

แชร์ประสบการณ์สอบ Cybersecurity Certificates



MAYASEVEN
HACK THINGS

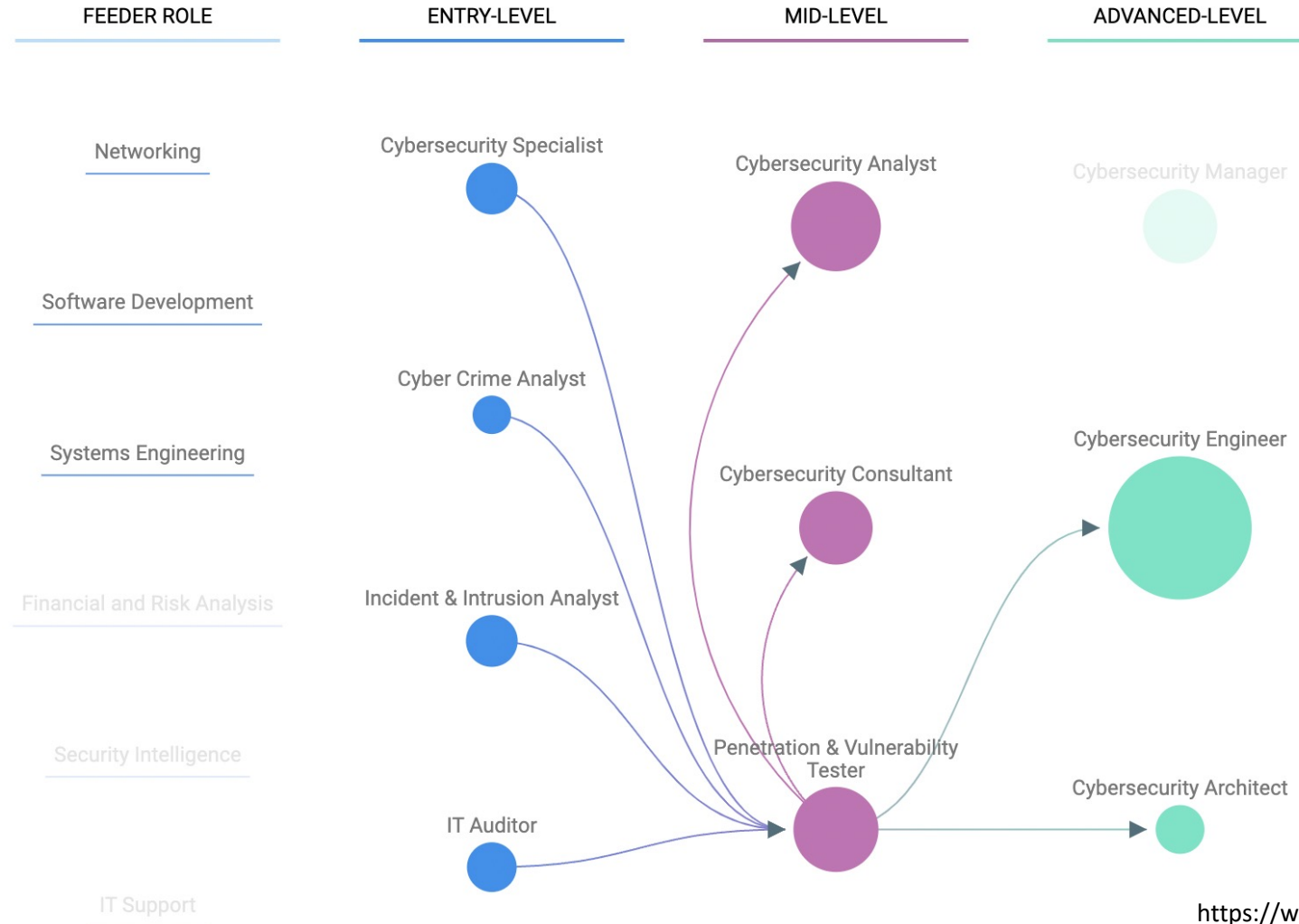


- Principal Cyber Security Consultant
- Penetration Testing
- Research new vulnerabilities
- Developing hacking tools
- Instructor of Ethical Hacking and Security Workshop
- Instructor of Secure Coding and Ethical Hacking
- Blog writer at <https://mayaseven.com>

