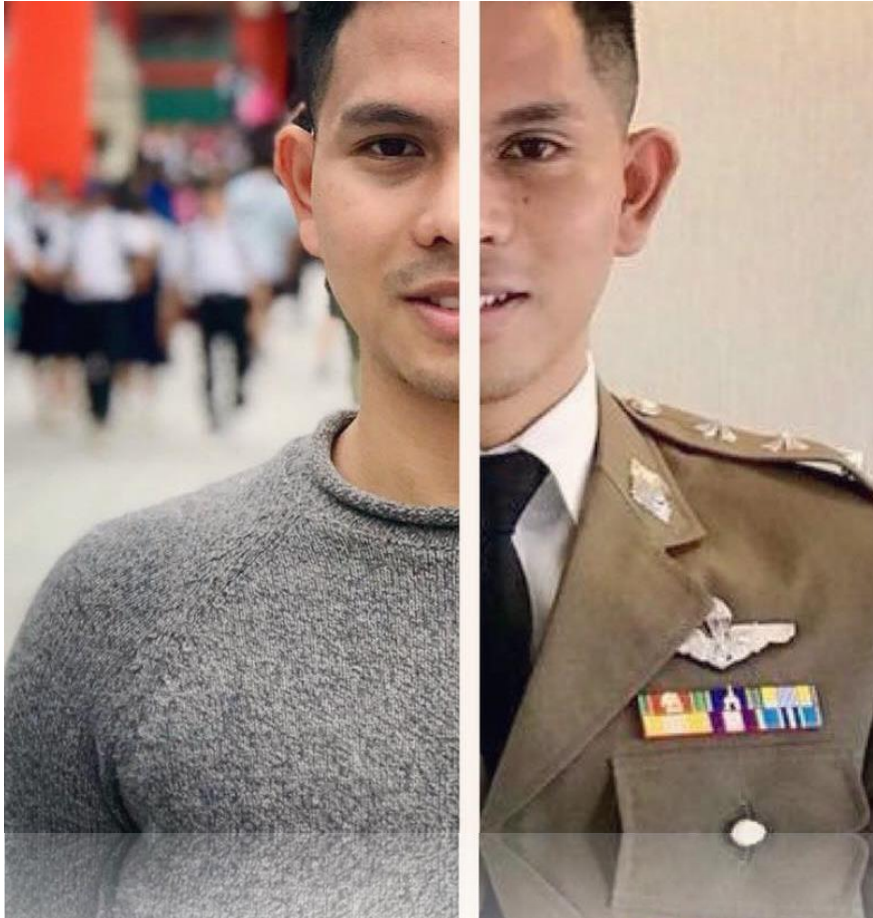
A red starburst graphic with multiple points, containing the text "Not Enough" in white.

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

CYBER**CRIME** & 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 SUPPRESSION 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



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

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 argument 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 extremely 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.

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

The Current Crimes in Thailand

General Crimes



Cyber Crimes



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

Cybercrimes Tools in Thailand

Social Media



Cryptocurrency



Dark Web



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

Cybercrimes Targets in Thailand

Bank



Government Agency



Computer Users



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

Cyber Security Training

2 Main Parts and Training Teams

Red Team

- Coding/Programming
- Reverse Engineering
- Digital Forensics
- Cryptography
- Web Security
- Exploitation

