**109年新型態資安實務示範課程發展計畫-資訊安全基礎實務課程**

**六大課程模組設計說明**

**一、課程目標**

1. 授課對象包括非資通訊科系領域之學生及高中職學生。依據初階資安入門之不同學習需求規劃課程模組。
2. 課程模組採彈性模組設計，依照需求規劃不同主題，授課教師可依據授課需求及課程大綱項目選擇適當的課程模組與教學單元。
3. 課程教學模組搭配國家高速網路中心提供之Cyber Defense Exercise，CDX平臺，進行實戰演練，讓學生實際動手做，以提高資安學習之樂趣。另CDX平台之實作課程分級：MyFirstSecurity CTF練習平台將題庫區分為基礎題(如linux101)與進階題(如linux102)，教師可依據授課時間長短酌予使用。

**二、課程特色**

1. 資安實務導向課程設計，不僅實務教授資安測試的測試手法更提供防禦的主題。
2. 可溶入國內108新課綱設計。
3. 跨域、跨校/系所的推動模式。
4. 整合新興科技(人工智慧)的主題。
5. 強調國內通過的資安管理法與資訊倫理及法律的正確觀念。

**三、六大課程模組架構**

**課程模組架構:**

|  |  |
| --- | --- |
| 模組名稱 | 模組內容(子模組) |
| 1.基礎模組 | 1.1.從資訊安全到資訊倫理與法律 |
| 1.2.Linux安全測試基礎 |
| 1.3.隱寫術 |
| 1.4.編碼與解碼 |
| 2.基礎密碼學模組 | 2.1.古典密碼學與破密分析 |
| 2.2.現代密碼學與演練 |
| 2.3.使用Python進行破密分析 |
| 3.網路安全模組 | 3.1.網路概論 |
| 3.2.網路封包分析實戰 |
| 3.3.Network-CTF實戰 |
| 3.4.網路攻擊分析與安全防護技術 |
| 3.5.防火牆防禦實戰 |
| 3.6.入侵偵測系統資安防禦實戰 |
| 4. 網站安全模組 | 4.1.網站運作原理 |
| 4.2.網站測試工具實戰 |
| 4.3.Web-CTF實戰 |
| 4.4.網站攻擊分析與安全防禦技術 |
| 4.5.網站漏洞分析與測試DVWA |
| 4.6.應用程式防火牆實戰 |
| 5. 系統安全模組 | 5.1.系統平台概論 |
| 5.2.系統平台安全初探 |
| 5-3-1.系統平台安全實測案例1--Windows XP系統安全測試 |
| 5-3-2.系統平台安全實測案例2--Linux伺服器安全測試 |
| 6. 人工智慧與資訊安全模組 | 6.1.使用Google Colab平台開發Python程式 |
| 6.2.基礎資料分析:NUMPY與Matplotlib實戰 |
| 6.3.基礎機械學習(ML) |
| 6.4.深度學習(DL)初體驗 |
| 6.5.人工智慧與資訊安全體驗專案:垃圾郵件 |

