關於開展網絡安全工程師——網絡與系統安全認證培訓的通知

各位專業人士：

為助力香港地區網絡安全專業人才掌握實戰攻防技能、提升職業競爭力，並銜接北京地區之認證與人才政策，現正式推出「網絡安全工程師——網絡與系統安全認證培訓」。本課程涵蓋初級與中級內容，統一培訓結束後將進行統一考核，考核結果合格者，根據學員條件，依據《HKCSA-00 網絡安全工程技術人才專業能力評價規範》進行評定，分別頒發初級或中級證書。該證書與北京網絡空間安全協會頒發之同級職稱證書互認（中國大陸境內考生不適用此互認政策）。取得初級證書的考生，當條件達到中級後可免考試申請中級。

課程以紅藍對抗實戰為核心，旨在培養攻防兼備的實戰型安全專家。歡迎各位專業人士踴躍報名，共同提升實戰能力，拓展職業發展空間！相關事項通知如下。

一、培訓對象

1. 網絡安全工程師、滲透測試工程師；
2. 系統管理員、運維安全人員；
3. 企業藍隊／安全營運中心（SOC）成員；
4. 有意向從事紅藍對抗與溯源分析的技術人員。

二、培訓形式

1. **理論精講＋實操演練**：每個知識點都配套靶場實戰，從「懂原理」到「會操作」，每節課都能上手驗證攻防效果。

2. **紅藍對抗實景模擬**：學員分組扮演紅隊（攻擊方）與藍隊（防禦方），還原真實網絡安全戰場，在實時攻防中感受「攻擊的緊張」與「防守的緊迫」。

3. **案例覆盤＋思路拆解**：每輪對抗後集中覆盤，紅隊拆解攻擊路徑與漏洞利用技巧，藍隊分享溯源過程與應急處置經驗，雙向視角互補提升。

4. **問題導向教學**：以真實業務漏洞和攻擊場景為切入點，用「如何突破？如何防守？如何溯源？如何加固？」的問題驅動學習，聚焦解決實際工作痛點。

三、課程特色

1. 全程基於授權靶場，每人分配獨立靶機；

2. 強調「攻防一體」，既學攻擊手法，更重防禦與溯源；

3. 每輪對抗後均有覆盤環節，提升實戰反思能力；

4. 內容緊扣企業真實業務場景，提升崗位適用性。

四、培訓時間和地點

1. **培訓時間**：2026 年 7 月 18-19 日、25-26 日，共 4 天（含考核）。

2. **培訓地點**：线上直播线下面授同步，线下具体培訓位於香港地區，报名后另行通知。

五、培訓收益

1. **獲取國際職業資格認證**

學員通過考核並符合《HKCSA-00 網絡安全工程技術人才專業能力評價規範》要求的，將獲得由香港網絡空間安全協會頒發的「網絡安全工程師認證證書（初級或中級）」。該證書已納入北京市人力資源和社會保障局、北京市人才工作局的《國際職業資格清單》和《國際職業資格互認清單》，並與北京網絡空間安全協會的評價標準及證書實現互認，具備高度的行業公信力與國際流通性。

2. **對接北京人才政策，開啟職業發展新通道**

根據北京市人力資源和社會保障局、北京市人才工作局最新聯合發佈的《北京市國際職業資格認可目錄（2025 年版）》（京人社事業發〔2025〕11 號），持有該《國際職業資格清單》內證書並與在京單位建立人事勞動關係的人員，可享受一系列人才便利化服務，包括但不限於：

中國籍人員：可納入北京市工作居住證辦理範圍；

職稱認定與晉升：部分職業資格可對應具備相應系列（專業）中級職稱，並可作為申報北京市高級職稱的條件；

技能等級認定：部分資格可對應核發相關職業技能等級證書，並享受技能人才培養相關政策；

外籍人員便利：可辦理有效期 5 年以內的多次簽證或居留許可，符合條件的納入永久居留便利通道；辦理工作許可條件大幅放寬（如年齡、學歷限制等），符合條件者可獲發 5 年期證件；