Nop Phoomthaisong

CISSP-ISSAP, CISSP, CSSLP, CREST (CRT, CPSA), CISM, eCXD, eWPTX, eMAPT, GXPN, OSWE, OSCE, OSCP, SPSE, CompTIA PenTest+, CDPSE

CYBERSECURITY CAREER PATHWAY



<https://www.cyberseek.org/pathway.html>

My Certificates



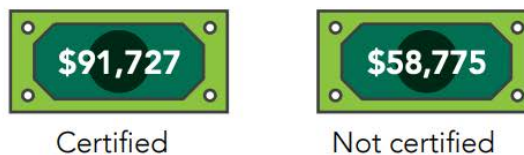
ทำไมเราต้องมี Cybersecurity Certificates

- คู่ค้าให้คุณค่าเพิ่มความน่าเชื่อถือในการให้บริการ
- ผู้บริหารหรือ HR ให้คุณค่าช่วยให้เติบโตในสายงาน Cybersecurity
- พิสูจน์หรือพัฒนาตัวเองว่าเรามีความรู้จริงตามมาตรฐานสากล

How Much Study Participants Earn Around the World (U.S. Dollars)



AVERAGE SALARY IF CYBERSECURITY CERTIFIED



Ref: (ISC)2 Cybersecurity Workforce Study, 2021

Types of cybersecurity certifications

Which of the following types of cybersecurity certifications does your organization require you to have?

Vendor-neutral cybersecurity certifications
(e.g. (ISC)², ISACA, CompTIA, etc.)

55%

Vendor-neutral certifications are particularly ubiquitous among **military** (82%) personnel.

Vendor-specific cybersecurity certifications
(e.g., Cisco, Microsoft, etc.)

38%

Requirements have dropped significantly in the past three years (**55% in 2019 vs. 38% in 2022**).

None, my organization doesn't require me to have any type of certification

32%

Base: 11,540 global cybersecurity professionals on cybersecurity teams

Ref: (ISC)² Cybersecurity Workforce Study, 2022

(ISC)2

(ISC)²: The World's Leading Cybersecurity Professional Organization

You face immense pressure to stay ahead of attacks and up-to-date in our ever-changing security profession. But you aren't alone.

(ISC)² is an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. Nearly 280,000 members, associates and candidates strong, we empower professionals who touch every aspect of information security.

How can we help you make an impact in your career and advance our industry? Through our globally recognized [certifications](#). Our vast networking and collaboration opportunities. Our [Professional Development Institute](#) and leadership tools.

We're also committed to educating the general public through our support of [The Center for Cyber Safety and Education](#). Because we get it. Protecting information is everyone's job — not just IT's job!

Join us in our vision of inspiring a safe and secure cyber world.

