2025新課

UECR 企業網路靶場Cyber Range實機攻防演練課程

Enterprise Cyber Range Hands-on Workshop

時數：35小時 | 費用：60,000元 | 點數：18點 | 教材：恆逸自製教材

適合對象	對實機攻防操作演練有興趣者
預備知識	本課程為實機操作課程，需具備 Windows與Linux實機操作能力
課程內容	Part I：網路靶場環境介紹 1. 如何連接網路靶場 2. 如何連接靶場之防火牆與SIEM服務 3. 如何使用模擬攻擊 Part II：攻防演練矩陣介紹 1. ATT&CK矩陣 2. D3FEND矩陣 Part III：紅隊攻擊靶場實戰演練 1. Web攻擊之實戰演練 2. ATT&CK矩陣之實戰演練 3. AD攻擊之實戰演練 Part IV：藍隊防禦靶場實戰演練 1. D3FEND矩陣之實戰演練 2. AD防禦之實戰演練 3. 安全防禦之極限挑戰
備註事項	1. 報名課程贈送OffSec Cyber Range 2個月(價值超過USD 666，約台幣$20,000元，於開課日期起算) 2. 上過恆逸CPENT及OSCP者，報名再贈送$2,000元即享券

2025新課

Owasp OWASP開發者相關通用資安知識實戰演練

Practical Drill on Common Information Security Knowledge for OWASP Developers

時數：14小時 | 費用：12,000元 | 點數：3點 | 教材：恆逸專用教材

適合對象	1. 網頁與API開發人員 2. 專案經理、專案主管 3. 系統架構師
預備知識	1. 網路基本概念 2. Http基本概念 3. Linux基本操作 4. 由於和網頁有關，對JavaScript有基本認識者佳
課程內容	1. OWASP 2021 top 10 1.1 A01 Broken Access Control(權限控制失效) 1.2 A02 Cryptographic Failures(加密機制失效) 1.3 A03 Injection(注入式攻擊) 1.4 A04 Insecure Design(不安全設計) 1.5 A05 Security Misconfiguration(安全設定缺陷) 1.6 A06 Vulnerable and Outdated Components(危險或過舊的元件) 1.7 A07 Identification and Authentication Failures(認證及驗證機制失效) 1.8 A08 Software and Data Integrity Failures(軟體及資料完整性失效) 1.9 A09 Security Logging and Monitoring Failures(資安記錄及監控失效) 1.10 A10 Server Side Request Forgery (SSRF)(伺服端請求偽造) 1.10.1 Spring Boot中相關的應變 1.10.2 1.10.2 其餘框架的相關說明 2. OWASP API top 10 2.1.API1:2023 Broken Object Level Authorization(失效的物件階層授權控制) 2.2.API2:2023 Broken Authentication(失效的認證) 2.3.API3:2023 Broken Object Property Level Authorization(失效的物件) 2.4.API4:2023 Unrestricted Resource Consumption(未管控的資源消耗) 2.5.API5:2023 Broken Function Level Authorization(失效的函數階層授權) 2.6.API6:2023 Unrestricted Access to Sensitive Business Flows(未控管機敏商業流程控管) 2.7.API7:2023 Server Side Request Forgery(伺服器端請求偽造) 2.8.API8:2023 Security Misconfiguration(安全性的錯誤配製) 2.9.API9:2023 Improper Inventory Management(不適當的倉儲管理) 2.10.API10:2023 Unsafe Consumption of APIs(不安全的API使用) 3. 相關的工具與Kali Linux設定介紹 4. 案例介紹
後續推薦課程	AppSec： Mobile App Security資訊安全程式實作演練-通訊與資料儲存的安全

GPTEH 掌握ChatGPT進行道德駭客攻擊和滲透測試

Master ChatGPT for Ethical Hacking and Penetration Testing

時數：7小時 | 費用：9,000元 | 點數：2.5點 | 教材：恆逸專用教材

適合對象	1. 想要學習活用ChatGPT進行網路攻防演練的資安從業人員 2. 具備基本滲透測試技術能力的資安從業人員與網路工程師
預備知識	1. 具備基本滲透測試技術能力 2. 已取得網路工程師、資安相關認證者 3. ChatGPT基礎概念與使用能力
課程內容	1. 道德駭客基礎知識 2. 了解ChatGPT的優點和局限性 3. 在滲透測試平台中整合ChatGPT 4. 使用ChatGPT進行偵察和掃描 5. 使用ChatGPT執行密碼破解和暴力攻擊 6. 使用ChatGPT執行SQL注入和XSS 7. 使用ChatGPT進行進階漏洞利用開發 8. 相關實作演練
備註事項	課程優惠方案： 學生優惠價：參加校園IT職涯學習護照方案，享有5折優惠價NT$4,500元
後續推薦課程	CEH：EC-Council CEH駭客技術專家認證課程