Blue Team

- Network Monitoring :
Splunk



Under Computer
Ethics

Cyber Security Training Tools

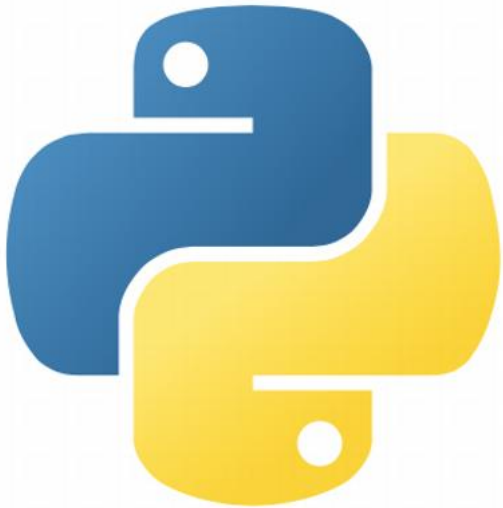


Kali Linux is main tools for this training

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

Tools for Computer Programming

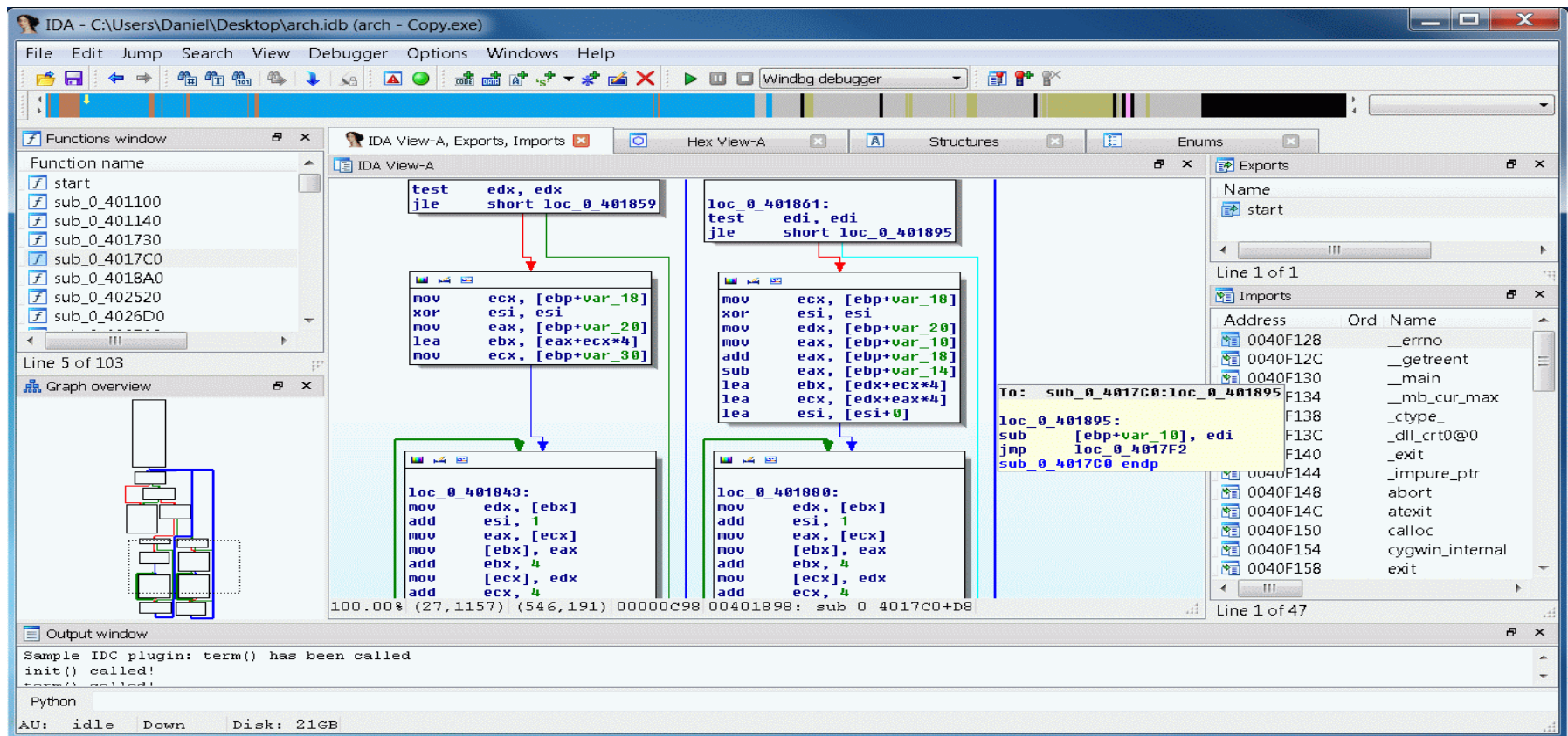
Python, Java and C are the main computer languages



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

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

HxD - [C:\Users\bankb\Desktop\RPCA-Logo.png]

File Edit Search View Analysis Extras Window ?

16 ANSI hex

RPCA-Logo.png

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	B9	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	PNG.....IHDR
00000010	00	00	01	74	00	00	01	46	08	06	00	00	00	7A	D1	64	...t...F.....zNd
00000020	F5	00	00	00	09	70	48	59	73	00	00	0B	B8	00	00	0B	õ....pHYs.....
00000030	B8	01	3E	B2	18	17	00	00	00	20	63	48	52	4D	00	00	..>^..... cHRM..
00000040	7A	25	00	00	80	83	00	00	F9	FF	00	00	80	E9	00	00	z%...€f...ùÿ...€é..
00000050	75	30	00	00	EA	60	00	00	3A	98	00	00	17	6F	92	5F	u0...ê`...:~...o'..
00000060	C5	46	00	02	04	22	49	44	41	54	78	DA	EC	9D	77	B8	ÅF... "IDATxÜi.w.
00000070	14	55	D2	C6	7F	A7	C3	84	9B	C8	39	67	05	24	8B	20	.U0Æ.\$Ã,,>È9g.\$<
00000080	82	92	51	44	24	89	01	10	31	60	40	14	31	60	04	04	, 'QDS%...l`@.l`..
00000090	31	11	54	0C	08	08	A2	02	06	54	40	09	8A	92	14	09	l.T....c...T@.Š'..
000000A0	82	24	05	24	E7	9C	2E	37	4C	E8	50	DF	1F	3D	33	5C	,\$. \$çæ.7LèPB.=3\
000000B0	D0	DD	75	57	F7	DB	75	9D	BA	4F	3F	33	77	62	CF	E9	ĐÝuW÷Ûu.°O?3wbİé
000000C0	EE	F7	D4	79	EB	AD	2A	25	22	24	2D	69	49	4B	5A	D2	î÷Ôÿë.*\$"\$-iIKZÒ
000000D0	FE	FC	A6	25	87	20	69	49	4B	5A	D2	92	80	9E	B4	A4	pü!;\$# iIKZÒ'€ž'¤
000000E0	25	2D	69	49	4B	02	7A	D2	92	96	B4	A4	25	2D	09	E8	%-iIK.zÒ'- '¤%-è
000000F0	49	4B	5A	D2	92	96	B4	24	A0	27	ED	AF	6B	ED	DA	5D	IKZÒ'- ' \$ 'i_kiÚ]
00000100	25	4A	99	72	69	E3	66	49	15	40	D2	92	80	9E	B4	A4	%Jªriãfi. @Ò'€ž'¤
00000110	FD	59	2D	23	23	43	F6	EE	D9	4F	97	CE	5D	59	BE	62	ýY-##CöiÛO-Î]Yªb
00000120	05	35	6B	D4	49	82	7A	D2	92	80	9E	B4	A4	FD	99	EC	.5kÔI,zÒ'€ž'¤ýªi
00000130	CA	2B	AF	14	A5	94	34	6E	DC	98	D9	B3	67	F3	FE	FB	Ê+~.¥"4nÜ~Ûªgópû

Tools for Cryptography

CyberChef to encrypt and decrypt the message

← → ↻ <https://gchq.github.io/CyberChef/> ☆    ⋮

Download CyberChef  Last build: A day ago - New in v8: Automated encoding detection and simplified operation buildi... Options  About / Support 

Operations	Recipe	Input
Search...		
Favourites ★		
To Base64		
From Base64		
To Hex		
From Hex		
To Hexdump		
From Hexdump		
URL Decode		
Regular expression		
Entropy		
Fork		