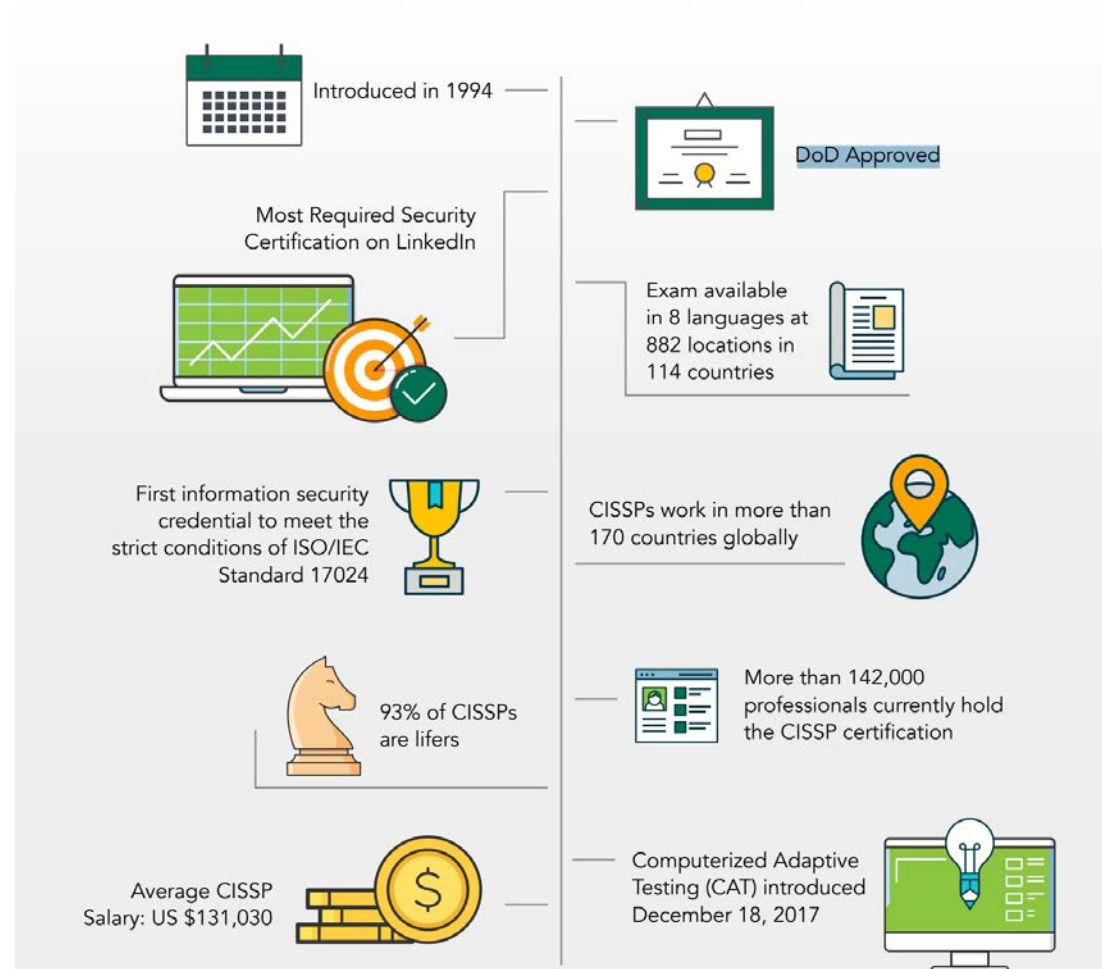
(ISC)2

- CISSP - Certified Information Systems Security Professional
- CISSP-ISSAP - Information Systems Security Architecture Professional
- CSSLP – Certified Secure Software Lifecycle Professional



CISSP - Certified Information Systems Security Professional

Fast Facts About CISSP



CISSP - Certified Information Systems Security Professional

Jobs that Typically Use or Require the CISSP

- » Chief Information Officer
- » Chief Information Security Officer
- » Director of Security
- » IT Director/Manager
- » Network Architect
- » Security Analyst
- » Security Architect
- » Security Auditor
- » Security Consultant
- » Security Manager
- » Security Systems Engineer

Ref: (ISC)2 THE ULTIMATE GUIDE TO THE CISSP

CISSP - Certified Information Systems Security Professional

Pathway to CISSP Certification

Obtain the Required Experience

To qualify for the CISSP, candidates must have at least five years of cumulative, paid full-time work experience in two or more of the eight domains:

Domain 1. Security and Risk Management

Domain 2. Asset Security

Domain 3. Security Architecture and Engineering

Domain 4. Communication and Network Security

Domain 5. Identity and Access Management (IAM)

Domain 6. Security Assessment and Testing

Domain 7. Security Operations

Domain 8. Software Development Security

CISSP exam registration fee \$749

If you don't have enough experience yet, you can still pass the CISSP exam and become an Associate of (ISC)² while you earn the work experience needed.

