



# ความปลอดภัยคอมพิวเตอร์ (424)

## แนวทางการเรียน การคิดคำแบน

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์

Email : songrit@npu.ac.th

สาขาวิชาวิศวกรรมคอมพิวเตอร์  
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

Revised 2020-06-26

# ວິສະກຮນຄວມພົວເຕວ່າ

- **华硕** 旺角办公室
  - การจัดองค์ประกอบและสถาปัตยกรรมคอมพิวเตอร์
  - โครงสร้างข้อมูล
  - อัลกอริทึม
  - การโปรแกรมคอมพิวเตอร์
  - คอมพิลิเออร์
  - ระบบปฏิบัติการ
  - เครือข่ายคอมพิวเตอร์
  - วิศวกรรมซอฟต์แวร์
  - การเรียนรู้ของคอมพิวเตอร์ และ เอไอ

# ด้าน Security จบไปทำอะไร



ผู้พัฒนาและอุดหนุน  
Securely Provision (SP)



ผู้ดูแลรักษา  
Operate and Maintain (OM)



ผู้บริหารและผู้ตรวจสอบระบบ  
Oversee and Govern (OV)



ผู้รับมือภัยคุกคาม  
Protect and Defend  
(PR)



ผู้วิเคราะห์ข้อมูล  
Analyze (AN)



ผู้เก็บพยานหลักฐาน  
Collect and Operate  
(CO)



ผู้ดำเนินการสืบสวน  
สอบสวน  
Investigate (IN)

NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

# **อาชีพทางไซเบอร์ ตลาดมีความต้องการสูง ประจำปี 7 สมรรถนะ**

- **การพัฒนาและออกแบบระบบ**
- **การดูแลระบบ**
- **การบริหารและผู้ตรวจสอบระบบ**
- **การรับมือภัยคุกคาม**
- **การวิเคราะห์ข้อมูล**
- การเก็บพยานหลักฐาน
- การดำเนินการสืบสวนสอบสวน

# อาชีพความมั่นคงปลอดภัยทางไซเบอร์ 52 อาชีพ (35 สาขา)

## Securely Provision (SP)

- Authorizing Official
- Security Control Assessor
- Software Developer
- Secure Software Assessor
- Enterprise Architect
- Security Architect
- Research and Development Specialist
- Systems Requirements Planner
- System Test & Evaluation Specialist
- Information Systems Security Developer
- Systems Developer



## Analyze (AN)

- Threat/Warning Analyst
- Exploitation Analyst
- All-Source Analyst
- Mission Assessment Specialist
- Target Developer
- Target Network Analyst
- Multi-Disciplined Language Analyst



## Operate and Maintain (OM)

- Database Administrator
- Data Analyst
- Knowledge Manager
- Technical Support Specialist
- Network Operations Specialist
- System Administrator
- Systems Security Analyst



## Protect and Defend (PR)

- Cyber Defense Analyst
- Cyber Defense Infrastructure Support Specialist
- Cyber Defense Incident Responder
- Vulnerability Assessment Analyst



## Collect and Operate (CO)

- All Source-Collection Manager
- All Source-Collection Requirements Manager
- Cyber Intel Planner
- Cyber Ops Planner
- Partner Integration Planner
- Cyber Operator



20171128\_ กำหนดแนวทางทักษะด้านคิวท์ลัลของข้าราชการครูที่สอน Cyber

## Oversee and Govern (OV)

- Cyber Legal Advisor
- Privacy Officer/Privacy Compliance Manager
- Cyber Instructional Curriculum Developer
- Cyber Instructor
- Information Systems Security Manager
- Communications Security (COMSEC) Manager
- Cyber Workforce Developer and Manager
- Cyber Policy and Strategy Planner
- Executive Cyber Leadership
- Program Manager
- Information Technology (IT) Project Manager
- Product Support Manager
- IT Investment/Portfolio Manager
- IT Program Auditor