SRAMT 資訊安全分析實務-方法、流程與工具

Information Security Implement-Methadology and Tools

時數：35小時 | 費用：28,000元 | 點數：7點 | 教材：恆逸專用教材

適合對象	1. 想要學習資安實用操作技巧的IT人員 2. 對系統的資安有興趣管理，希望能加強實作技巧的IT人員
預備知識	1. TCP/IP網路通訊協定 2. 已取得微軟Windows MCSA認證、紅帽RHCE認證之工程師，或具備網路基本架構概念者 3. 資訊安全基礎概念
課程內容	1. 評估系統的資訊安全 2. 評估流程與相關工具 3. 列舉與入侵系統的參考步驟 4. 駭客的矛盾對決 5. 探索與測試 6. 常見服務檢測：電子郵件伺服器 7. 常見服務檢測：網站伺服器 8. 常見服務檢測：搭配伺服器加密需求TLS 9. 跡證保存與警報系統 10. 備份與復原 11. 標準化建立系統與弱掃零檢出 12. 相關實作演練
後續推薦課程	CHFI：EC-Council CHFI資安鑑識調查專家認證課程

SECTMK 資通安全法令遵循實務

Cyber Security Law Compliance

時數：14小時 | 費用：20,000元 | 點數：5點 | 教材：恆逸專用教材

適合對象	法務人員、IT人員、資安人員、稽核人員
預備知識	具備基礎資安管理能力
課程內容	1. 資通安全現況 2. 資通安全事故案例研析 3. 資通安全法律規範 – 刑法妨害電腦使用罪章 4. 資通安全法律規範 – 個人資料保護法 5. 資通安全法律規範 – 資通安全管理法 6. 資通安全技術面應用 7. 資通安全管理面設計 8. 資通安全法令遵循執行策略與方法
備註事項	課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價
後續推薦課程	CEH：EC-Council CEH駭客技術專家認證課程

SONDRA 安全最佳化-網路設備與遠端存取

Security Optimization：Network Device and Remote Access

時數：21小時 | 費用：32,000元 | 點數：8點 | 教材：恆逸專用教材

適合對象	1. 想要學習網路安全實用技術的IT人員 2. 想要了解設備與遠端存取安全作業標準的資安管理員 3. 需要管理交換器、路由器、遠端桌面、遠端存取安全的IT人員
預備知識	1. 了解網路架構、並具備Cisco IOS基本操作能力 2. 熟悉Windows與Linux系統、網路基本管理 3. 網路安全基本概念
課程內容	1. 網路安全，縱深防禦(defense-in-depth) 2. 管理與實作二層交換器安全基準線 3. 運用與實作802.1X 4. 管理與實作路由器安全基準線 5. 使用Playbook集中管理網路設備安全 6. 管理與實作VPN Tunnel安全 7. 管理與實作Linux SSH Tunnel安全 8. 管理與實作遠端桌面(RDP)安全 9. 使用遠端桌面閘道(RDS GATEWAY)，強化遠端桌面安全 10. 強化遠端管理(ssh)安全 11. 集中管理設備驗證、授權與稽核
後續推薦課程	SRAMT：資訊安全分析實務-方法、流程與工具

AppSec Mobile App Security資訊安全程式實作演練-通訊與資料儲存的安全

Mobile App Security for Communication and Data Storage

時數：14小時 | 費用：20,000元 | 點數：5點 | 教材：恆逸專用教材

適合對象	1. 已完成Android或iOS行動裝置應用系統課程者，或具備基本App觀念與關聯式資料庫、網路存取的學員 2. Android方面需對Activity生命週期與Java語法有基礎認識 3. iOS方面需了解基本的Objective-C/swift，對MVC架構有基本理解
預備知識	1. 已完成Android或iOS行動裝置應用系統課程者，或具備基本App觀念與關聯式資料庫、網路存取的學員 2. Android方面需對Activity生命週期與Java語法有基礎認識 3. iOS方面需了解基本的Objective-C，對MVC架構有基本理解
課程內容	1. iOS的keychain swift實作 2. iOS的sqlite加密sqlcipher說明 3. iOS的sqlite加密sqlcipher應用 4. Android的keyguard實作 5. Android的sqlcipher實作與說明 6. Android的sqlcipher建置 7. OWASP mobile重點說明與其餘補充 8. 網路傳輸與加解密基礎導論
備註事項	CEH：EC-Council CEH駭客技術專家認證課程

獨家課程 網路安全封包分析認證

NSPA 網路安全封包分析認證課程

Network Security of Packet Analysis Course

時數：21小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

NSPA

適合對象	1. 具備TCP/IP網路技術概念者 2. 企業網路之管理人員	3. 欲從事網路安全之相關人員 4. 對網路安全有興趣者
先修課程	已完成以下課程所具備技術能力 NINS：網路基礎架構與網路服務	
課程內容	1. 網路封包分析的基本知識與常用技巧 2. 常見網路服務FTP、Telnet、SSH、SMTP、POP3、IMAP封包行為分析 3. 常見HTTP、HTTPS之正常與異常封包行為分析 4. 網路芳鄰(CIFS/SMB/NAS)之正常與異常封包行為分析	5. ODBC、MS-SQL、MySQL、PostgreSQL、Oracle資料庫之封包行為分析 6. 惡意程式(Malware)、跳板主機與駭客攻擊封包行為分析 7. 網路異常與駭客攻擊的案例分析
備註事項	1. 白天班之上課時間為09:30~17:30 2. 本課程結束後將頒發結業證書 3. 本課程與中華民國網路封包分析協會(NTPA)合作開班 4. 本課程包含一次認證考試，考試時間將於課程第三天下午舉行筆試，考試時間60分鐘，題數33題 證照寄發：7天知道考試結果，30天後收到中華民國網路封包分析協會(NTPA)寄發的電子證書 通過標準：滿分100分，測驗及格分數70分即可通過考試，取得網路安全封包分析認證 5. 課程優惠方案：早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價	
後續推薦課程	ANSPA：網路安全封包分析進階實作	