CISSP - Certified Information Systems Security Professional

125 - 175

Number of items on the English CISSP CAT
(Computer Adaptive Testing) exam

The non-English linear, fixed-form CISSP exam has 250 items

4 hrs.

Maximum amount of time
for the CISSP CAT exam

The non-English linear, fixed-form CISSP
exam allows 6 hours to complete

700

Score you need out of 1,000
to pass the exam

CISSP CAT

As of December 18, 2017, all English CISSP exams worldwide use CAT. Non-English CISSP exams are administered as a linear, fixed-form exam.

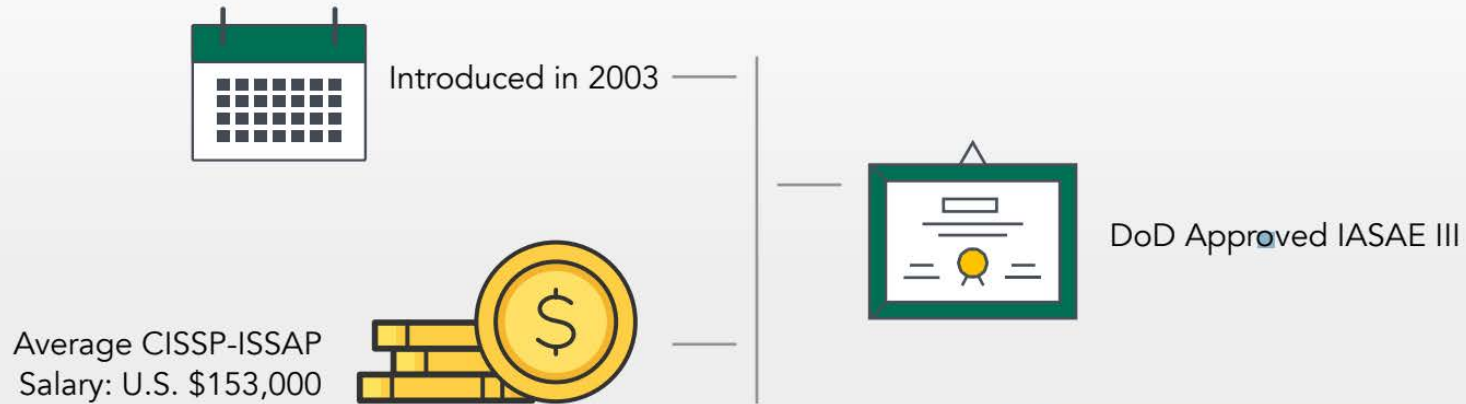
[Learn more about CAT](#)

Exam availability: English, French, German, Brazilian Portuguese, Spanish Modern, Japanese, Simplified Chinese, Korean

Testing Centers: (ISC)² Authorized PPC and PVTC Select Pearson VUE Testing Centers

CISSP-ISSAP - Information Systems Security Architecture Professional

Fast Facts About CISSP-ISSAP



SHOUT-OUTS

CISSP-ISSAP
RANKED #2
on the 2019
**CERTIFICATION SALARY
SURVEY 75 LIST**
— CertMag

CISSP-ISSAP - Information Systems Security Architecture Professional

Jobs that Typically Use or Require the CISSP-ISSAP

- » Security Architect
- » Security Analyst
- » Chief Security Officer
- » Chief Technology Officer
- » System Architect
- » System and Network Designer

Ref: (ISC)2 THE ULTIMATE GUIDE TO THE CISSP-ISSAP

Pathway to CISSP-ISSAP Certification

Obtain the Required Experience

To qualify for the CISSP-ISSAP, you must be a CISSP in good standing and have two years of cumulative, paid, full-time work experience in one or more of the six domains of the CISSP-ISSAP Common Body of Knowledge (CBK):

Domain 1. Identity and Access Management Architecture

Domain 2. Security Operations Architecture

Domain 3. Infrastructure Security

Domain 4. Architect for Governance, Compliance and Risk Management

Domain 5. Security Architecture Modeling

Domain 6. Architect for Applications Security

CISSP-ISSAP - Information Systems Security Architecture Professional

125

Number of items on the CISSP-ISSAP exam

3

Maximum amount of time for
the CISSP-ISSAP exam

hrs.