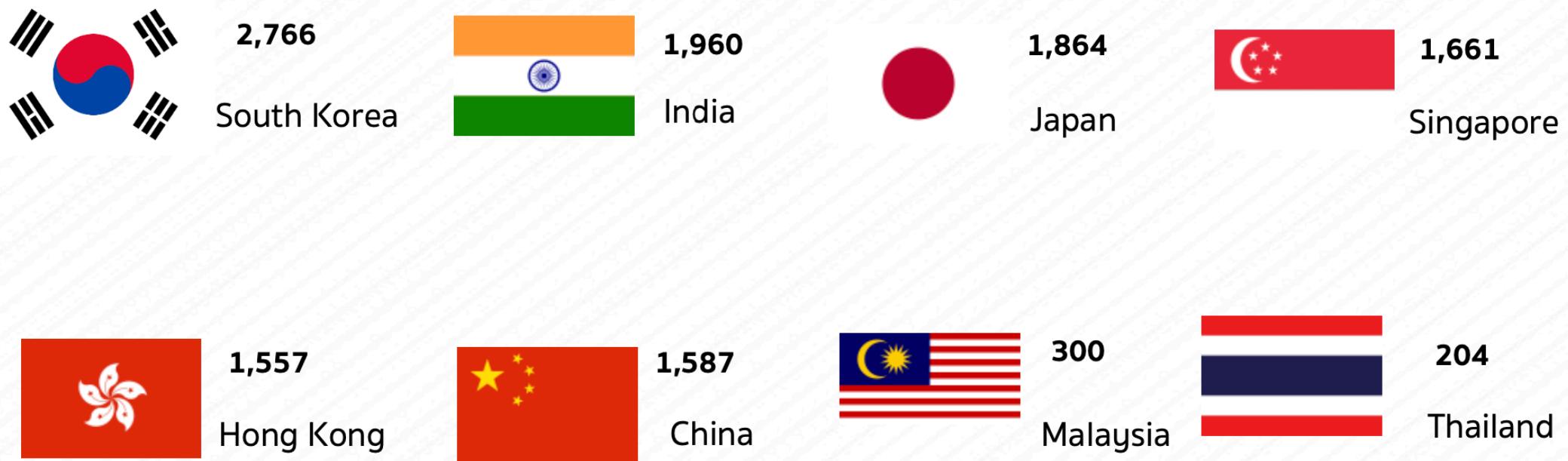
## Investigate (IN)

- Cyber Crime Investigator
- Law Enforcement/Counterintelligence Forensics Analyst
- Cyber Defense Forensics Analyst



# สายงานด้านนี้ควรมี Certificate

- ใบประกาศนียบัตรด้านความมั่นคงปลอดภัยไซเบอร์
- CISSP (Certified Information Systems Security Professional) -- 2560



# Computer Security Professional Certificates



CISSP  
SSCP  
CAP  
CSSLP  
CCFP  
CCSP  
HCISPP



eJPT  
eCPPT Gol  
eWP  
eCRE  
eMAPT



CASP  
CSA+  
Security+  
  


CCNA  
Security  
CCNP  
Security  
CCIE  
Security  
CCNA  
CyberOps



C)PTE  
C)PTC  
C)DFE  
C)IHE  
C)ISSO  
C)PEH  
C)ISSM  
C)ISSA  
C)ISRM  
C)NFE  
C)VVA



EITCA/IS



CISA  
CISM  
CRISC



OSCP  
OSWP  
OSCE  
OSEE  
OSWE



CIPP  
CIPM  
CIPT



CEH  
ECSA

LPT  
CHFI

ECIH  
ENSA  
CCISO  
EDRP  
ECVP  
ECES  
ECCSP

GISF  
GSEC

GISP  
GCFE

GPPA  
GCIA  
GCIH

GCUX  
GCW  
N  
GCED



GWAPT  
GSLC  
GCPM  
GSSP-NET  
NET  
JAVA  
GSNA  
GCFA  
GLEG  
GAWN  
GXPN  
GREM  
GSE

# แนวการเรียน

---

- ในวิชานี้ เราจะศึกษาการเจาะระบบ
- เจาะระบบจำลองทุกสัปดาห์
  - บันทึกคะแนนในระบบ <https://elab.npu.world>
- สัปดาห์ละเรื่อง
- Capture the flag (CTF)
  - มีโจทย์การเจาะระบบทุกสัปดาห์
  - เจาะระบบแต่ละสัปดาห์ไม่ต่อเนื่องกัน

# แนะนำรายวิชาและข้อตกลง

---

- Coaching : ทรงฤทธิ์ กิติศรีเวรพันธุ์ (ทอม)
- ห้องพัก : EN1 503
- อีเมล : [songrit@npu.ac.th](mailto:songrit@npu.ac.th)
- Class : อังคาร 9-12u.
- TAs : ???
  - OHs : ศุกร์ 13-15u.

# Syllabus

---

- วิชา ก่อนเรียน:
  - เครื่อข่ายคอมพิวเตอร์
- Textbook:
  - N/A
- เว็บไซต์:
  - <https://git.npu.world/Lecture-CPE/501>
  - <https://elab.npu.world>
  - ประกาศ สไลด์ การบ้าน
- Class Mailing List: ??
  - Discord : <https://discord.gg/bS57zPk>
  - Sending mail direct to me. [songrit@npu](mailto:songrit@npu) or TAs.