Output time: 1ms
length: 0
lines: 1     

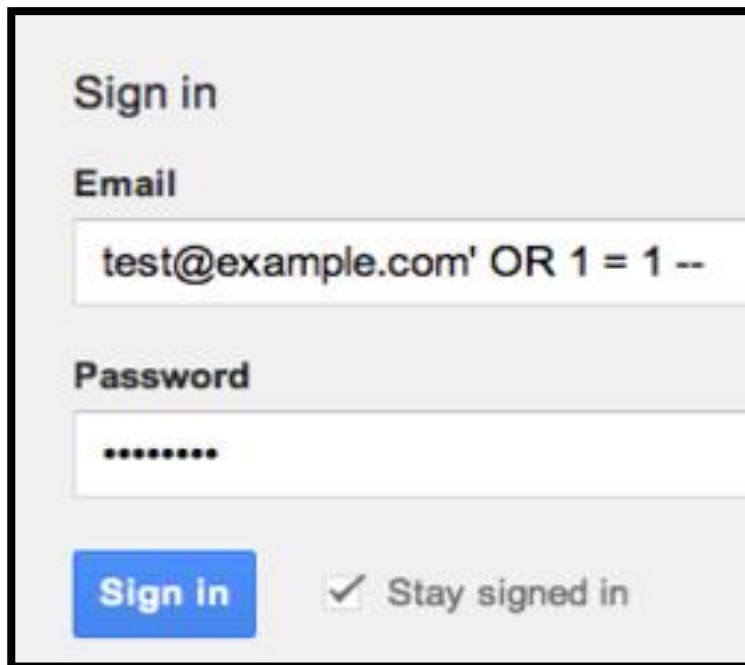
STEP  **BAKE!**  Auto Bake

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

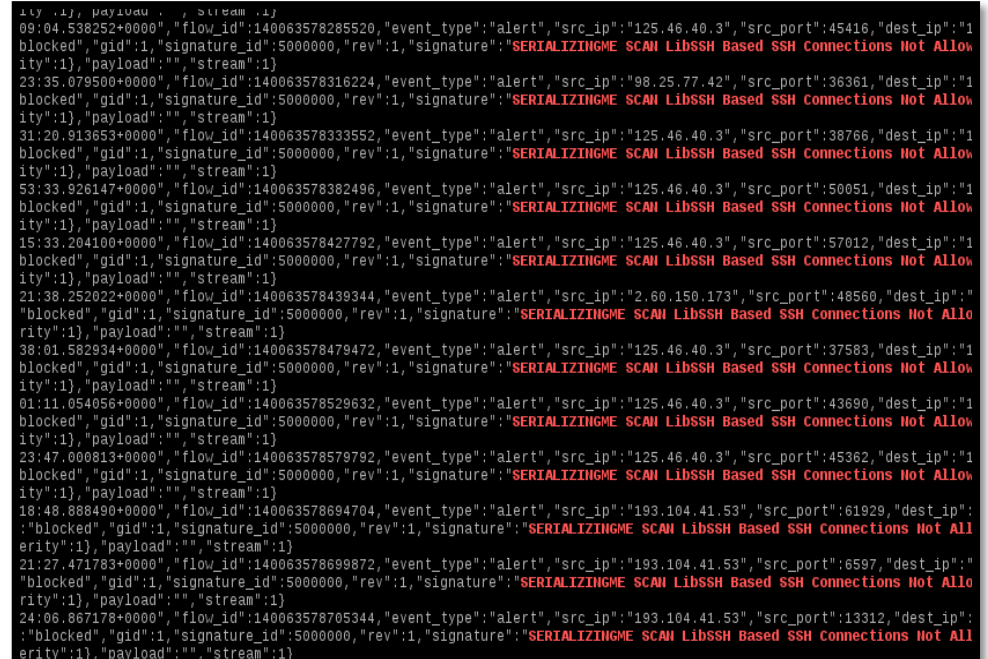


The image shows a web login interface with the following elements:

- Sign in** header
- Email** label above a text input field containing the payload: `test@example.com' OR 1 = 1 --`
- Password** label above a password input field containing eight dots (masked).
- A blue **Sign in** button.
- A checkbox labeled **Stay signed in** with a checked mark.

The payload `test@example.com' OR 1 = 1 --` is a classic SQL injection used to bypass authentication by forcing the database to execute a true statement.

Brute Force Attack



The image displays a network traffic capture (likely from Wireshark) showing a brute force attack on an SSH service. The traffic consists of multiple 'alert' events from the 'SERIALIZINGME SCAN LibSSH Based SSH Connections Not Allowed' rule. Key details include:

- Source IP:** 125.46.40.3
- Destination IP:** 193.104.41.53
- Source Port:** Varies (e.g., 45416, 36361, 38766, 50051, 57012, 48560, 37583, 43690, 45362, 61929, 6597, 13312)
- Destination Port:** 22 (SSH)
- Event Type:** alert
- Signature:** SERIALIZINGME SCAN LibSSH Based SSH Connections Not Allowed

The repeated alerts indicate that the attacker is attempting to establish an SSH session using incorrect credentials, which is characteristic of a brute force attack.

Tools for Web Security

Wireshark to capture the network traffic

The image shows the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main window displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 8652) is highlighted in blue. Below the packet list, the detailed view shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The packet data is displayed in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
8647	28.953832	Routerbo_1e:82:d4	Broadcast	ARP	56	Who has 10.0.0.15? Tell 10.0.0.1
8648	28.995211	216.58.209.234	10.0.0.47	GQUIC	62	Payload (Encrypted), PKN: 11
8649	29.138631	10.0.0.47	10.0.0.1	DNS	90	Standard query 0xa857 A nexusrules.officeapps.live.com
8650	29.163599	Routerbo_1e:82:d4	Broadcast	ARP	56	Who has 10.0.0.7? Tell 10.0.0.1
8651	29.173687	Routerbo_1e:82:d4	Broadcast	ARP	56	Who has 10.0.0.16? Tell 10.0.0.1
8652	29.175352	10.0.0.1	10.0.0.47	DNS	155	Standard query response 0xa857 A nexusrules.officeapps.live.com CNAME prod.nexusr...
8653	29.176884	10.0.0.47	52.109.12.18	TCP	66	2372 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
8654	29.276828	Routerbo_1e:82:d4	Broadcast	ARP	56	Who has 10.0.0.92? Tell 10.0.0.1
8655	29.303584	Routerbo_1e:82:d4	Broadcast	ARP	56	Who has 10.0.0.27? Tell 10.0.0.1
8656	29.333878	Routerbo_1e:82:d4	Broadcast	ARP	56	Who has 10.0.0.35? Tell 10.0.0.1