700

Score you need out of 1,000
to pass the exam

Exam availability: English

Testing Centers: Pearson VUE

CSSLP – Certified Secure Software Lifecycle Professional

Fast Facts About CSSLP



Introduced in 2008



DoD Approved

Average CSSLP
Salary: US \$126,463



(ISC)² certified members
work in more than 170
countries globally



Ref: (ISC)2 THE ULTIMATE GUIDE TO THE CSSLP

CSSLP – Certified Secure Software Lifecycle Professional

Jobs that Typically Use or Require the CSSLP

- » Application Security Specialist
- » IT Director/Manager
- » Penetration Tester
- » Project Manager
- » Quality Assurance Tester
- » Security Manager
- » Software Architect
- » Software Developer
- » Software Engineer
- » Software Procurement Analyst
- » Software Program Manager

Ref: (ISC)2 THE ULTIMATE GUIDE TO THE CSSLP

CSSLP – Certified Secure Software Lifecycle Professional

Pathway to CSSLP Certification

Obtain the Required Experience

To qualify for the CSSLP, candidates must have at least four years of cumulative, paid full-time work experience in one or more of the eight domains:

Domain 1. Secure Software Concepts

Domain 2. Secure Software Requirements

Domain 3. Secure Software Design

Domain 4. Secure Software Implementation
Programming

Domain 5. Secure Software Testing

Domain 6. Secure Lifecycle Management

Domain 7. Software Deployment, Operations,
and Maintenance

Domain 8. Supply Chain and Software Acquisition

ISACA

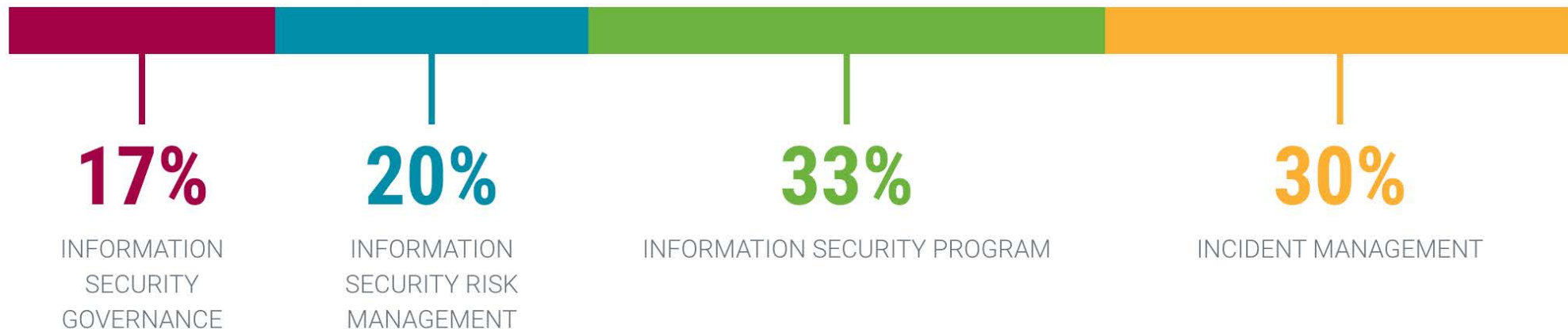
- CISM - Certified Information Security Manager
- CDPSE - Certified Data Privacy Solutions Engineer



CISM - Certified Information Security Manager

Review the CISM Exam Content Outline

CISM validates your expertise in the four work-related domains listed below that are applicable across industry verticals:



<https://www.isaca.org/credentialing/cism/cism-exam-content-outline>

Offensive Security

- OSCP - Offensive Security Certified Professional
- OSWE - Offensive Security Web Expert
- OSCE - Offensive Security Certified Expert



OSCP - Offensive Security Certified Professional

Who is this course for?

