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	1. 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 2. 請於上課前完成GPT帳號申請，以利課堂練習進行
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

2026新課

SECISS 資通安全管理法合規實務解析

Analysis of Compliance Practices under the Information and Communications Security Management Act

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	公務機關（含中央、地方機關（構）或公法人）及特定非公務機關（含關鍵基礎設施提供者、公營事業及政府捐助之財團法人）
預備知識	具備基礎資安管理能力
課程內容	1. 資通安全威脅發展趨勢包含： • 全球與國內近期重大資安事件解析，深入探討國內外典型資安事件（如APT、勒索軟體攻擊）與其對政府機構與關鍵基礎設施之衝擊 • 新興威脅技術與攻擊手法演進，分析 AI 驅動攻擊、社交工程手法、供應鏈攻擊等攻擊模式。 • 關鍵基礎設施面臨的資安挑戰與應對趨勢，探討關鍵基礎設施（能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區、糧食）領域在資安防護上的新挑戰與國際趨勢。 2. 資通安全管理法解析 • 資通安全管理法與相關子法規定之責任與義務，說明主管機關、機關（構）、特定非公務機關之角色與法律義務。 • 資通安全維護計畫之訂定，說明依據資通安全管理法施行細則所要求資通安全維護計畫應包括事項之訂定重點。 • 資通安全事件之通報及應變機制，說明依據資通安全事件通報與應變辦法所要求訂定資通安全事件通報及應變機制之重點。 3. 資通安全管理實作策略與技巧 • 委外之選任及監督責任，說明委外辦理資通系統之建置、維運或資通服務之提供時，其選任及監督受託者時，應注意事項之實作建議。 • 資通安全維護計畫之實施策略與技巧，說明依據組織營運需求、風險評鑑結果以及國際資安標準（如 ISO/IEC 27001）進行整體規劃與部署。另亦針對資安防護技術應用與委外管理風險控管，探討資安控制措施選型與委外管理風險控管重點說明。 • 資通安全事件通報與應變流程實作技巧，由資通安全事件處理生命週期說明資通安全事件通報與應變機制之制定，並透過實務之資通安全事件情境設計進行演練規劃與執行。
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，享有早鳥恆逸銀卡優惠價

2026新課

SECPDP 個人資料保護法合規實務解析

Analysis of Compliance Practices with the Personal Data Protection Act

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	公務機關（含中央或地方機關或行政法人）及非公務機關（含自然人、法人或其他團體）
預備知識	具備基礎資安及個人資料管理能力
課程內容	1. 個人資料威脅發展趨勢 • 攻擊手法趨於高度社交化與智慧化，說明駭客不再只依靠技術入侵，透過社交工程與AI工具進行精準詐騙（如假冒信件、語音、影像）成為主流。尤其針對個人資料（如身份證號、聯絡方式、財務資訊）進行「針對性攻擊」。 • 資料大量集中與跨平台、跨境傳輸風險升高，說明個人資料在政府機關、金融機構、電商、醫療平台之間大量集中，且日益依賴雲端與第三方服務，使得「單一破口、大量外洩」的風險上升。 • AI技術與大數據分析引發個資隱私新挑戰，說明AI與大數據普及促使各行業高度依賴個資進行建模、推薦與自動化決策。但這也讓「隱私侵犯」與「非授權用途」的風險顯著上升。 2. 個人資料保護法解析 • 個人資料保護原則，說明個人隱私資訊概念及個人資料保護原則。 • 個人資料生命週期之要求，說明個人資料於蒐集、處理、利用、傳輸、刪除（個人資料生命週期）之要求事項重點。 • 個人資料保護要求重點，說明由資訊科技角度解釋個人資料保護法對於個人資料保護要求之重點內容。 3. 個人資料保護法實作策略與技巧 • 說明國內外包含ISO 27701、BS 10012以及TPIPAS有關隱私資訊管理系統之現況。 • 個人資料檔案安全維護計畫之實施策略與技巧，說明依據組織的營運需求、風險評鑑結果以及國際隱私資訊管理標準（如 ISO/IEC 27701）進行整體規劃與部署與探討資安控制措施選型與委外管理風險控管重點。
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，享有早鳥恆逸銀卡優惠價

2026新課

SECLOC 上市上櫃公司資通安全管控指引合規實務解析

Analysis of Compliance Practices in the Guidelines for Information Security Control of Listed and OTC Companies

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	上市上櫃（或預計上市上櫃）之公司行號
預備知識	具備基礎資安管理能力
課程內容	1. 資通安全威脅發展趨勢 • APT攻擊與勒索軟體威脅升級，說明上市櫃公司因財務價值高、商業機密多，成為高度針對性的攻擊目標。駭客集團傾向發動APT（Advanced Persistent Threat）長期滲透，並以勒索軟體進行資料加密或竊密勒贖，特別是在財報發布、董事會會期前夕進行攻擊，以放大破壞效果。 • 商業與財務資訊外洩風險加劇，影響公司信譽與股價，說明個人資料在政府機關、金融機構、電商、醫療平台之間大量集中，且日益依賴雲端與第三方服務，使得「單一破口、大量外洩」的風險上升。 • 供應鏈資安風險成為新型攻擊突破口，說明駭客傾向攻擊供應鏈中的弱點廠商或合作夥伴（如第三方 IT 廠商、雲端服務商、物流業者等）進而滲透上市公司主體系統。這類間接入侵手法（Supply Chain Attack）難以防範，且影響範圍可能跨足整個產業鏈。 2. 上市上櫃公司資通安全指引解析 • 說明上市上櫃公司資通安全指引之內函。 • 說明資通安全指引與ISO 27001資訊安全管理系統之對應。 3. 上市上櫃公司資通安全管控指引實作策略與技巧 說明上市上櫃公司資通安全管控指引於下列項目之實作策略與技巧，包含： • 資通安全政策及推動組織，說明如何依據組織全景及關注方之需要及期望訂定資通安全政策及目標以及建置適切之管理組織推動組織資通安全管理作業。 • 核心業務及其重要性，說明依據組織的核心業務鑑別應遵守之法令及契約要求，並制定核心業務持續運作計畫。 • 資通系統盤點及風險評估，說明實施資通系統盤點之技巧以及如何針對盤點結果進行風險評鑑並妥採適切之控制措施降低風險。 • 資通系統發展及維護安全，說明資通系統於獲取、開發及維護過程，應遵循之要求事項。 • 資通安全防護及控制措施，說明資通安全管控指引所要求之安全防護及控制措施實施重點及程序規範設計。 • 資通系統或資通服務委外辦理之管理措施，說明規劃資訊作業委外安全管理程序，包含委外選商、監督管理及委外關係終止相關規定之重點。 • 資通安全事件通報應變及情資評估因應，說明由資通安全事件處理生命週期說明如何規劃資安事件應變處置及通報作業程序，以及如何威脅情資管理之實作重點。 • 資通安全之持續精進及績效管理機制，說明如何透過內部及委外廠商之資安稽核作業，針對發現事項進行改善措施並持續追蹤。
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，享有早鳥恆逸銀卡優惠價

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	

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：15,000元 | 點數：3.5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	Devop：DevOps原理與實作	

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

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，享有早鳥恆逸銀卡優惠價	
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

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, GlobleImposter)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，享有早鳥恆逸銀卡優惠價
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

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，享有早鳥恆逸銀卡優惠價	
後續推薦課程	ANSPA：網路安全封包分析進階實作	