**四、課程主題說明與教學資源配套**

本節將詳細說明模組課程主題內容、課程目標與本計畫提供之教學資源。

1.基礎課程模組

|  |  |  |
| --- | --- | --- |
| 單元內容 | 學習目標 | 本計畫教學資源配套 |
| 1-1: 從資訊安全到資訊倫理與法律 | | |
| 1-1-1. 資訊倫理  1-1-2. 智慧財產權  1-1-3. 網路霸凌與犯罪  1-1-4. 個資保護與資安事件  1-1-5. 假新聞 | 引領學生對資訊安全的認識並了解資訊倫理的主題，並以案例分析方式介紹國內外重要的資訊安全法律（如資通安全管理法、歐盟GDPR），最後再以實際案例探討假新聞之重要性。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 1-2: Linux安全測試基礎 | | |
| 1-2-1. Linux系統介紹  1-2-2. Linux系統目錄結構  1-2-3. Linux指令-檔案與目錄操作  1-2-4. Linux指令-redirection(重定向)與pipe(管道)  1-2-5. Linux指令-網路  1-2-6. Linux指令-找尋檔案  1-2-7. Linux指令-壓縮與解壓縮  1-2-8. Linux指令-行程管理 | 透過搭配CTF平台實際運用Linux進行演練來了解Linux常用指令與熟悉Linux作業系統，上完本課程學生可學到如何查詢網路相關指令、查找檔案、加/解壓縮與行程管理等。 | ☑簡報□MOOCS  ☑教學錄影☑CTF平台  教學環境建置：  1.使用計畫辦公室所建置的CTF平台需提前一週與計畫辦公室確認上課時間  2.使用計畫辦公室所建置的IMAGE檔 |
| 1-3: 隱寫術 | | |
| 1-3-1. 隱寫術介紹  1-3-2. WORD、PDF的隱藏資訊  1-3-3. 圖片中的隱藏資訊  1-3-4. 檔案格式  1-3-5. 使用hex編輯器分析檔案  1-3-6. Linux中的dd、binwalk指令  1-3-7. 使用xxd查看檔案格式 | 本課程將透過CTF平台的解題來訓練學生熟悉隱寫術(Steganography)，課程將包括文件隱寫術與圖片隱寫術的技術，本課程將使用Linux平台上的binwalk 及dd演練，並以CTF的建置題目進行實測。 | ☑簡報□MOOCS  □教學錄影☑CTF平台 |
| 1-4: 編碼與解碼 | | |
| 1-4-1. 編碼與解碼之基本觀念  1-4-2. ASCII  1-4-3. Morse Code  1-4-4. Base64 | 本課程將教授資訊科技常見的不同編碼與解碼，包括ASCII及Base64編碼與解碼的基本觀念，本課程將以線上工具講授實際編碼與解碼的作法。  本課程將使用ＣＴＦ平台上的題目進行實際編碼與解碼。 | ☑簡報☑MOOCS  ☑教學錄影☑CTF平台 |
| 1-5: 隨堂測驗與問卷調查 | | |
| 1-5-1. 隨堂小測驗  1-5-2. 課後問卷調查 | 提供隨堂測驗10題及問卷調查[使用Google From]  提供會後測驗分析[考後提供給授課老師加分] |  |

2. 基礎密碼學模組

|  |  |  |
| --- | --- | --- |
| 單元內容 | 學習目標 | 本計畫教學資源配套 |
| 2-1: 古典密碼學與破密分析 | | |
| 2-1-1. 凱撒密碼  2-1-2. 換位加密法  2-1-3 Vigenere Cipher | 教授基本古典密碼學的加密與解密，包含凱薩密碼、頻率分析、密碼棒…等，並實際以線上工具完成破密並使用CTF平台上的題目進行實際演練 | ☑簡報☑MOOCS  ☑教學錄影☑CTF平台  教學環境建置：  1.使用計畫辦公室所建置的CTF平台需提前一週與計畫辦公室確認上課時間 |
| 2-2: 現代密碼學與演練 | | |
| 2-2-1. 對稱式加解密(DES、3DES)  2-2-2. 非對稱式加解密(RSA) | 本課程將教授現代密碼學的加密與解密，包括RSA及AES密碼學的基本觀念，本課程將以實際openssl及Python模組進行加解密。本課程將使用ＣＴＦ平台上的題目進行實際破密分析。  本課程不涉及密碼學演算法，先讓學生了解實際密碼學的加解密後再鼓勵學生後續研究相關演算法及其實作。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 2-3: 使用Python進行破密分析 | | |
| 2-3-1. 使用Python程式解編碼問題  2-3-2. 使用Python程式解密碼問題 | 本課程將教Python程式設計技術，為強化學習，本計畫以CTF的編碼與密碼學題目加以說明python程式設計的應用領域。透過實際演練將可使學生更清楚體驗運算思維及其實際應用。本課程將使用ＣＴＦ平台上的題目進行實際演練。 | ☑簡報□MOOCS  □教學錄影☑CTF平台  教學環境建置：  1.使用計畫辦公室所建置的CTF平台需提前一週與計畫辦公室確認上課時間 |
| 2-4: 隨堂測驗與問卷調查 | | |
| 2-4-1. 隨堂小測驗  2-4-2. 課後問卷調查 | 提供隨堂測驗10題及問卷調查[使用Google From]  提供會後測驗分析[考後提供給授課老師加分] |  |