經歷認可與綜合保障：境外從業經歷可視同境內經歷，並在創新創業、子女入學、社會保障等方面獲得支持。

3. **增強核心競爭力**

無論學員計劃前往北京發展，還是在香港或國際舞台深耕，此認證均能顯著提升其個人專業資質，在重大項目參與、職位晉升、跨域合作中佔據優勢。

4. **享受會員待遇**

可申請成為北京網絡空間安全協會學術會員，享受會員在京的便利服務。

六、培訓費用

XX 港元 / 人（含培訓費、教材費、實驗環境使用費及認證考試費）。

七、報名方式

歡迎企業或個人報名。請掃描二維碼，按附件報名表填寫相關資訊，或發送郵件至 cyberspacehk@163.com。

諮詢電話：成老師 15360402627（微信同號）、陳老師 1598929645（微信同號）

附件

1. 網絡安全工程師認證培訓課程表
2. 網絡安全工程師認證培訓（網絡與系統安全）報名表
3. 證書樣本
4. 《HKCSA-00 網絡安全工程技術人才專業能力評價規範》

香港網絡空間安全協會

2026 年 4 月 27 日

附件 1：網絡安全工程師認證培訓課程表

核心主題	培訓內容要點	實戰聚焦
第一天（主機系統溯源分析——筑基篇）	1. 系統隱患排查實操：系統資訊深度探查、磁碟空間異常定位、異常進程精準查找、進程資源佔用分析。 2. 安全溯源與加固實操：網絡／路由／用戶資訊排查、異常檔案/Rookit 查殺、Linux 後門（SSH 軟連結／計劃任務／自啟動項等）原理與排查；歷史命令／登錄日誌排查；密碼策略設置、SSH 安全配置（禁止 root 遠程登錄、登錄失敗鎖定）、服務與中介軟體加固。 **思考：**當伺服器被入侵，你能從這些痕跡中鎖定攻擊者嗎？	-快速定位 CPU 飆升的「真兇」 -Linux 安全加固，抵禦常見攻擊
第二天（電子商務系統紅藍對抗——實戰篇）	**紅隊攻擊實操路徑：** 1. SQL 注入漏洞利用→獲取管理員密碼並破解→上傳小馬→提權→反向連接→植入內核級 Rootkit。 2. XSS 多種方式利用→新增後台帳號或釣魚獲取密碼→登錄後台植入 WebShell。 3. CSRF 攻擊植入後門檔案。 **藍隊即時回應實操：**監控系統異常流量→分析入侵痕跡（日誌／進程／檔案）→定位攻擊入口→清除惡意檔案→加固漏洞。 **思考：**程式漏洞如何成為攻擊的「突破口」？攻擊正在發生時，你能快速「止損」嗎？	-利用 SQL 注入獲取電商後台管理員權限 - 用 XSS 釣魚獲取電商管理員密碼 -從日誌中還原紅隊攻擊路徑
第三天（跨業務場景滲透與溯源——進階篇）	**紅隊迂迴攻擊實操：** 1. 社工收集 A 公司與服務商 B 公司關聯資訊→滲透 B 公司業務系統→網站掛馬控制 A 公司內網終端→搭建 80/443 Webshell 隧道→竊取 B 公司業務數據。 2. 紅隊如何繞開目標的防禦，迂迴攻擊如何實現？ **藍隊全鏈路溯源實操：** 1. 分析 B 公司伺服器被控制的關鍵漏洞→追蹤終端被入侵的痕跡→還原代理搭建與數據竊取過程→出具溯源報告與防禦方案。 2. 藍隊如何溯源分析伺服器痕跡、終端電腦被種植木馬的各種異常？ **思考：**面對跨業務攻擊，你能理清完整「攻擊鏈」嗎？	- 通過掛馬獲取內網終端控制權 - 撰寫完整的跨場景攻擊溯源報告

