



OffSec Cert : from 0 to 0.5

Jason3e7

[illegible]

Certifications ?

Earned 13 out of 16



Expires on 01/15/2028



Expires on 01/05/2028



Expires on 10/19/2027



Expires on 12/07/2027



Agenda

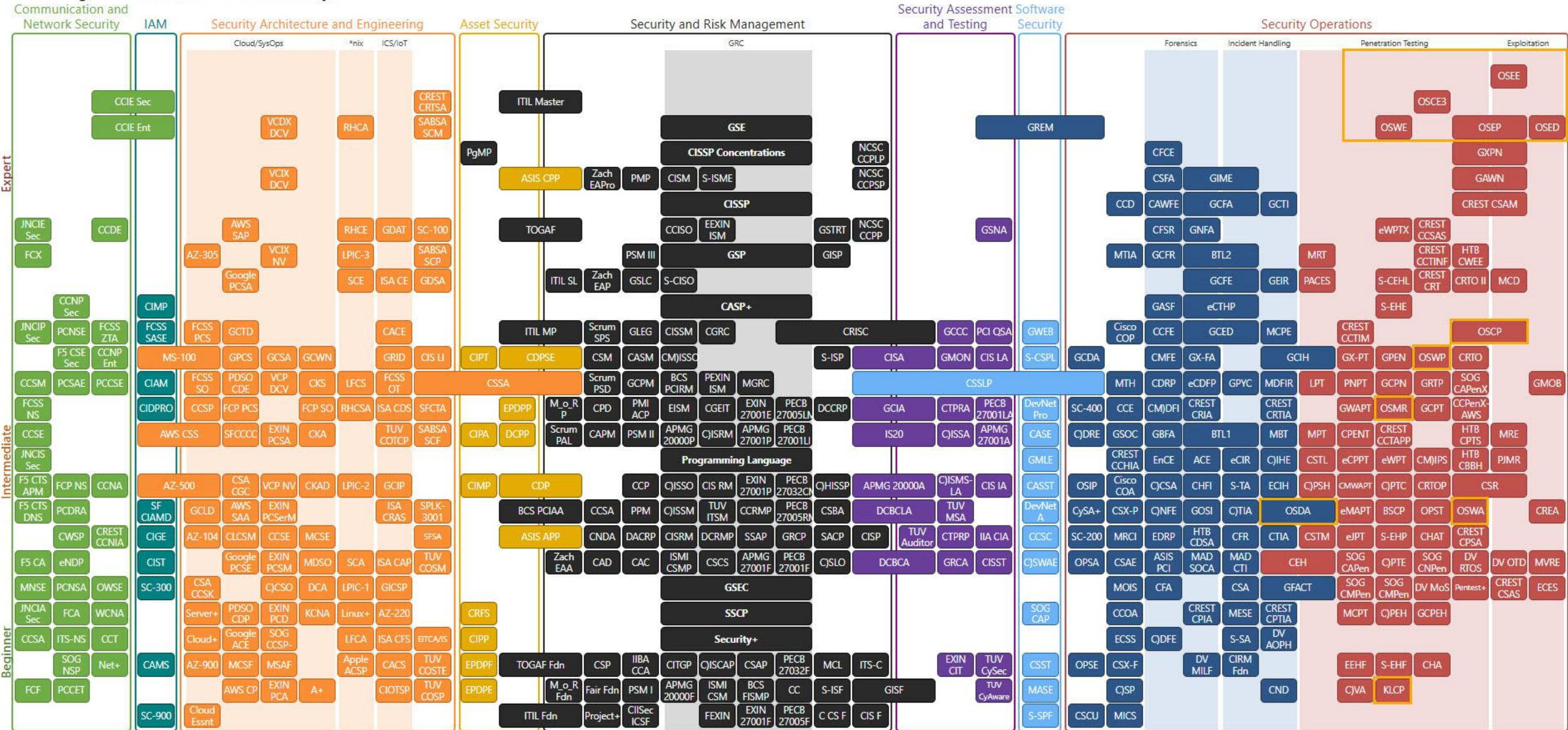
- 01 Why OffSec Certifications ?
- 02 What Are OffSec Certifications ?
- 03 How to Obtain OffSec Certifications ?
- 04 Takeaway



Why OffSec Certifications ?



Security Certification Roadmap



481 certifications listed | July 2024

2025

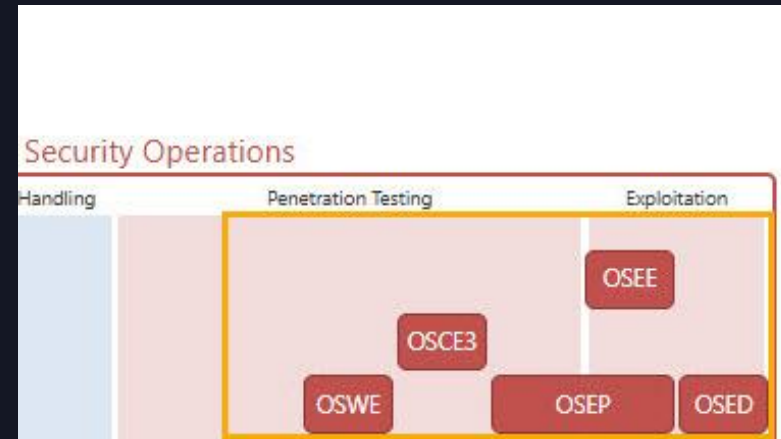
資通安全專業證照清單 (1140124修正)