# គេហទ័រ

- គិតគេហទ័រ

- Attend-30%, Assignment-20%, Exam-20%, 30%

- HWs:

- មិនមែនការបាន
  - កែចំណែនីយប្រព័ន្ធ

- Exams:

- ការការណ៍ (CTF)
  - ការការណ៍ (Web – CTF)

# **Week project**

---

- งานประจำ
  - งานเดี่ยว
  - ส่ง flag ในคาบทุกสัปดาห์
- สอบบกกลางภาค
  - เดี่ยว
- สอบปลายภาค
  - ทีมละ 2 คน
  - หรือ 3 คน (กรณีพิเศษ)

# ความสำคัญ ความปลอดภัยไซเบอร์

---

- ความจำเป็นในการมีระบบรักษาความปลอดภัย
  - ส่วนตัว
  - องค์กร
  - ประเทศ
  - รับมือผู้ก่อการร้ายทางไซเบอร์ (Cyberwarfare)

# องค์ความรู้ที่จะได้

---

- องค์ประกอบความมั่นคงปลอดภัยระบบคอมพิวเตอร์
- เทคนิควิธีการทดสอบความมั่นคงปลอดภัยทางไซเบอร์
- มาตรฐานการรายงานช่องโหว่
- เทคนิค-เครื่องมือการเจาะระบบ
- การบริหารจัดการด้านความมั่นคงปลอดภัย

# Clip

---

- สารคดี cybersecurity
- รายการ คิดยกกำลังสอง (ThaiPBS)

# เนื้อหาในวิชา

---

## • กล่องภาค

- **W1** แบบนำวิชา การใช้ค่าแบบ
- **W2** Vulnerability and Exploit
- **W3** Binary and execution file
- **W4** Layer 2 attack
- **W5** Layer 3 attack
- **W6** Remote code execution
- **W7 Midterm exam**
- **W8** Site visited

## • ปลายภาค

- **W9** Phishing and Pharming attack
- **W10** XSS (Cross Site scripting)
- **W11** Cookies attack
- **W12** Cryptographic issues
- **W13** SQL injection
- **W14** Reverse
- **W15 เจาะระบบภาคปฏิบัติ**

# แบบนำวิธีเรียน

---

- **มีส่วนร่วม** – มีส่วนร่วมในการเรียน พูดคุยกับอาจารย์ เพื่อน หรือการใช้เบอร์
- **วางแผน** – จัดช่วงเวลาเรียนรู้เวลาเดิม ใช้เวลาประมาณ 2-4 ชั่วโมงต่อสัปดาห์
- **ทบทวน** – ทบทวนเนื้อหาเป็นระยะ สืบคัน สอบคลานส่วนที่ยังไม่เคลียร์
- **ฝึกทำโจทย์** – ฝึกตอบคำถามจากโจทย์ ทำการบ้าน
- **เขียนโค้ด** – เขียนโค้ดด้วยตนเอง
- **ท่องโลกใช้เบอร์** – ศึกษาจากอินเทอร์เน็ตเพิ่มเติม หรือจากความรู้เสริมที่แนะนำ

# การเรียนด้านความปลอดภัยคอมพิวเตอร์

---

- ความมั่นคงทางคอมพิวเตอร์
- ใช้งานค์ความรู้ในแนวกว้าง
- เทคนิคการเจาะระบบใหม่ๆ ยังต้องการความคิดสร้างสรรค์
- ปัญหาด้านความปลอดภัยคอมพิวเตอร์มีมาตั้งแต่เมื่อคอมพิวเตอร์
- ผู้เชี่ยวชาญให้การยอมรับวิธีการเรียนรู้ด้านความปลอดภัยแบบ **CTF**
- ช่วยได้ดีกว่าการ Lecture เพียงอย่างเดียว

# Capture the flag

---

- **Capture** คือ ตามจับ / ตามหา / ค้นหา
- **the flag** คือ ธง / สัญลักษณ์
- ในที่นี่ flag code คือสิ่งที่เราตามหา
- การจะได้ flag code ต้องแก้ปัญหา(เจาะระบบ) โดยยั่งๆ ข้อ

flag{W3lc0m3\_t0\_CTF}

NPU-CTF{W3lc0m3\_NPU}

# ປະເກທຂອງ CTF

---

- Jeopardy (ຈັບ-ປາ-ດີ້)
  - ຄັນຫາ ‘flag’ ທີ່ໜ້ອນວ່າຢູ່ໃນໂຈກຍົດ້ວຍວິຣີກາຣຕ່າງ ໃາ
- Attack-Defense
  - ແບ່ງ 2 ຝ່າຍ
    - Attack ເປັນຝ່າຍຄັນຫາວິຣີເຈາະຮະບບ
    - Defense ເປັນຝ່າຍຕັ້ງແນວຮັບ

# องค์ความรู้สำคัญ พบใน CTF

---

- การใช้สคริป
- การเจาะระบบปฏิบัติการ
- การแครกค์ซอฟต์แวร์ (Reverse engineering)
- การวิเคราะห์เทคโนโลยีรหัสลับ (Cryptanalysis)
- การพิสูจน์หลักฐาน (Forensic)
- เทคโนโลยีเครือข่าย
- การโจมตีในชีวิตจริง
- เทคโนโลยีการซ่อนรหัส
- เทคโนโลยีเว็บบราวเซอร์
- เทคโนโลยีเว็บเซิร์ฟเวอร์

# Capture the flag เว็บไซต์

---

- <https://picoctf.com>
- <https://ctf.hacker101.com>
- <https://ctftime.org/event/list/upcoming>

NPU-CTF{.....}

ແບ່ງຂັນ CTF ເປົ້າແລ້ວ  
ໃຫຍ່ ??

---