> Frame 8652: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface 0
> Ethernet II, Src: Routerbo_1e:82:d4 (cc:2d:e0:1e:82:d4), Dst: IntelCor_e2:29:d5 (68:07:15:e2:29:d5)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.47
> User Datagram Protocol, Src Port: 53, Dst Port: 59347
> Domain Name System (response)

```
0000  68 07 15 e2 29 d5 cc 2d e0 1e 82 d4 08 00 45 00  h...).--.....E-
0010  00 8d 78 58 00 00 40 11 ed d8 0a 00 00 01 0a 00  ..xX-@.....
0020  00 2f 00 35 e7 d3 00 79 7c f1 a8 57 81 00 00 01  ./-5...y|..W....
0030  00 02 00 00 00 00 0a 6e 65 78 75 73 72 75 6c 65  .....n exusrule
0040  73 0a 6f 66 66 69 63 65 61 70 70 73 04 6c 69 76  s.office apps.liv
0050  65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 05 00 01  e.com.....
0060  00 00 0d 76 00 25 04 70 72 6f 64 0a 6e 65 78 75  ...v-%p rod.nexu
0070  73 72 75 6c 65 73 04 6c 69 76 65 03 63 6f 6d 06  srules.l ive.com.
0080  61 6b 61 64 6e 73 03 6e 65 74 00 c0 3c 00 01 00  akadns.net<...
0090  01 00 00 00 99 00 04 34 6d 0c 12                .....4 m...
```

User Datagram Protocol (udp), 8 bytes

Packets: 9110 · Displayed: 9110 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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