9.	Offensive Security[9]		1. OffSec Certified Professional (OSCP) 2. Offensive Security Certified Expert (OSCE) 3. OffSec Wireless Professional (OSWP) 4. OffSec Exploitation Expert (OSEE) 5. OffSec Web Expert (OSWE) 6. OffSec Exploit Developer (OSED) 7. OffSec Experienced Penetration Tester (OSEP)
----	-----------------------	--	--



OffSec Certification Pros and Cons

- Security Certification Roadmap
- 資通安全專業證照清單 (1140124修正)
- Hands-on Practice, Hands-on Exam
- Mental Training



1. OffSec Certified Professional (OSCP)
2. Offensive Security Certified Expert (OSCE)
3. OffSec Wireless Professional (OSWP)
4. OffSec Exploitation Expert (OSEE)
5. OffSec Web Expert (OSWE)
6. OffSec Exploit Developer (OSED)
7. OffSec Experienced Penetration Tester (OSEP)



OffSec Certification Cons

Essential content



CyberCore™

\$899/year

Billed annually*

Buy now

Most popular



Course + Cert Exam Bundle

\$1,749

One-time payment

Buy now

Best value



Learn One

\$2,749/year

Billed annually*

Buy now

iPhone X^S

貴，從來都不是它的缺點，
而是你的缺點。

進一步了解 > 預購 >





OSCE³ers (動機篇)

- 學習不同思路
- 減少技術債，彌補技術缺漏部分
- 因為很酷，OSCP 就很有水準了，覺得 OSCE³ 應該更值得挑戰！
- 在高中時就決定將 OSCE³ 作為人生目標之一，也很幸運在大一時就達成了





Certifications ?

Earned 13 out of 16



Expires on 01/15/2028



Expires on 01/05/2028



Expires on 10/19/2027



Expires on 12/07/2027



level 100 x 3
level 200 x 6 + 1
level 300 x 4 + 1
level 400 x 1



New course! SJD-100: Secure Java Development Essentials

Build more securely from the start. Develop skills with hands-on training to identify and prevent common vulnerabilities in Java. A strong foundation in secure software development starts here.



Course Designation System



Difficulty:

- 100 - Essentials
- 200 - Foundational
- 300 - Advanced
- 400 - Expert

OS Designation:

- 0 - Multiple OS
- 1 - Windows
- 2 - macOS
- 3 - Linux





Requirement



的三張資安證照



https://speakerdeck.com/aifred0729_tw/nian-yi-lai-de-xin-lu-li-cheng

Certifications ?

Earned 13 out of 16



Expires on 01/15/2028



Expires on 01/05/2028



Expires on 10/19/2027



Expires on 12/07/2027



level 100 x 3

level 200 x 6 + 1

level 300 x 4 + 1

level 400 x 1



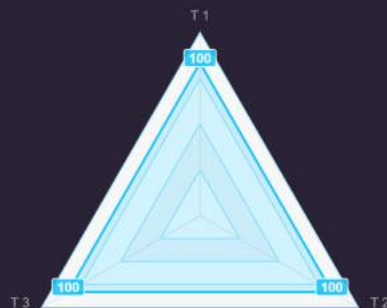
New course! SJD-100: Secure Java Development Essentials

Build more securely from the start. Develop skills with hands-on training to identify and prevent common vulnerabilities in Java. A strong foundation in secure software development starts here.



level 100

- OSCP SEC-100
 - 像是資安概論, 有實務的那種
 - 考試玩得蠻開心的
- KCLP
 - 選擇題, closed book exam
 - 專注於 Kali Linux 上
 - Learn One 方案包含
- OSCP SJD-100
 - Secure Java Development Essentials



Congratulations, Jun-Shen! You PASSED!

We are pleased to announce that you have passed the OSCP exam.

You may now generate your Digital Certificate in the OSCC exam tab.

Attempt status

Total number of points

Points scored

Percentage

TOPICS

1. Attack - 100%
2. Defend - 100%
3. Build - 100%



都沒有在資通安全專業證照清單上



level 100 x 3

level 200 x 6 + 1

level 300 x 4 + 1

level 400 x 1



New course! SJD-100: Secure Java Development Essentials

Build more securely from the start. Develop skills with hands-on training to identify and prevent common vulnerabilities in Java. A strong foundation in secure software development starts here.



level 200(Red Team)

- OSCP/OSCP+(PEN-200)
 - 經典, 內容既多且雜
 - 在資通安全專業證照清單上
- OSWP(PEN-210)
 - WPS
 - WPA-PSK
 - WPA-MGT
 - Learn One 方案包含, 目前可能無法單獨購買
 - 在資通安全專業證照清單上
- OSWA(WEB-200)
 - XSS(Cross-Site Scripting), lab
 - SQL injection, 4 types of database
 - XXE(XML eXternal Entity)
 - SSTI(Server-side Template Injection)
 - SSRF(Server-side Request Forgery)
 - 沒有在資通安全專業證照清單上



OSCP/OSCP+

- Before the OSCP exam(long term)
- Before the OSCP exam(short term)
- Doing the OSCP exam
- After the OSCP exam



Before the OSCP exam(long term)

Penetration Testing with Kali Linux

help.offsec.com/hc/en-us/sections/6970444968596-Penetration-Testing-with-Kali-Linux-PEN-200-

OffSec

OffSec Support Portal > Course Specific Resources for Offsec Students > Penetration Testing with Kali Linux (PEN-200)

Penetration Testing with Kali Linux (PEN-200)