- Infosec professionals transitioning into penetration testing
- Pentesters seeking one of the best pentesting certifications
- Those interested in pursuing a penetration tester career path
- Security professionals
- Network administrators
- Other technology professionals

OSCP - Offensive Security Certified Professional

All students are required to have:

- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity with basic Bash and/or Python scripting

About the exam:

- 24-hour exam
- Proctored
- \$1599 USD

OSCP - Offensive Security Certified Professional

Penetration Testing with Kali Linux Syllabus

- | | |
|---------------------------------------|--|
| 1 Penetration Testing with Kali Linux | 14 Locating Public Exploits |
| 2 Getting Comfortable with Kali Linux | 15 Fixing Exploits |
| 3 Command Line Fun | 16 File Transfers |
| 4 Practical Tools | 17 Antivirus Evasion |
| 5 Bash Scripting | 18 Privilege Escalation |
| 6 Passive Information Gathering | 19 Password Attacks |
| 7 Active Information Gathering | 20 Port Redirection and Tunneling |
| 8 Vulnerability Scanning | 21 Active Directory Attacks |
| 9 Web Application Attacks | 22 The Metasploit Framework |
| 10 Introduction to Buffer Overflows | 23 PowerShell Empire |
| 11 Windows Buffer Overflows | 24 Assembling the Pieces: Penetration Test Breakdown |
| 12 Linux Buffer Overflows | 25 Trying Harder: The Labs |
| 13 Client-Side Attacks | |

<https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf>

OSCP - Offensive Security Certified Professional

Exam Structure You must achieve a minimum score of 70/100 points to pass the exam

60 points

3 independent targets

- 2-step targets (low and high privileges)
- Buffer Overflow may (or may not) be included as a low-privilege attack vector
- 20 points per machine
 - 10 points for low-privilege
 - 10 points for privilege escalation

40 points

2 clients

1 domain controller

- Active Directory set
- Points are awarded only for the full exploit chain of the domain
- No partial points will be awarded

<https://help.offensive-security.com/hc/en-us/articles/360040165632-OSCP-Exam-Guide>

OSWE - Offensive Security Web Expert

Syllabus

- 1 Cross-Origin Resource Sharing (CORS) with CSRF and RCE
- 2 JavaScript Prototype Pollution
- 3 Advanced Server-Side Request Forgery (SSRF)
- 4 Web security tools and methodologies
- 5 Source code analysis
- 6 Persistent cross-site scripting
- 7 Session hijacking
- 8 .NET deserialization
- 9 Remote code execution
- 10 Blind SQL injection
- 11 Data exfiltration
- 12 Bypassing file upload restrictions and file extension filters
- 13 PHP type juggling with loose comparisons
- 14 PostgreSQL Extension and User Defined Functions
- 15 Bypassing REGEX restrictions
- 16 Magic hashes
- 17 Bypassing character restrictions
- 18 UDF reverse shells
- 19 PostgreSQL large objects
- 20 DOM-based cross site scripting (black box)
- 21 Server-side template injection
- 22 Weak random token generation
- 23 XML external entity injection
- 24 RCE via database functions
- 25 OS command injection via WebSockets (black box)

<https://www.offensive-security.com/documentation/awae-syllabus.pdf>

OSWE - Offensive Security Web Expert

Exam Structure

You must achieve a minimum score of 85/100 points to pass the exam



<https://help.offensive-security.com/hc/en-us/articles/360046869951-OSWE-Exam-Guide>

GIAC - Global Information Assurance Certification



GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

GIAC - Global Information Assurance Certification

Areas Covered

- Network Attacks, Crypto, Network Booting, and Restricted Environments
- Python, Scapy, and Fuzzing
- Exploiting Windows and Linux for Penetration Testers

Who is GXPN for?