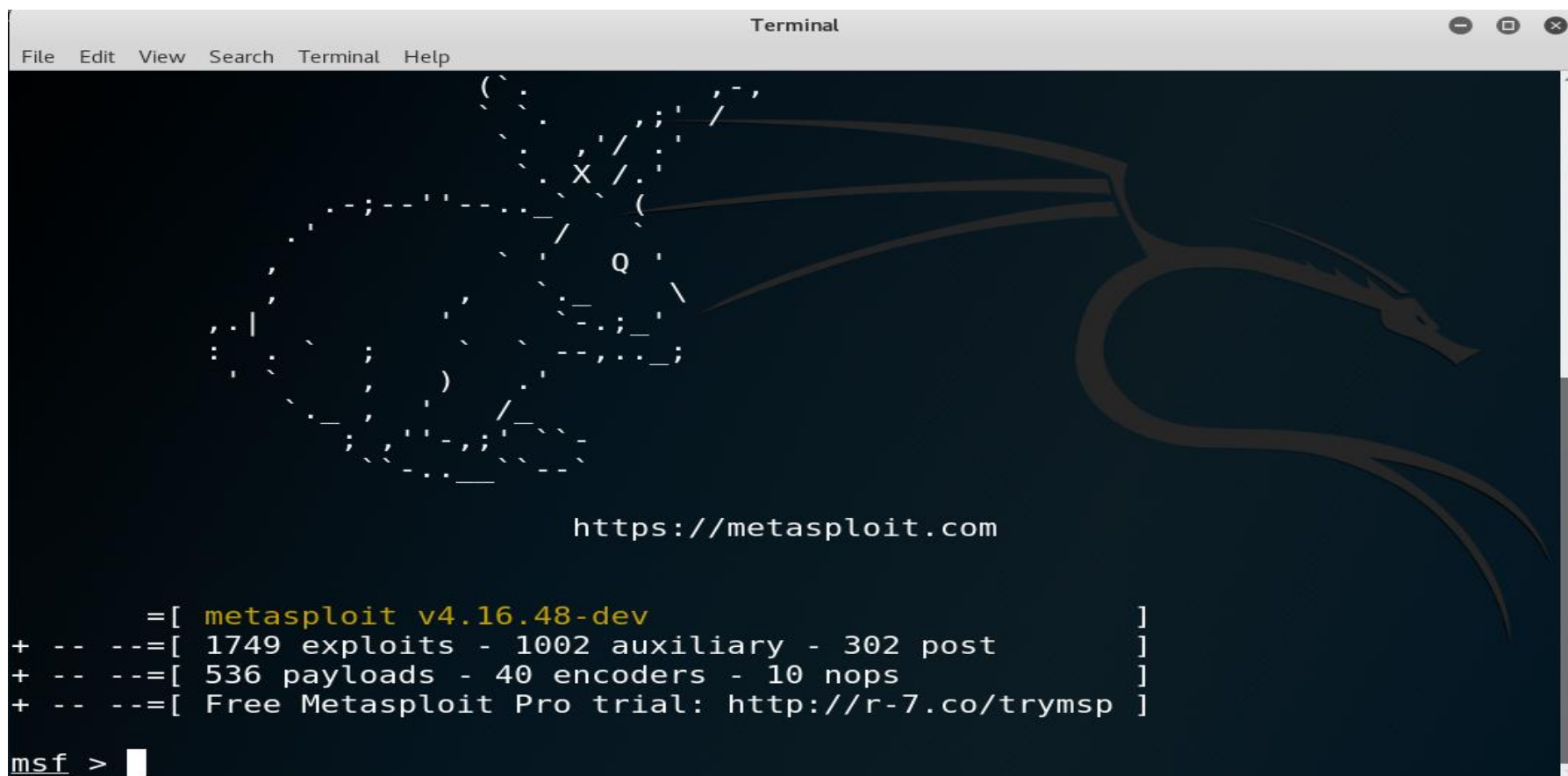
Tools for Exploitation

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



A screenshot of a terminal window titled "Terminal" with a menu bar containing "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal background is dark blue with a large, stylized dragon logo in a lighter blue color. The dragon is facing right and has its wings spread. Below the logo, the URL <https://metasploit.com> is displayed. At the bottom of the terminal, the Metasploit version and statistics are shown:

```
msf > =[ metasploit v4.16.48-dev ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

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

Tools for Network Monitoring

Splunk to analyze the computer logs

Q New Search Save As Close

"f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0000" AND NOT framework=f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0000 All time Q

✓ 336 events (before 11/20/15 9:32:11.000 PM) Job II ■ ↗ ↓ 📄 Smart Mode

Events (336) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields All Fields	i	Time	Event
Selected Fields a host 1 a source 1 a sourcetype 1 Interesting Fields # date_hour 5 # date_mday 1 # date_minute 36 a date_month 1 # date_second 20 a date_wday 1 # date_year 1 a index 1 # linecount 1 a punct 14	>	11/18/15 11:03:06.000 PM	Nov 18 23:03:06 ip-10-0-7-193.us-west-2.compute.internal mesos-master[1271]: I1118 23:03:06.086488 1276 hierarchical.hpp:1103] Recovered ports(*):[1025-2180, 2182-3887, 3889-5049, 5052-8079, 8082-8180, 8182-17516, 17518-19502, 19504-32000]; cpus(*):3.8; mem(*):13987; disk(*):32541 (total: ports(*):[1025-2180, 2182-3887, 3889-5049, 5052-8079, 8082-8180, 8182-32000]; cpus(*):4; mem(*):14019; disk(*):32541, allocated: ports(*):[17517-17517, 19503-19503]; cpus(*):0.2; mem(*):32) on slave f0c9dc61-27fb-4d1a-b774-2d3163c23db7-S0 from framework f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0000 host = ip-10-0-7-193.us-west-2.compute.internal source = /home/core/splunkforwarder/bin/scripts/journald-master.sh sourcetype = exec
	>	11/18/15 11:03:06.000 PM	Nov 18 23:03:06 ip-10-0-7-193.us-west-2.compute.internal mesos-master[1271]: I1118 23:03:06.086324 1276 master.cpp:2918] Processing ACCEPT call for offers: [f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0102] on slave f0c9dc61-27fb-4d1a-b774-2d3163c23db7-S0 at slave(1)@10.0.2.71:5051 (10.0.2.71) for framework f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0000 (marathon) at scheduler-6215179f-a047-40f0-9b36-817fd6b4eed4@10.0.7.193:50983 host = ip-10-0-7-193.us-west-2.compute.internal source = /home/core/splunkforwarder/bin/scripts/journald-master.sh sourcetype = exec