Topic Exercises Hints FAQ

OffSec PEN-200 Learning Plan - 12 Week

OffSec PEN-200 Learning Plan - 24 Week

PEN-200 FAQ

OffSec Academy: PEN-200 FAQ

PEN-200 Onboarding - A Learner Introduction Guide to the OSCP

Topic Exercises FAQ

PEN-200 Training Library Lab Connectivity Guide

PEN-200: Penetration Testing with Kali Linux FAQ

OSCP Exam Guide

OffSec OSCP Exam with AD Preparation

PEN-200 Reporting Requirements

OSCP Exam FAQ

Learning Plan - 12 Week

Jump to Week: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Week 1

Overview and Study Approach

The first four topics serve as an introduction to the course material and provide a general approach to the course. We also recommend learners explore the following OffSec communication mediums:

- OffSec Help and FAQs: <https://help.offsec.com/hc/en-us>
- Discord: [How may I join the OffSec Community?](#)
- Youtube Channel: [@OffSecTraining](#)
- Twitch Channel: [@offsecofficial](#)
- Twitter: [@OffSecTraining](#)

Learning Topics

- 1) Penetration Testing with Kali Linux: General Course Information
- 2) Introduction To Cybersecurity
- 3) Effective Learning Strategies
- 4) Report Writing for Penetration Testers
- 5) Information Gathering
- 6) Vulnerability Scanning

- 6.2.1. Whois Enumeration
- 6.2.2. Google Hacking
- 6.2.3. Netcraft
- 6.2.4. Open-Source Code
- 6.3.1. DNS Enumeration
- 6.3.2. TCP/UDP Port Scanning Theory
- 6.3.3. Port Scanning with Nmap



Practice

- Not for the points, but for making sure you really learned it.

Bonus Points

Topic Exercises + 30 Lab Machines

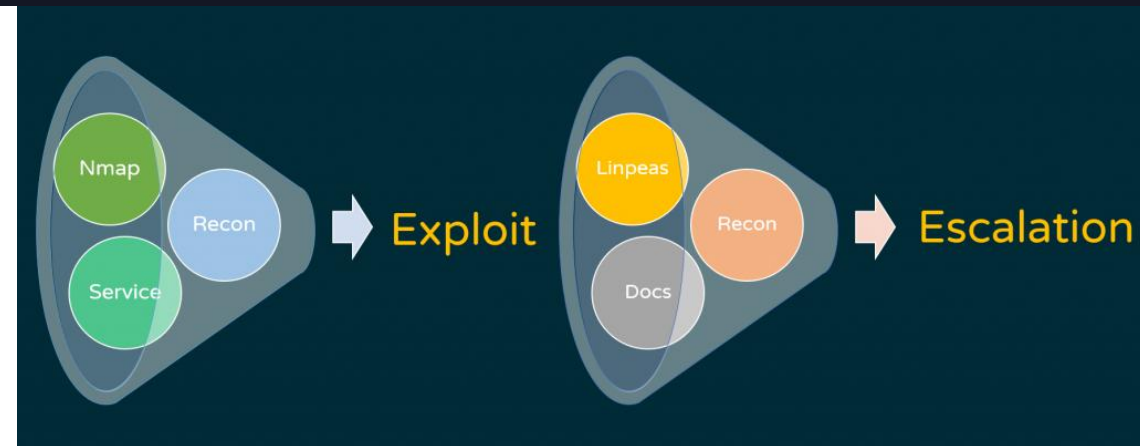
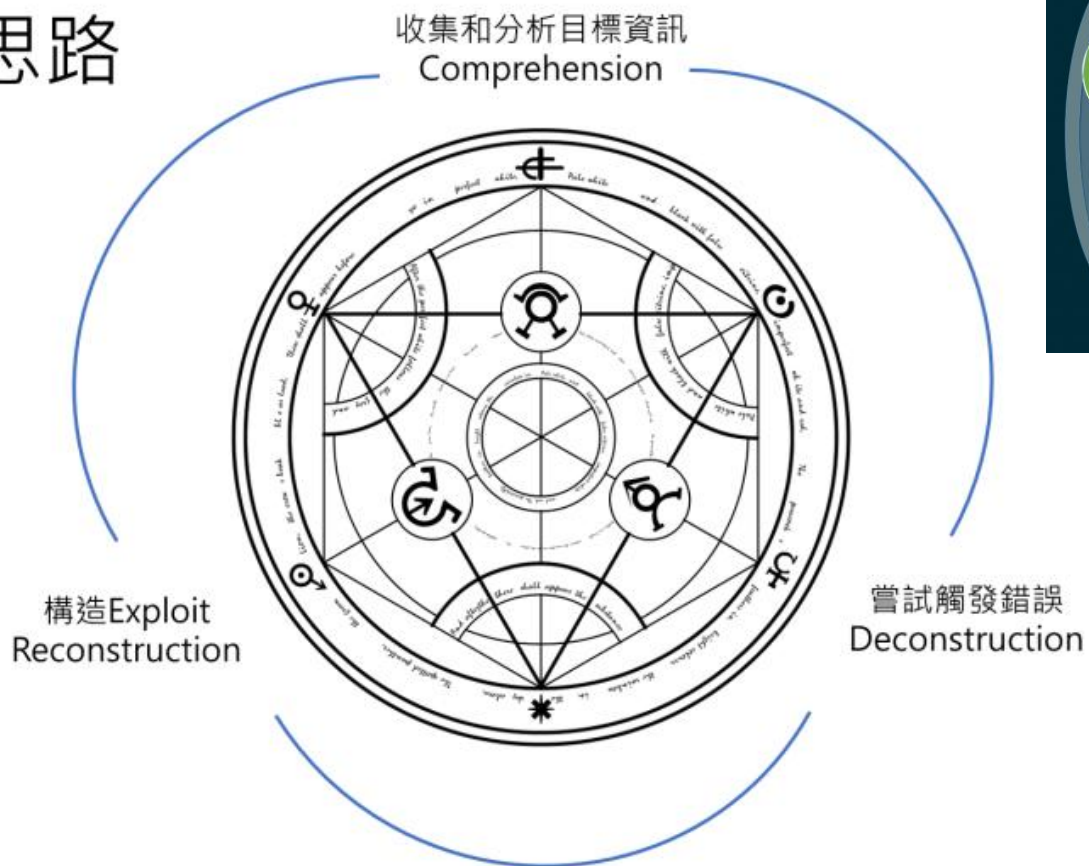
- In order to receive ten (10) bonus points, you must submit at least **80% of the correct solutions** for **topic exercises in every topic** in the PEN-200 course and submit **30 correct proof.txt hashes** in the OffSec Learning Platform.