3. 網路安全模組

|  |  |  |
| --- | --- | --- |
| 單元內容 | 學習目標 | 本計畫教學資源配套 |
| 3-1: 網路概論 | | |
| 3-1-1.電腦通訊概說  3-1-1-1.電腦與網路:基本觀念  3-1-1-2.資訊傳輸模式  3-1-1-3.網路傳輸速度  3-1-1-4.電腦網路的類型  3-1-2.網路的組成與架構  3-1-2-1.電腦網路的功能  3-1-2-2.區域網路的拓樸  3-1-2-3.Client/server與P2P  3-1-3.網路標準與通訊協定  3-1-3-1.通訊協定與標準  3-1-3-2.OSI通訊標準  3-1-3-3.TCP/IP協定  3-1-3-4.傳輸層重要協定:TCP vs UDP  3-1-3-5.IP與DNS(網域名稱) | 本課程將教授  [1]基礎的網路概念，包含網路類型、網路拓樸、網路架構、網路傳輸媒介等  [2]網路協定:包括OSI 模型與TCP/IP網路協定  使同學對網路能有更進一步的認識。  1. 瞭解電腦網路類型及現代相關應用  2. 瞭解訊息傳遞方式並能說明網路協定每一層的功能  3. 瞭解TCP、UDP、IP協定與之特性  4. 瞭解IP、DNS運作原理 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 3-2: 網路封包分析實戰 | | |
| 3-2-1. Wireshark 封包側錄  3-2-1-1.安裝Wireshark  3-2-1-2.封包側錄  3-2-2.測試情境與分析  3-2-2-1.封包分析Connect2Google  3-2-2-2. DNS查詢分析  3-2-2-3. TCP 三向交握分析.  3-2-2-4. UDP封包格式分析  3-2-2-5.IP封包格式分析  3-2-3. FTP 側錄實務  3-2-4. Telnet 側錄實務  3-2-4. 網路攻擊封包分析:DDoS | 教導學生網路協定分析與攻擊封包分析。並實際以  wireshark /tshark讓學生由實作中了解TCP/IP網路協定中的HTTP/TCP/DNS　/UDP/IP協定規範。 | ☑簡報□MOOCS  □教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 3-3:Network-CTF | | |
| 3-3-1. Networking 1  3-3-2. woodstock-1-10  3-3-3. Network Forensic(MUST)  3-3-4. Special Agent User(MUST) | 教導學生透過CTF題目解題了解網路封包中的重要概念，包含從網路封包中擷取密碼、分析使用者使用之瀏覽器等、Linux相關指令操作等相關技術。 | ☑簡報□MOOCS  ☑教學錄影☑CTF平台  教學環境建置：  1.使用計畫辦公室所建置的CTF平台需提前一週與計畫辦公室確認上課時間 |
| 3-4:網路攻擊分析與安全防護技術 | | |
| 3-4-1. 網路攻擊模式分析  3-4-1-1. APT  3-4-1-2. DOS/DDOS  3-4-1-3. 社交工程(Social engineering)  3-4-1-4. 勒索軟體(ransomeware)威脅  3-4-1-5. 網路攻擊鏈Cyber Kill Chain  3-4-1-6. MITRE ATT&CK框架  3-4-2. 網路資安防禦技術  3-4-2-1. 存取控制清單  3-4-2-2. 防火牆  3-4-2-3. 入侵偵測系統 | 教授學生網路攻擊的模式與分析，包含DOS/DDOS、社交工程以及勒索軟體的威脅，再說明網路攻擊類型與流程，最後說明網路攻擊的防治對策與安全防護技術。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 3-5: 防火牆防禦實戰[進階部分] | | |
| 3-5-1. Linux防火牆簡介  3-5-2. Linux的防火牆  3-5-3. iptable防火牆實務 | 教授學生網路防禦技術常用的防火牆技術，並以所提供的Ubuntu Linux環境教導學生使用Iptables/ ufw設定防禦規則，並實際進行網路防禦的實際演練。 | ☑簡報□MOOCS  ☑教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 3-6:入侵偵測系統資安防禦實戰[進階部分] | | |
| 3-6-1. Snort簡介  3-6-2. SYN FLOOD detection流程簡介  3-6-3. 環境配置  3-6-4. 入侵偵測系統實務 | 教授學生網路防禦技術常用的入侵偵測系統技術，並以所提供的Ubuntu　linux環境教導學生使用snort設  定偵測規則，並實際進行網路攻及偵測的實際演練。 | ☑簡報□MOOCS  ☑教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 3-7: 隨堂測驗與問卷調查 | | |
| 3-7-1. 隨堂小測驗  3-7-2. 課後問卷調查 | 提供隨堂測驗10題及問卷調查[使用Google From]  提供會後測驗分析[考後提供給授課老師加分] |  |