	>	11/18/15 11:03:06.000 PM	Nov 18 23:03:06 ip-10-0-7-193.us-west-2.compute.internal mesos-master[1271]: I1118 23:03:06.084765 1279 master.cpp:4967] Sending 1 offers to framework f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0000 (marathon) at scheduler-6215179f-a047-40f0-9b36-817fd6b4eed4@10.0.7.193:50983 host = ip-10-0-7-193.us-west-2.compute.internal source = /home/core/splunkforwarder/bin/scripts/journald-master.sh sourcetype = exec
	>	11/18/15 11:03:00.000 PM	Nov 18 23:03:00 ip-10-0-7-193.us-west-2.compute.internal mesos-master[1271]: I1118 23:03:00.081466 1275 hierarchical.hpp:1103] Recovered ports(slave_public):[1-21, 23-5050, 5052-32000]; cpus(slave_public):4; mem(slave_public):14019; disk(slave_public):32541 (total: ports(slave_public):[1-21, 23-5050, 5052-32000]; cpus(slave_public):4; mem(slave_public):14019; disk(slave_public):32541, allocated:) on slave f0c9dc61-27fb-4d1a-b774-2d3163c23db7-S1 from framework f0c9dc61-27fb-4d1a-b774-2d3163c23db7-0000 host = ip-10-0-7-193.us-west-2.compute.internal source = /home/core/splunkforwarder/bin/scripts/journald-master.sh sourcetype = exec

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

Contents

Exercise

4

RPCA Cyber Teams and Challenges

RPCA Cyber Teams 2018

ผู้เข้าร่วมแข่งขัน Cyber War ทหาร-ตำรวจ

ตัวแทน รร.นรต. ทีมที่ ๑



นรต.ณัฐชนน ภูสมดา ชั้นปีที่ ๔



นรต.ภัทรารักษ์ ดำราชฤทธิ์ ชั้นปีที่ ๔



นรต.สิริคณัย ยะอุโฆงค์ ชั้นปีที่ ๔



นรต.อนุสรณ์ ปินใจ ชั้นปีที่ ๔

FirstHUNTER

2 จาก 3

ผู้เข้าร่วมแข่งขัน Cyber War ทหาร-ตำรวจ

ตัวแทน รร.นรต. ทีมที่ ๒



นรต.ภัทรพงศ์ ระมิ่งทอง ชั้นปีที่ ๓



นรต.ชัยสิทธิ์ เขมกมลพิธิ ชั้นปีที่ ๓



นรต.ศุภเกียรติ สบง ชั้นปีที่ ๒



นรต.หญิง สาวตรี ราวีนิจ ชั้นปีที่ ๒

SecondHUNTER

3 จาก 3

ผู้เข้าร่วมแข่งขัน Cyber War ทหาร-ตำรวจ

ตัวแทน รร.นรต. ทีมที่ ๓



นรต.ปรีชญา นุราชักษ์ ชั้นปีที่ ๓



นรต.เอกกรินทร์ ทองหยด ชั้นปีที่ ๓



นรต.สรวิชัย เจริญไพศาล ชั้นปีที่ ๓



นรต.ภฤชภูมิกุล ถิอคำโสภาคย์ ชั้นปีที่ ๒

ThirdHUNTER

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

New Blood Cyber Police Officers

ผู้เข้าร่วมแข่งขัน Cyber War ทหาร-ตำรวจ

ตัวแทน รร.นรต. ทีมที่ ๑



นรต.ณัฐชนน ภูสมดา ชั้นปีที่ ๔



นรต.ภัทรารัฐ ดำราชภูริ ชั้นปีที่ ๔