OSCP+ 已經沒有 Bonus Points

How to do it ?

測試思路



Before the OSCP exam(short term)

- Weaknesses
- Booking exam and writing on calendar
- OSCP Exam Guide
 - Exam process
- Passport
- Janus WebRTC Extension



Offsec - Exam Page : OS-

Choose a course

You are viewing this exam calendar in time zone
Asia/Taipei.



A time of 0:00 on the scheduling form is the very beginning of that day, regardless of what order it is presented in the selection.

Course

Penetration Testing with Kali Linux

Exam Setting

Dear Student You have scheduled your challenge for
Sat, 04 Nov 2023, 06:00 (Asia/Taipei) .
You may not reschedule your exam within 48 hours of its scheduled start time.

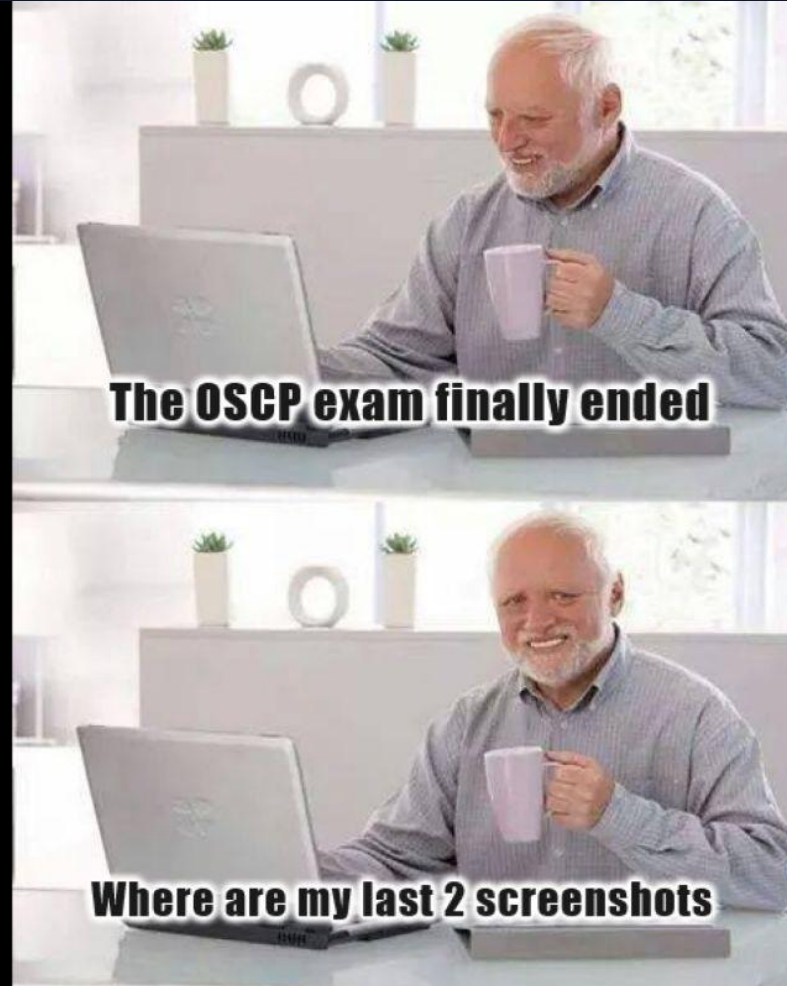
Please send an email to orders@offensive-security.com with any further questions.

Sincerely,

The Offsec Team

Doing the OSCP exam

- Take a break !
 - Body and Time management
- Monitors
- Screenshot
- Do math(solution)
- Try Harder
 - Persistent
 - Creative
 - Perceptive



After the OSCP exam

- Report
 - CH5 Report Writing for Penetration Testers
 - Exam Report Template
 - Offensive Security Exam Report Template in Markdown
- Do math(don't skip step)



After the OSCP exam

```
(kali㉿kali)-[~/OSCP-Exam-Report-Template-Markdown]
$ ruby osert.rb generate -i 20231105_oscp_coll/OSCP-exam-report-template_OS
_v2.md -o 20231105_oscp_coll
[+] Preparing your final report...
[+] Choose syntax highlight style [breezedark]:
0. pygments
1. tango
2. espresso
3. zenburn
4. kate
5. monochrome
6. breezedark
7. haddock
>
[+] Choose a Certification:
0. OSCP
1. OSPA
2. OSWE
3. OSCE
4. OSEE
5. OSWP
6. OSED
7. OSEP
8. OSDA
9. OSMR
> 0
[+] Enter your OS ID:
> OS-
[+] Generating report...
[+] PDF generated at 20231105_oscp_coll/OSCP-OS-Exam-Report.pdf
[+] Do you want to preview the report? [Y/n]
> n
[+] Generating archive...
[+] Do you want to add an external lab report? [Y/n]
> n
[+] Archive generated at 20231105_oscp_coll/OSCP-OS-Exam-Report.7z
[+] Calculating MD5 of the archive...
[+] Archive MD5 (upload integrity check): 5cbe2b5f-f989ff1c5
```



Time to rest

Upload your Exam/Lab report

upload.offsec.com



FILES SUBMITTED

Thank you for submitting your exam files.