第四天（多輪次紅藍對抗——強化篇）	**紅隊攻擊實操場景：** 1. 資訊收集（伺服器埠 / 服務探測、網站後台定位）→漏洞掃描與驗證→利用常規漏洞登錄後台→後台與系統漏洞聯動→反向連接→提權獲取 root。 2. 精準探測（聚焦檔案上傳 / 命令執行漏洞）→突破後台權限限制→利用操作系統高危漏洞提權。 3. 探測小眾漏洞→迂迴突破後台→建立隱蔽控制通道。 **藍隊溯源實操場景：** 1. 實時監控伺服器狀態→排查異常進程 / 連接→定位後門檔案→快速處置漏洞。 2. 優化監控策略→針對高頻攻擊路徑設置防護規則→實時溯源攻擊鏈路。 3. 覆盤前兩輪短板→完善防禦體系→快速定位漏洞攻擊痕跡。 **全維度數據流溯源實操：** 1. 以四天對抗為背景，還原紅隊打點突破全過程。 2. SQL 注入 / XSS 攻擊的數據包特征藏在何處？後門檔案上傳的數據包痕跡如何識別？暴力破解的數據包有哪些典型規律？內網哪台機器先成為跳板？紅隊又探測到了哪些內網伺服器及對外埠？ **HTTPS 安全加固與驗證實操：** 1. 針對紅隊攻擊暴露的傳輸層隱患，配置 HTTPS 加密、證書部署、安全協議優化、防劫持策略。 2. HTTPS 加固能抵禦哪些攻擊？如何驗證加固效果是否達標？HTTPS 典型的部署漏洞是怎麼被利用的，原理是什麼？ **考核**	- 紅隊：通過後台+系統漏洞組合拿下 root - 藍隊：20 分鐘內清除後門並封堵漏洞 - 紅隊：利用檔案上傳漏洞結合提權拿下目標 - 藍隊：精準阻斷惡意上傳行為並溯源 - 紅隊：利用小眾漏洞建立持久控制 - 藍隊：從日誌碎片中追蹤漏洞攻擊痕跡
備註	課程安排可能會根據實際情況有所調整。	

附件 2：網絡安全工程師認證培訓（網絡與系統安全）報名表

一、基本資訊

項目	填寫內容
姓名	
性別	□ 男　□ 女
聯絡電話	
電子郵箱	
所在單位 / 學校	
職務 / 專業	
工作年限	□ 1 年以下　□ 1-3 年　□ 3-5 年　□ 5 年以上
是否需要企業發票	□ 是（抬頭：_____ 納稅人識別號：_____） □ 否
報名類型	□ 個人報名　□ 企業團報（人數：___人）
支付方式	□ 銀行轉帳　□ 支付寶　□ 微信支付　□ 信用卡

二、技術背景（可多選）

類別	掌握程度（請勾選）
操作系統	□ Linux 基礎　□ Windows Server　□ 其他：_____
網絡基礎	□ TCP/IP 協議　□ 路由交換　□ 防火牆配置
安全技能	□ 滲透測試基礎　□ 漏洞掃描　□ 日誌分析　□ 應急回應
編程 / 腳本	□ Python　□ Shell　□ 其他：_____
是否參與過紅藍對抗	□ 是　□ 否

附件 3：

<網絡安全工程師認證證書>

Certified Cyberspace Security Engineer

證書編號:HKCCSEBSAS202512001

Certification No.

姓　　名
Name　　：[redacted]

專業方向:業務安全

Certification Specialization: Business Security

級　　別:高級工程師

Level　　: Senior Engineer

茲證明，上述人員已符合《網絡安全工程技術人員職業能力評價規範》相關要求，特授予其高級工程師任職資格。

It is certified that the above-named person has met the requirements of *Professional Competency Assessment Specification for Cybersecurity Engineering Technical Personnel* and is admitted as Senior Engineer.

本證書的有效性還需依據發證機構的年度監督獲得維持，可登錄香港網絡空間安全協會網站（www.hkinsa.hk）查詢或掃描下方二維碼查詢。

The validity of this certificate is subject to ongoing maintenance through the annual supervision by the issuing authority. To verify its status, please visit the website of the Hong Kong Cyberspace Security Association (www.hkinsa.hk) or scan the QR code below for further inquiry.

查詢二維碼

Dec 20, 2025

發證日期
Date of Issue

秘書長
Secretary General

香港網絡空間安全協會

Hong Kong Cyberspace Security Association