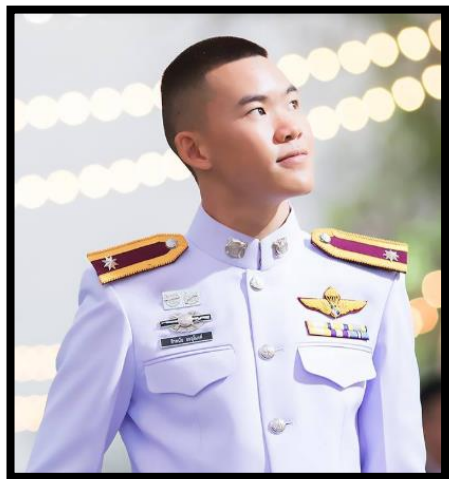


นรต.สิรัตนัย ยะอุโมงค์ ชั้นปีที่ ๔



นรต.อนุสรณ์ ปินใจ ชั้นปีที่ ๔

FirstHUNTER



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

RPCA Cyber Teams 2019



SecondHUNTER

ThirdHUNTER

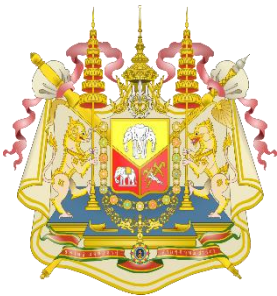
FourthHUNTER

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

1st Cyber Security Competition for Military and Police Academy

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

Capture The Flag (CTF) Training



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

The list of capture the flag (CTF) tools

ID : raining ##
password:

- Number of Mac.

⑥ Exploit

- Wireshark
- Nmap

⑦ Misc.

- Autopsy

① Tutorial

- w3school
- tutorialpoint
- hacking article
- abatchy*
- root me
- defcon

- Translator Tools

② Crypto

- Cybercef
- Cryptool 2
- Reverse String

③ Code

- Python
- Java → Eclipse
- Text Editor
- Edit Plus / Notepad ++
- Sublime
- Jsbeautiful
- Dev-C++

- Bytecode Viewer

- Boomerang

- Xiao Steganography

- Sonic Visualizer } 1 new

- Sound Forge

- HXD → Hex → HEX

- GeoSetter → Map

- IDA | Abbyy → OCR

⑤ Web

- Google Chrome

- Hack Bar → Firefox

- Dirbuster

- IP Scanner

1st Cyber Security Competition for Military and Police Academy

The competition day, with consecutive 8 hours



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



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

1st Cyber Security Competition for Military and Police Academy

The competition day, try to be the winner



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

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

1st Cyber Security Competition for Military and Police Academy

A cup and prizes in this competition



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

1st Cyber Security Competition for Military and Police Academy

The first runner up for Second HUNTER



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

RPCA cyber team in this competition



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

Financial Cyber Security Boot Camp 2018

Financial Cyber Security Boot Camp 2018

FINANCIAL BOOT CAMP #2/2018



#FINCYBERSEC
THAILAND

Organized by the Bank of Thailand (BOT)

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

Financial Cyber Security Boot Camp 2018

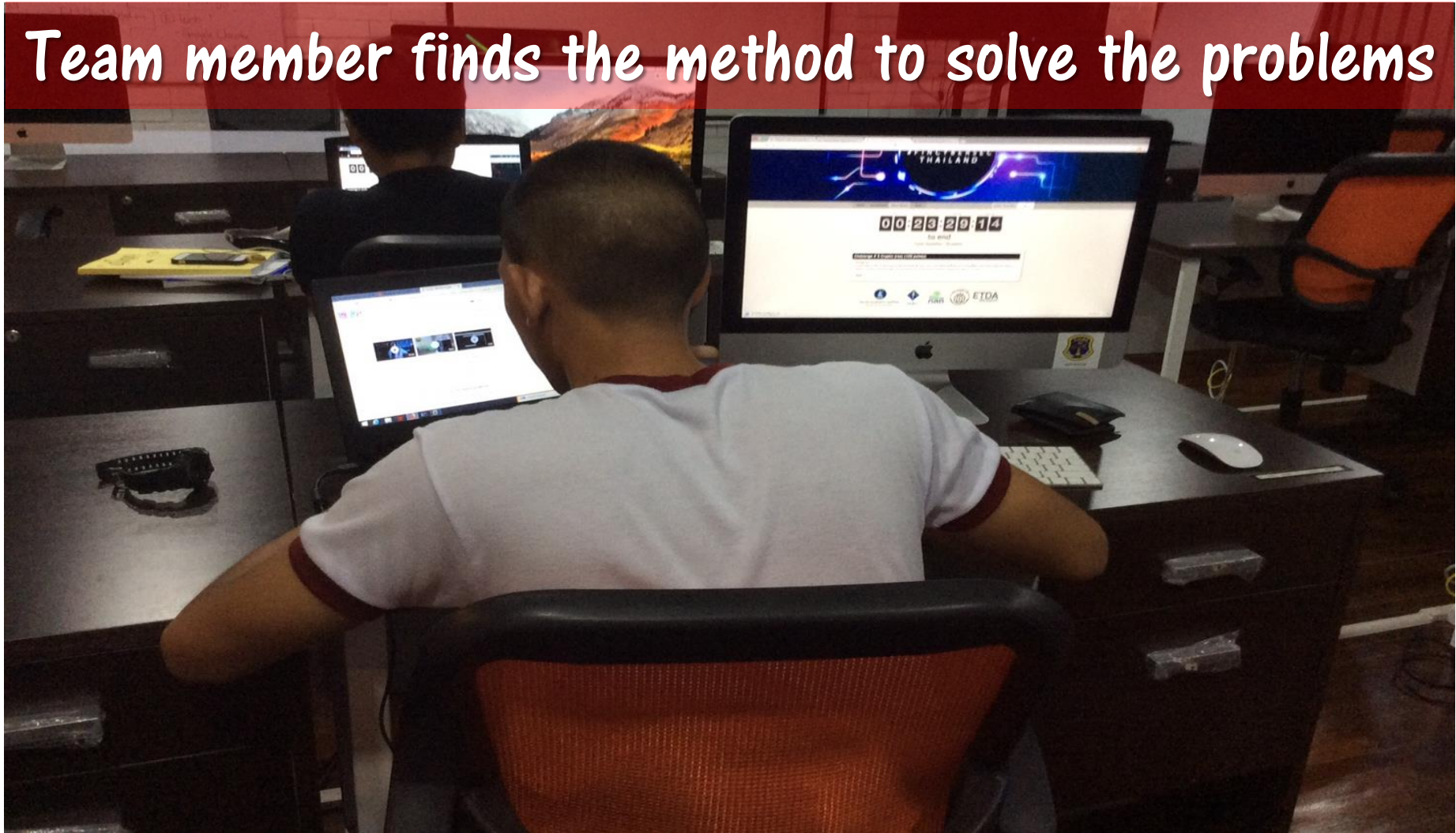
The first round in online competition



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