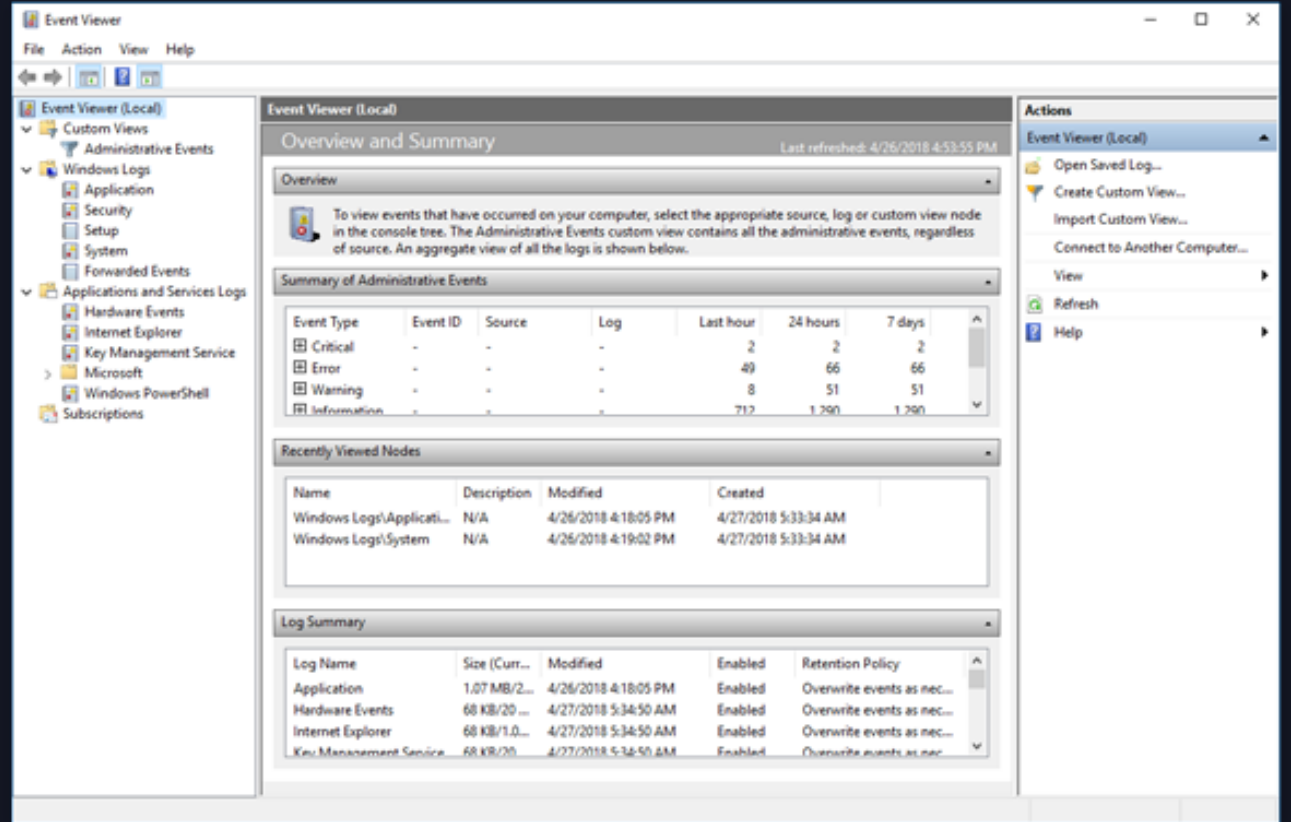
Once we review them and grade your exam, you will receive an email with your certification exam results (pass/fail) within ten (10) business days after submitting your documentation.

© 2020 Offensive Security | Privacy | Terms of service



level 200(Blue Team)

- OSDA(SOC-200)
 - ELK
 - bottom-up
 - 有 13 組 Lab, 對答案比較麻煩
- OTH(TH-200)
 - Splunk
 - top-down
 - 目前只有 1 組 Lab
 - 目前只有 7 個章節
- OSIR(IR-200)
 - Splunk
 - bottom-up
 - 目前只有 1 組 Lab
 - Log 會有雜訊的考驗



都沒有在資通安全專業證照清單上

Certifications ?

Earned 13 out of 16



Expires on 01/15/2028



Expires on 01/05/2028



Expires on 10/19/2027



Expires on 12/07/2027



level 100 x 3
level 200 x 6 + 1
level 300 x 4 + 1
level 400 x 1



New course! SJD-100: Secure Java Development Essentials

Build more securely from the start. Develop skills with hands-on training to identify and prevent common vulnerabilities in Java. A strong foundation in secure software development starts here.