4. 網站安全模組

|  |  |  |
| --- | --- | --- |
| 單元內容 | 學習目標 | 本計畫教學資源配套 |
| 4-1:網站運作原理 | | |
| 4-1-1. 瀏覽器與伺服器  4-1-2. 網站基本組成架構  4-1-3. HTTP 超文本傳輸協定  4-1-4. HTTP 協定(HTTP Protocol)  4-1-5. HTTP 請求(HTTP Request)  4-1-6. HTTP 回應(HTTP Response) | 本課程模組分為兩大部分。基礎部分將講授並實際演練HTTP協定及其相關測試工具，內容包含基礎運作原理、網站組成，溝通協定(HTTP)、HTTP 請求與回應方法(GET、POST、HEAD、OPTIONS…)、網頁狀態碼(200、403、404、503)…等。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 4-2:網站測試工具實戰 | | |
| 4-2-1.CURL工具的安裝與使用  4-2-2.Burp Suite工具的安裝與使用  4-2-3.Developer Tools安裝與使用 | 將講授並實際演練網站相關測試工具包括developer tools、curl、burpsuite等工具，課程將以CTF題目來強化學生的安全測試能力。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 4-3: Web-CTF實戰 | | |
| 4-3-1. 網站原始碼  4-3-2. 網站目錄與Robots.txt  4-3-3. Robots.txt與基礎編碼  4-3-4. 網址重新導向 | 課程將以CTF題目來強化學生的安全測試能力，內容包括網站原始碼、網站目錄、Robots.txt、測試工具(developer tools、curl)、Linux工具(Curl)使用方式、HTTP method簡介、CTF解題技巧等。 | ☑簡報□MOOCS  ☑教學錄影☑CTF平台  教學環境建置：  1. 使用計畫辦公室所建置的CTF平台需提前一週與計畫辦公室確認上課時間 |
| 4-4: 網站攻擊分析與安全防禦技術 | | |
| 4-3-1. OWASP TOP TEN  4-3-2. 強化網站安全  4-3-3. 漏洞掃描  4-3-4. 網站應用程式防火牆 | 課程將講授OWASP TOP 10(2017)所揭露的部分常見的網站漏洞，再講授網站威脅的常見類型，最後講授網路防禦技術常用的技術。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 4-5: 網站漏洞與分析 | | |
| 4-5-1. 漏洞與漏洞揭露平台  4-5-2. OWASP TOP 10  4-5-3. 測試環境建置  4-5-4. Command Injection  4-5-5. SQL Injection  4-5-5-1. SQL Injection防禦實務  4-5-5-2. SQL Injection Log分析  4-5-6. Reflected Cross Site Scripting  4-5-6-1. XSS 防禦實務  4-5-6-2. XSS LOG分析 | 講授OWASP TOP 10(2017)所揭露的部分常見的網站漏洞，以一完整的實測案例教導學生網站安全的安全測試技術包括DVWA漏洞平台、Command Injection原理與技術、Linux指令、SQL Injection原理與技術、SQL查詢語法、HTML5、JavaScript、XSS跨站腳本威脅原理與技術分析、網站黑名單過濾、bypass技術、網站防禦技術。 | ☑簡報□MOOCS  ☑教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 4-6: 應用程式防火牆實戰[進階部分] | | |
| 4-6-1. 網站攻防實戰環境  4-6-2. 環境建置  4-6-3. 應用程式防火牆實務 | 教授學生網站防禦技術常用的應用程式防火牆技術，並以所提供的Ubuntu　Linux環境教導學生使用  modsecurity設定規則，並實際進行網路攻及偵測的  實際演練。 | ☑簡報□MOOCS  ☑教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 4-7: 隨堂測驗與問卷調查 | | |
| 4-7-1. 隨堂小測驗  4-7-2. 課後問卷調查 | 提供隨堂測驗10題及問卷調查[使用Google From]  提供會後測驗分析[考後提供給授課老師加分] |  |