Financial Cyber Security Boot Camp 2018

Team member finds the method to solve the problems



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

Financial Cyber Security Boot Camp 2018

Some of team member can solve the problem



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

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

Financial Cyber Security Boot Camp 2018

Two of RPCA cyber team go to the final round

:0{ :|:& }::

!IsCaptured

1amN00b

AA K

cnior

CPCUCTF

Cyber Guardian

FTTS

Hamburger

Maiden

MUTAE

OLAN

Omega3

Talardlang

test

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

Financial Cyber Security Boot Camp 2018

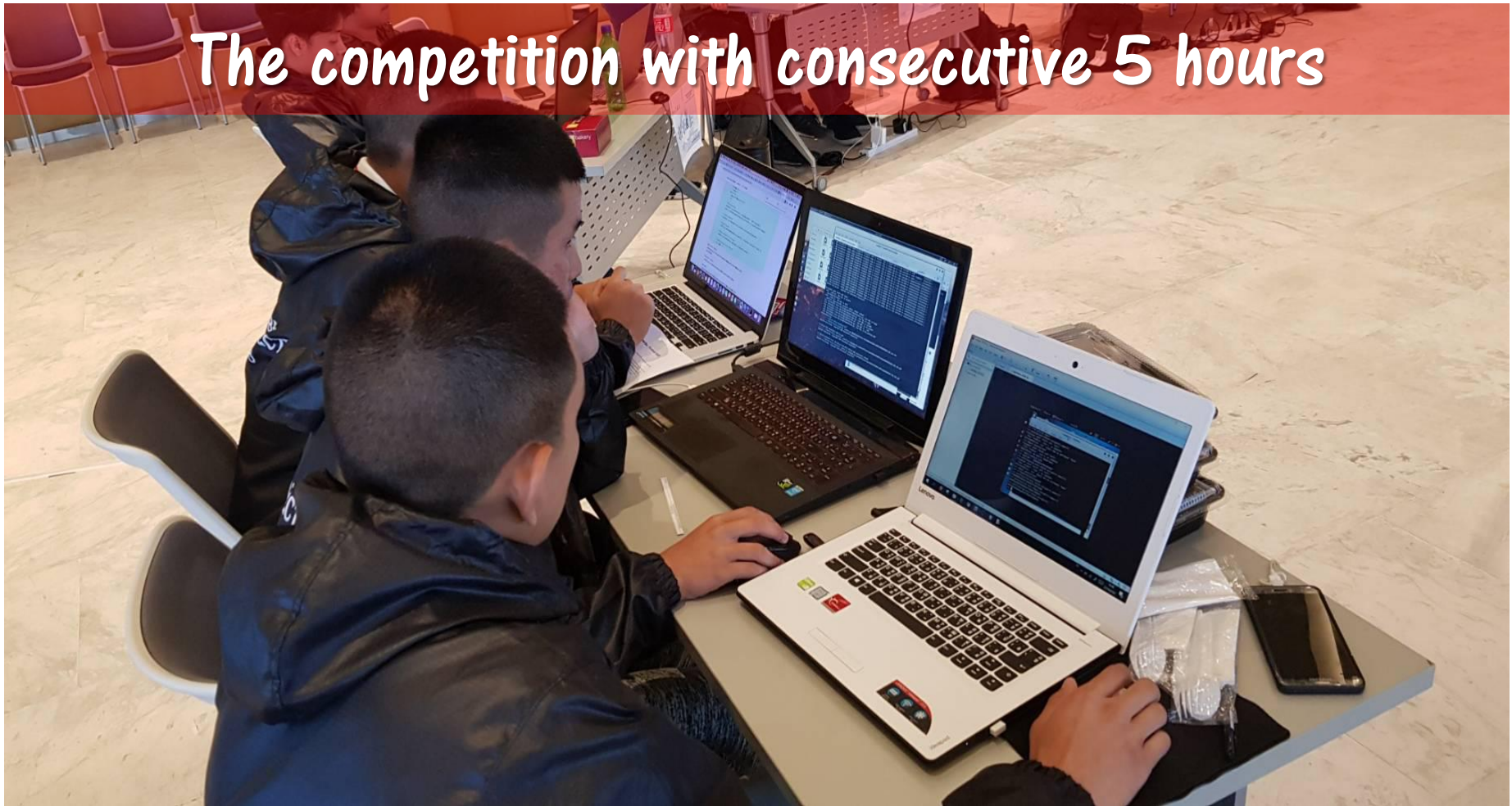
The final round at the learning center of BOT



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

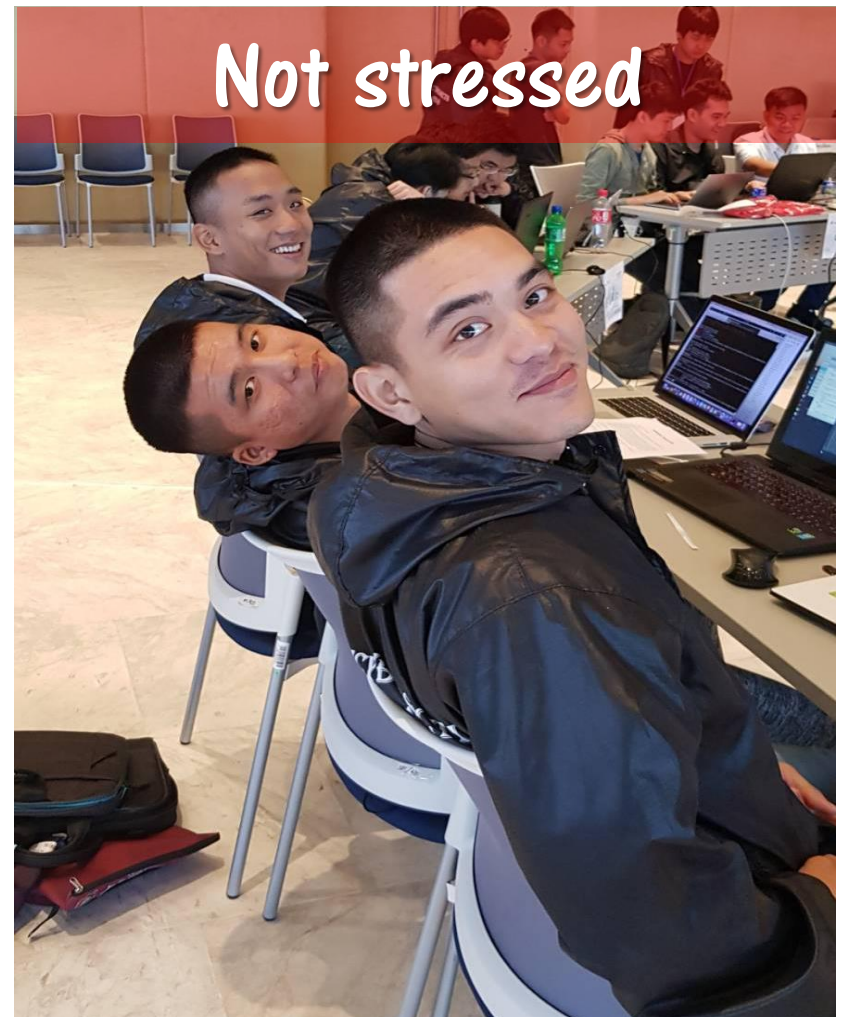
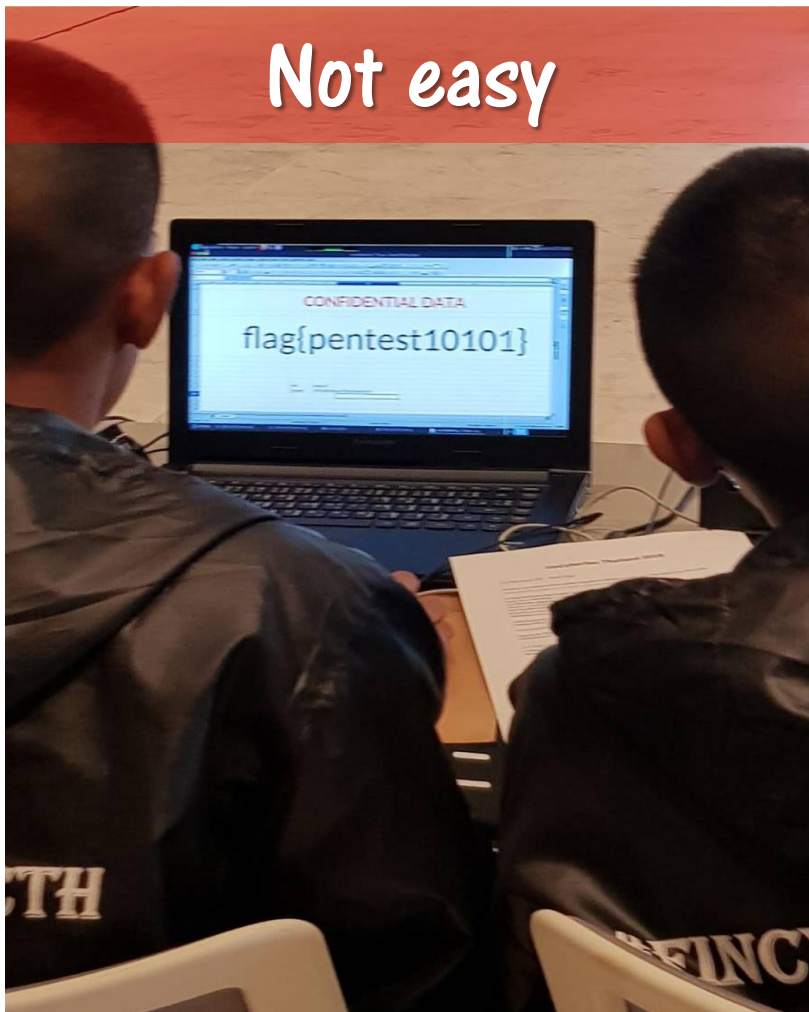
Financial Cyber Security Boot Camp 2018

The competition with consecutive 5 hours



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

The 7th places for this competition



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.

Are you ready to take on
this year's challenge?

[Watch the video](#)



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

Very hard problems for this competition



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

KPMG Cyber Security Challenge 2018

Cyber Security

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

Cyber Security

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

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

KPMG Cyber Security Challenge 2018

RPCA cyber team in this competition



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

Thailand Cyber Security Competition for Military and Police Institutes

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

The competition with consecutive 12 hours



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
bcd6c493029480225ec5b2fle4a4b7a4
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

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

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	Odaysober		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**
n.w. 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**
n.w. 03, 2019 21:00 UTC | On-line

Place	Team	Country	Points
1	PetCatGetFlag		46.400
2	d4rk0de		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

Thank You