OSMR 目前已經沒有線上 Lab, 環境有教但要自行架設



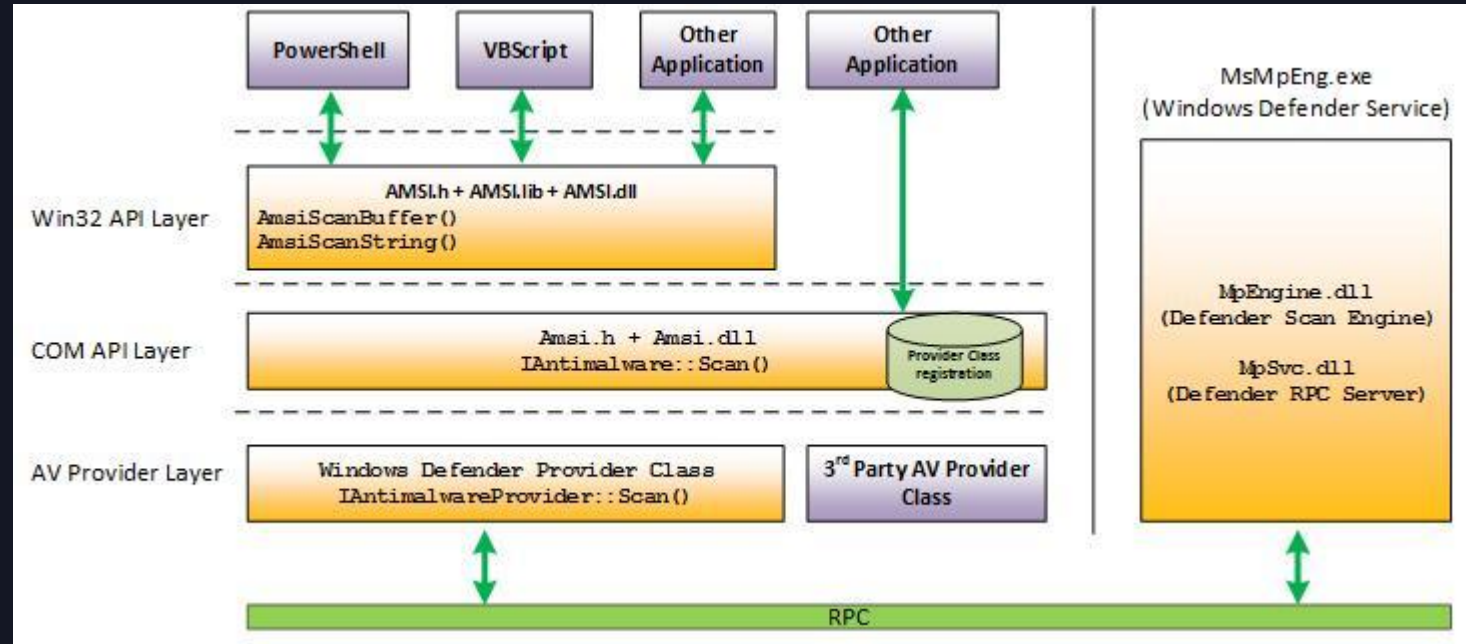
OSWE (WEB-300)

- 建議基礎技能
 - OWASP Top 10 實務能力
 - 有能力閱讀 2 種以上 web 開發程式語言
- 認證核心技能
 - Java/PHP/.NET
 - Environment Setup(非必要但很有用)
 - Code Review
 - Web Program Interruption
 - Exploit Script



OSEP (PEN-300)

- 建議基礎技能
 - OSCP 實務, 打靶機的能力
- 認證核心技能
 - OSCP 加強版
 - Lateral Movement 加強版
 - Antivirus Evasion(Microsoft)
 - Microsoft Office Fishing
 - Microsoft Defender
 - UAC bypass
 - AMSI bypass



OSD (EXP-301)

- 建議基礎技能
 - x86 組合語言
 - Operating System
 - Process, Memory 基本運作原理
- 認證核心技能
 - WinDbg
 - shellcode from zero to one
 - ROP(Return-Oriented Programming)
 - DEP bypass
 - ASLR bypass

請用 **Shellcode** 寫出這段程式碼



system("/bin/sh")

push rax

```
mov rax, "/bin/sh"
```

systemcall

```
xor rsi, rsi
```

```
xor rdx, rdx
```

```
mov rdi, rsp
```

```
mov rax, 0x3b
```



OSCE³ers (準備篇)

- 紅隊思維就像藝術，我們不只學習技術，我們也培養直覺
- 直接報名下去，不要總是說沒時間，時間是擠出來的，死到臨頭就會激發出潛能，Try Harder !
- OSED 組語
- OSWE Java/PHP/.NET 選一個框架搭設測試開發環境 並實際下斷點觀察程式流程
- OSEP 架設熟悉 AD 環境



level 400



EXP-401

LIVE Training: Advanced Windows Exploitation (AWE)