ANSPA 網路安全封包分析進階實作

Network Security of Packet Analysis – Practice Course

時數：21小時 | 費用：24,000元 | 點數：6點 | 教材：專用教材

ANSPA

適合對象	1. NSPA Class C認證人員 2. 企業網路之管理人員	3. 欲從事網路安全之相關人員 4. 對網路安全有興趣者
先修課程	1. TCP/IP網路通訊協定 2. 資訊安全基礎概念	3. NSPA：網路安全封包分析認證(Class C) 4. NINS：網路基礎架構與網路服務
課程內容	1. 網路安全封包分析-常見木馬程式實例 包括有：網路資安基本檢測方式、判斷網路異常通訊方式、正常網路封包的分析(實作)、惡意程式攻擊實作與封包分析(AgentTesla, HawkEye, QuasarRAT, NjRAT, NanoCore, AveMaria, Lucifer等等)、封包分析技巧的學習評量與討論(實作題5題、木馬程式部分) 2. 網路安全封包分析-常見加密勒索實例 包括有：加密勒索的運作與偵測、加密勒索的案例研析、加密勒索攻擊實作與封包分析(Loocipher, WannaCry,Sodinokibi, Dharma, Nemty, GlobeImposter)的分析、封包分析技巧的學習評量與討論(實作題5題、加密勒索部分) 3. 網路安全封包分析-常見IDS/IPS與手機封包實例 包括有：APT組織的探討與案例、駭客攻擊的策略與戰術、多重複合式攻擊的案例、IDS/IPS偵測規則與Wireshark的規則轉換、封包分析技巧的學習評量與討論(實作題18題)	
備註事項	1. 白天班之上課時間為09:30~17:30 2. 全程參加課程者授予「上課證明」 3. 本課程與中華民國網路封包分析協會(NTPA)合作開班	4. 課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價
後續推薦課程	CNSPA：網路安全封包分析案例探討	

CNSPA 網路安全封包分析案例探討

Network Security of Packet Analysis-Case Study

時數：21小時 | 費用：32,000元 | 點數：8點 | 教材：專用教材

CNSPA

適合對象	1. NSPA Class C 認證人員 2. 企業網路之管理人員	3. 欲從事網路安全之相關人員 4. 對網路安全有興趣者
先修課程	1. TCP/IP網路通訊協定 2. 資訊安全基礎概念	3. NSPA：網路安全封包分析認證(Class C) 4. NINS：網路基礎架構與網路服務
課程內容	1. 網路安全封包分析-國際資安案例之Cobalt Strike Beacon案例 包括有：實際案例解說、Cobalt Strike 介紹、Beacon用途、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題: Cobalt Strike Beacon部分) 2. 網路安全封包分析-國際資安案例之DoppelPaymer案例 包括有：實際案例解說(Hyndai-KIA, Foxconn, Compal, A123 Systems, Mitsubishi Polysilicon)、Doppel Paymer介紹、Mimikatz用途、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題: Doppel Paymer部分) 3. 網路安全封包分析-國際資安案例之GlobeImposter案例 包括有：實際案例解說(醫療院所)、GlobeImposter 介紹、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題:GlobeImposter部分) 4. 網路安全封包分析-國際資安案例之 Solar Wind供應鏈案例 包括有： Solar Wind 介紹、軟體系統供應鏈案例分析、American Bank System案例分析、Solar Wind之惡意樣本程式、學習評量與討論 5. 網路安全封包分析-國際資安案例之WastedLocker, LockBit, MountLocker案例 包括有：實際案例解說(Garmin與其他受駭廠商)、WastedLocker 介紹、LockBit介紹、封包分析技巧、實際獵殺演練、學習評量與討論(封包題3題: LockBit, MountLocker部分) 6. 網路安全封包分析-國際資安案例之Insider Offensive 案例 包括有：實際案例解說(CPC、FEIB)、ARP Scan 介紹、C#-Powershell介紹、svchost介紹、SWIFT/Bitsran介紹、封包分析技巧、實際獵殺演練、學習評量與討論(封包題2題: svchost部分，封包題2題: Bitsran部分)	
備註事項	1. 白天班之上課時間為09:30~17:30 2. 全程參加課程者授予「上課證明」 3. 本課程與中華民國網路封包分析協會(NTPA)合作開班	4. 課程優惠方案： 早鳥優惠價：開課前2周完成報名繳費，享有早鳥優惠價
後續推薦課程	ANSPA：網路安全封包分析進階實作	