- Network Penetration Testers
- Systems Penetration Testers
- Incident Handlers
- Application Developers
- IDS Engineers
- Security personnel responsible for assessing target networks, systems and applications to find vulnerabilities

eLearnSecurity

- eMAPT - eLearnSecurity Mobile Application Penetration Tester
- eWPTXv2 - eLearnSecurity Web application Penetration Tester eXtreme
- eCXD - eLearnSecurity Certified eXploit Developer



[Thai]Cybersecurity supply/demand workers

JobsDB by SEEK

Job search

Profile

Career advice

Fresh Graduate

New

English

Login

For employers

Search

Salary

Job type

Date posted

Sort By Relevance

1-30 of 1,877 jobs



Penetration Tester / Pentester / Red Team/นักทดสอบเจาะระบบ
MAYASEVEN CO., LTD.

Huaykwang
THB 30K - 70K /month

- ได้เรียนรู้งานเจาะระบบจากทีมงานมืออาชีพระดับประเทศ
- สวัสดิการดีที่สุดในย่านตามความต้องการของพนักงาน
- โบนัสทุกปีตามผลงานและการประเมินผลงานที่เป็นธรรม

1d ago

Apply Now

View in new tab

Close



WORK WITH ETHICAL HACKERS
MAYASEVEN CO., LTD.

We have achieved the certification for ISO 9001:2015 and ISO/IEC 27001:2013 and have expanded our business to Southeast Asia.

LET'S MAKE*
THE WORLD MORE SECURE
[HTTPS://MAYASEVEN.COM/CAREER](https://mayaseven.com/career)



The Roadmap to Becoming A Penetration Tester



The Roadmap to Becoming A Penetration Tester

สำหรับใครที่อยากทำงานเป็นนักทดสอบเจาะระบบแต่ไม่รู้จะเริ่มศึกษาอะไร

จัดตามรายการได้เลยครับ 😊

1. OWASP Testing Guide

<https://owasp.org/www-project-web-security-testing-guide/>

2. Guideline for Penetration Testing

http://www.pentest-standard.org/index.php/Main_Page

3. OSCP-like materials

3.1. Hack The Box (Find OSCP like machines and Active Directory)

3.1.1 Consider reading the walkthrough of the retired machine to get the grip of the penetration testing method.

3.1.2 Or you can find the walkthrough video on the IppSec channel

(<https://www.youtube.com/c/ippsec/videos>)

<https://app.hackthebox.com/tracks/Active-Directory-101>

3.1.3 Hack the Box Academy: <https://academy.hackthebox.com/>

4. TryHackMe

<https://tryhackme.com/>

5. Burp Suite Web Security Academy

<https://portswigger.net/web-security>

<https://portswigger.net/web-security/all-materials>

<https://portswigger.net/web-security/all-labs>

<https://portswigger.net/web-security/learning-path>

6. Pentesterlab

<https://pentesterlab.com/>

7. vulnhub

<https://www.vulnhub.com/>

เรียนรู้เพิ่มเติม

1. <https://www.youtube.com/mayaseven>
2. <https://www.facebook.com/LifeAtMayaseven>
3. <https://www.facebook.com/mayase7en>

MAYASEVEN
4.33K subscribers

SUBSCRIBE

HOME VIDEOS PLAYLISTS COMMUNITY CHANNELS ABOUT

แท็กเว็บ Web Application Hacking and Ethical Hacker

Web Hacking

3,458 views • 3 years ago

เนื้อหาบางส่วนจากคอร์ส แท็กเว็บ Web Application Hacking and Ethical Hacker รายละเอียด : <https://mayaseven.com/product/%E0%B8%...>

Uploads PLAY ALL

ช่องโหว่ที่รุนแรงที่สุดเท่าที่เคยมีมา Log4j, Log4Shell
1.1K views • Streamed 2 months ago

Malware Analysis EP.3
1.1K views • Streamed 2 months ago

เส้นทางสู่นักทดสอบเจาะระบบ(Ethical Hacker) และสา...
3.6K views • 2 months ago

สรุป OWASP API Security Top 10 - 2019
2.5K views • 1 year ago

ช่องโหว่ Command Injection และวิธีป้องกัน | OWASP Top 1...
1K views • 2 years ago



MAYASEVEN

HACK THINGS

✉ info@mayaseven.com

📱 02-026-3231

🌐 <https://mayaseven.com>