OSEE Certification

NT\$369,000 / USD\$11,300

Aug. 18 - Aug. 22, 2025

iPhone X^S

貴，從來都不是它的缺點，
而是~~你~~的缺點。

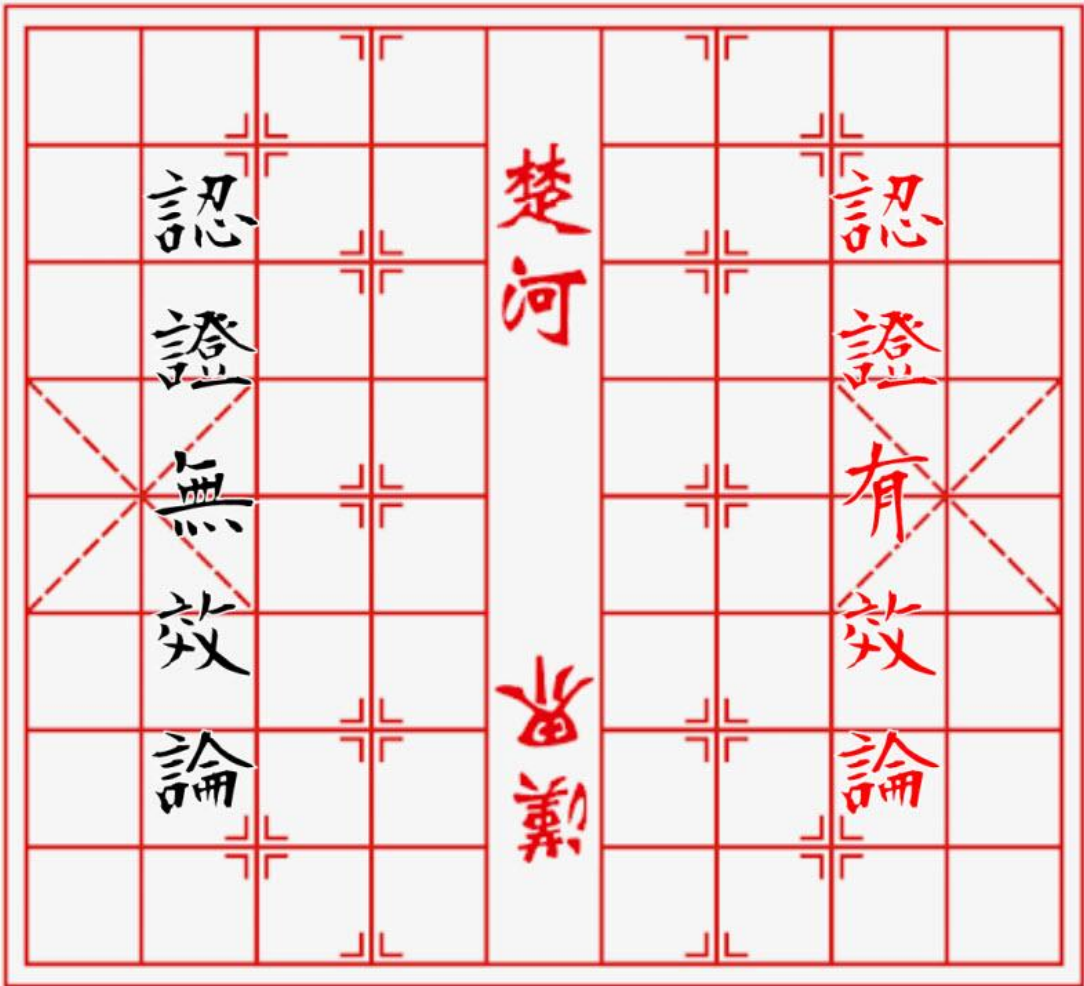
進一步「解」 > 預購 >



64-bit kernel exploitation



追求安全是目標



OSCP OSWE OSCE
OSWP OSEE OSED OSEP
OSCE3 CISSP
CPENT CEH ESCA
Certificated

A hacker who
have a pet cat



CYBERSEC 2024 臺灣資安大會 | 3



<https://cybersec.ithome.com.tw/2024/session-page/2898>

<https://www.facebook.com/10sec.tw>

For What !?

- 職涯發展
 - 入職
 - 升遷
 - 接案
- 自我實現
- 挑戰難題
- Hands-on Skill
- Mental Training
- ...etc



Change

- From OSCP to OSCP+
 - Enhancements Active Directory Exam
 - Removal of bonus points
- New OffSec Certifications Expire After 3 Years
 - OSCP+, OSIR, OSTH, OSCE
- Learn Unlimited cooling off periods
 - Ex : 1st failed exam: 2 weeks -> 4 weeks
- 04/09 OffSec Annual Membership live
 - CPE program

會持續成長
的證照

會持續花錢
的證照



Takeaway



Try Harder: From Mantra to Mindset

- Persistent, **Try Again**
 - When we feel like we've hit a brick wall, stepping away for a moment and taking a break is usually the best advice.
- Creative, **Try Differently**
 - Outside the box.
- Perceptive, **Try Smarter**
 - Making time to step back and actively assess a situation is critical to being able to make good decisions.