5. 系統安全模組

|  |  |  |
| --- | --- | --- |
| 單元內容 | 學習目標 | 本計畫教學資源配套 |
| 5-1: 系統平台概論 | | |
| 5-1-1.Windows作業系統  5-1-2.Linux作業系統 | 教授學生基本系統平台概念，包含Windows與Linux作業系統。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 5-2:系統平台安全初探 | | |
| 5-2-1. 系統與漏洞  5-2-2. 漏洞揭露平台  5-2-3. 強化安全防禦 | 教授學生基本硬體、作業系統漏洞與安全強化的基本觀念，探討系統漏洞在實務上如何偵測、改善並強化安全防護，包含硬體(CPU)漏洞、作業系統常見漏洞及漏洞揭露平台，最後再講解如何強化安全防禦。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 5-3-1: 系統平台安全實測案例1--Windows XP系統安全測試[進階部分] | | |
| 5-3-1-1. 滲透測試概論  5-3-1-2. 滲透測試平台與相關工具  5-3-1-3. Windows XP 滲透測試  5-3-1-4. 防護技術 | 教授學生系統安全的基本觀念，並實際以kali linux的nmap 及metasploit針對windows系統進行威脅模式分析，課程也將介紹如何使用windows系統的工具進行防禦。 | ☑簡報□MOOCS  ☑教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 5-3-2: 系統平台安全實測案例2-- Linux伺服器安全測試[進階部分] | | |
| 5-3-2-1. Metasploitable 2環境確認  5-3-2-2. Linux伺服器安全測試 | 教授學生系統安全的基本觀念，並實際以kali linux的nmap 及metasploit針對Linux系統進行威脅模式分析。 | ☑簡報□MOOCS  ☑教學錄影□CTF平台  教學環境建置：  1.使用計畫辦公室所建置的IMAGE檔 |
| 5-4: 隨堂測驗與問卷調查 | | |
| 5-5-1. 隨堂小測驗  5-5-2. 課後問卷調查 | 提供隨堂測驗10題及問卷調查[使用Google From]  提供會後測驗分析[考後提供給授課老師加分] |  |

6. 人工智慧與資訊安全模組

|  |  |  |
| --- | --- | --- |
| 單元內容 | 學習目標 | 本計畫教學資源配套 |
| 6-1.使用Google Colab平台開發Python程式 | | |
| 6-1-1. 使用Google Colab平台開發Python程式 | 使用Google Colab平台開發Python程式與人工智慧程式、Google Colab使用介紹 與 基礎實務演練。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 6-2.基礎資料分析:NUMPY與Matplotlib實戰 | | |
| 6-2-1.資料科學與資料分析  6-2-2.NUMPY技術  6-2-3.資料視覺化與Matplotlib實作 | 本課程以資料分析為主軸， Numpy學習基礎矩陣運算，接著透過Matplotlib實作資料視覺化，將資料以圖形、圖示呈現，讓學生了解資料分析之重要性與應用。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 6-3.基礎機械學習(ML) | | |
| 6-3-1. 機器學習概論  6-3-2. 機器學習線性回歸分析  6-3-3. 機器學習分類演算法--決策樹  6-3-4. 機器學習非監督學習--叢集演算法  6-3-5. 機器學習與資安分析--案例研究 | 以迴歸分析實戰說明機器學習的核心，包括梯度下降法及相關技術，讓學生對機器學習與AI技術有所了解，上完課學生須了解機器是如何進行學習。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 6-4. 深度學習(DL)初體驗 | | |
| 6-4-1. 人工智慧與深度學習概論  6-4-2. 類神經網路與學習  6-4-3. CNN與RNN  6-3-4. 人工智慧與資安分析--案例研究 | 引領學生對人工智慧的認識並實際演練基本的神經網路演算法。另外將示範人工智慧在資訊安全分析的應用，並以人工智慧與深度學習為主軸，CNN與RNN為例，實際講解類神經網路之學習。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |
| 6-5. 人工智慧與資訊安全體驗專案:垃圾郵件 | | |
| 6-5-1. 人工智慧與資訊安全體驗專案:垃圾郵件 | 介紹人工智慧如何用在資訊安全領域，並以一個實際案例讓學生了解人工智慧用在資訊安全領域的應用。 | ☑簡報□MOOCS  □教學錄影□CTF平台 |