Takeaway

- Try Harder 實務, 不僅僅是個口號
- For What, 找到你的起心動念
- 教學相長, 一群人走的遠



推動台灣專業知識價值的正循環



<https://conf.devco.re/2025/>



Thanks

- 兩位師傅
- TeamT5 小夥伴
- 資安圈 夥伴
- 感謝各位聽眾, 知識的傳承, 我的旅程也從 to 0.5 -> to 0.9



zha0

TeamT5 杜浦數位安全

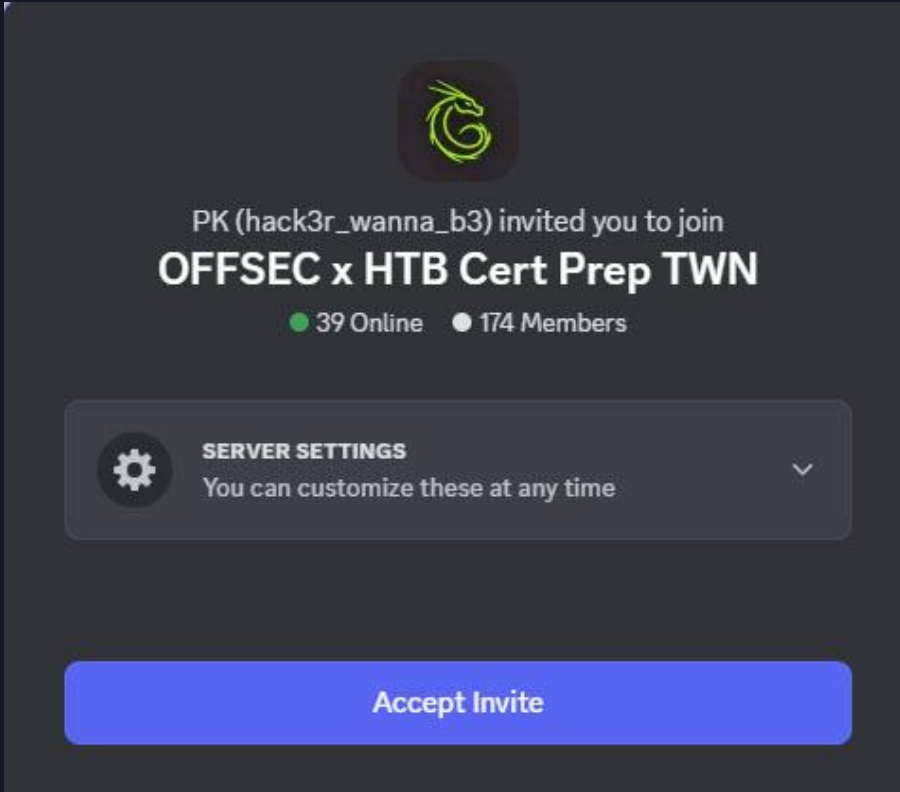


盜賊

- CARLOS



OFFSEC x HTB Cert Prep TWN(協助推廣)



CYBERSEC 2025
臺灣資安大會

4.15 Tue - 4.17 Thu
南港展覽二館 1 樓



威脅三振出局
防守無懈可擊



BALLS	攤位編號			OUTS
●●●				○○
Q	1	1	2	



TEAMT5



Q&A



Appendix



OffSec 證照通過者(動機篇)

- 了解紅隊攻擊手法
- 自我挑戰以及接案需求
- 因為覺得攻擊方面的了解有助於藍隊調查
- 目前從事藍隊的工作，想透過學習攻擊者的思維及手法，增加防禦的思路及廣度
- 原因有二，一是想精進自己，二是工作上要承接新的任務，OSCP是門檻
- 因為想讓自己變得更優秀，OSCP是一門有系統的打底證照，當地基穩了，可以在有一定基礎下，一路往上走。



OffSec 證照通過者(動機篇)

當初剛好同事有揪OSCP讀書會，也加上本身對這張證照有興趣

除了想證明自己實力

也想得到要考取這張證照的成就感

畢竟是純上機考試，考試的LAB也是不固定(意思是通常你抽到的機器不太會跟別人一樣)

而且對於不管工作還有個人技能都對我來說幫助非常大



OffSec 證照通過者(準備篇)

- 多練習官方的靶機
- 多練習 Offsec 官方 Lab 提供的靶機
- 真的要先看 OSCP 課程後再去亂打 lab，方向會明顯很多，之後就要多打靶機繼續熟悉
- 小白可以直接先讀OSCP提供的完整教材培養基礎，教材讀完後就是透過大量的靶機練習增加實戰經驗
- 不正經的回答：找到好的前輩(x；正經的回答：課程認真上，買proving ground認真做30天，至少intermediate要可以在4小時內解掉
- Anonymous X
 - 建議報名OSCP課程前，先練習HTB靶機一段時間後再報名課程，可參考以下連結清單：
 - Lainkusanagi OSCP Like
 - https://docs.google.com/spreadsheets/d/18weuz_Eeynr6sXFQ87Cd5F0sI0j9Z6rt/edit?gid=487240997#gid=487240997
 - 妥善規劃時間是很重要的，網路上有很多學習資源，但還是做好自己的筆記和融會貫通整門課程內容。
 - 可以和同事朋友組讀書，可以彼此增進讀書學習動力，另外也可以向他人學習其思維模式，察覺自我不足之處。



OffSec 證照通過者(準備篇)

建議把Offsec Pen-200 的訓練課程給的練習做好
OSCP的90天課程老實說蠻有系統性的
學習的也是偏比較全面的滲透測試的基礎
也順便讓自己的思考方式可以想更多不一樣的層面
彌補一些平常不會特別想到的點或是利用方式



OffSec 證照通過者(收穫篇)

- 有挑戰OSCP的人都是戰士
- 看事情的邏輯會有一點落差，不會太表面，比較會out of box思考
- 一直覺得攻防是一體兩面的，當越了解攻擊手法，就越能知道和完善如何進行偵測和防範，在既有的認知下，可以多學習其他優秀者的攻擊手段，擴長自己的知識庫，並運用在生活和工作上。
- 加深對攻擊者思維的理解，在工作上有助於分析攻擊手法
- 第一點(增加防禦的思路及廣度)不僅僅是考完後，而是在學習中就已經有明顯的感受
- 有比較了解自己調查的東西，可以有更多的聯想 (以攻擊者思維去找可能使用的方法、等等)



OffSec 證照通過者(收穫篇)

我是6台機器全Pwn的人 (小炫耀一下)

這部份算蠻自豪的XDD

尤其AD這個部份讓我成長很多

剛好公司同事有部門專門在研究AD

好幾次讀書會都有分享AD的打法還有原理

實際考試反而不會到太難

就是有些細節要特別去注意(藏帳密之類的)

再來就是 Try Harder 的部份，也是offsec的精神

不管怎樣不要放棄其中一個細節而且去嘗試

魔鬼就藏在細節裡!

也幫助我在工作中不管Debug或是實際案例都很有幫助

