

**教育部補助大學校院新型態資安實務示範課程發展計畫**

**書面審查意見回覆表**

|  |  |
| --- | --- |
| 審查意見 | 意見回覆 |
| 計劃培養學生標的清楚，符合目前資訊安全扎根與資安技術人力年均年齡下降趨勢，且可導正年輕學子對資安的趨勢興趣與資訊倫理。技術訓練趨勢符合目前主流(CTF)，藉由攻防了解資安產業與技術實務，但建議參考高中職資訊概論課綱，調整課程內容。 | 感謝委員指導，本計畫已遵照委員指導參酌高中職資訊概論課綱及其他相關課程課綱，將計畫課程模組與現行高中職資訊課程做一對應，並再提出不同使用模式與情境來協助與輔導高中職資訊教師使用本示範課程的不同課程模組。 |
| 本課程之主題領域為資安認知教育(通識) 課程，課程規劃除資訊安全到資訊倫理與法律外，以安全測試、加密/解密與破密及網站安全防護等為主。對於本領域之授課對象為非資通訊科系領域之學生，包括高中職學生及一般民眾資安認知教育使用，內容似乎太偏技術，建議增加一些與日常生活相關之資安議題，如行動化安全、行動支付安全及雲端安全等，以增加同學之學習興趣。 | 感謝委員指導，本屆示範課程共有兩個團隊參與資安認知教育(通識) 課程，我們已經和另一個團隊討論協同合作與分工事宜，將委員指示的與日常生活相關之資安議題納入修正計畫書。 |
| 在參與師資的部份，部分主要師資並無資安相關背景，其專業程度有疑慮，但至少業師的部份有請到資安專業的公司員工來做專業部分的講解。 | 感謝委員指導，本計畫主要參與成員以高中職教師為主，我們也會如委員預期邀請參與業師協助高中職教師的專業提升。 |
| 經費與進度規劃合宜。 | 感謝委員肯定 |
| 以通識課程而言，預期成效應偏高。 | 感謝委員體恤，我們一定會全力以赴完成計畫書所規畫之預期成效。 |

**啟動會議委員意見回覆表**

107.9.13啟動會議建議

|  |  |
| --- | --- |
| 審查意見 | 意見回覆 |
| 該課程內容規劃以實作為主，建議可加強資安課程議題的基本知識，特別是資安倫理等部分。 | 感謝委員指導，本計畫已遵照委員指導加強資安課程議題的基本知識並特別強化資安倫理的部分內容。 |
| 網路「攻擊」與「防守」為資安一體兩面，建議加強宣導資安倫理觀念，以免學生誤觸法網。 | 感謝委員指導，本計畫已遵照委員指導將加強宣導資安倫理觀念。 |
| 建議與設置於台南二中的「高中資訊學科中心」合作，以利資安基礎及認知教育課程推廣至全國高中。 | 感謝委員指導與協助，我們會積極與台南二中的「高中資訊學科中心」合作將課程模組推廣至全國高中職學校。 |

**教育部補助大學校院辦理第二期新型態資安實務示範課程發展計畫**

學校：崑山科技大學

系所： 資工系

計畫主持人：曾龍副教授

**計畫書修正對照表**

107年9 月 25 日

|  |  |  |
| --- | --- | --- |
| **原計劃書** | **修改後計畫書** | **說 明** |
| 無 | 頁碼第32頁:新增說明  根據高中資訊科技概論課程大綱調整與推薦課程模組。 | 根據書面審查意見參考高中職資訊概論課綱，調整課程內容 |
| 頁碼第18頁  原《人工智慧與資訊安全》模組之課程模組說明。 | 頁碼第23頁:  將《人工智慧與資訊安全》模組調整成《新興資訊安全課題》模組除《人工智慧與資訊安全》模組並新增《行動APP安全》與《雲端安全》等主題。 | 根據書面審查意見增加一些與日常生活相關之資安議題 |
| 頁碼第15頁:  課程目標無明確說明基本知識的加強。資安倫理的部分內容強化同下說明。 | 頁碼第20頁:新增說明  本計畫規劃的模組化課程依照不同的範疇有不同的課程學習目標。各課程模組不僅講授相關基本知識外更強調實作學習，基本知識的講授將提供所有上課簡報與部分影片教學，實作學習則供學習環境與配套工具。 | 根據啟動會議委員意見加強資安課程議題的基本知識並特別強化資安倫理的部分內容 |
| 頁碼第15頁  《從資訊安全到資訊倫理與法律》模組將以案例的方式說明國內外資安事件與相關的法律，本課程模組也將以案例說明相關法律的內涵，並引入資訊倫理的主題，以建立學生正確的行為。 | 頁碼第20頁:  《從資訊安全到資訊倫理與法律》模組將強調資訊倫理的重要性，將以生動的說明來強調資訊倫理上四大議題(Mason的PAPA模式)。另將以案例的方式說明國內外資安事件與相關的法律(包括我國通過的資通安全管理法與歐盟GDPR等)，以建立學生正確的行為。 | 根據啟動會議委員意見加強宣導資安倫理觀念 |
| 頁碼第19頁  推動策略之說明 | 頁碼第26頁:  新增推動策略第三項目:與現有高中職學科中心合作。 | 根據啟動會議委員意見:建議與設置於台南二中的「高中資訊學科中心」合作，以利資安基礎及認知教育課程推廣至全國高中。 |
| 頁碼第24頁  原開課時間為107年第1學期 | 頁碼第31頁:  將開課時間調整為107年第2學期及新增相關說明。 | 根據總計畫規劃調整將開課時間調整為107年第2學期，以利課程內容調整。 |

**目 錄**

1. **基本資料(7)**
2. **資安實務課程相關計畫執行成果(8)**
3. **課程規劃與設計(17)**
4. **課程目標與特色(17)**
5. **課程綱要與導引(26)**
6. **教學方式與課程配套(35)**
7. **學習成效評量機制(39)**
8. **課程學習互動與回饋機制(40)**
9. **教學資源發展規劃**
10. **實務課程教學環境或演練平臺的布建 (42)**
11. **實務課程教學設計與操作手冊(43)**
12. **結合網路、影音等多媒體教學資源(45)**
13. **校內外教學資源之配合(51)**
14. **參與師資(53)**
15. **參與教師簡介(53)**
16. **外聘專家簡介(61)**
17. **經費與進度規劃(63)**
18. **進度規劃及相關行政配置(63)**
19. **經費規劃(64)**
20. **預期成效(68)**
21. **預期質化效益(68)**
22. **預期量化指標(69)**
23. **基本資料**

|  |  |  |  |
| --- | --- | --- | --- |
| 申請單位 | 崑山科技大學資訊工程系 | | |
| 主題領域  (擇一) | ▓資安認知教育(通識) 課程  □核心資安課程  □進階資安課程  □跨領域資安應用課程 (勾選跨領域，以下領域知識單選，必選)  　□關鍵基礎設施系統安全：□電力 □電信 □交通 □其他＿＿＿＿＿  　□AI人工智慧應用與安全  　□硬體安全  　□金融科技安全  　□醫療資訊系統安全  ✽主題領域定義詳徵件須知五、課程主題領域 | | |
| 課程名稱 | (中文)資訊安全基礎實務課程  (英文)A practical introduction to security | | |
| 計畫主持人 | 崑山科技大學曾龍副教授 | | |
| 協同主持人  (共同主持人) | 國立臺南第一高級中學高英耀圖書館主任 | | |
| 開課教師 | 國立臺南第一高級中學高英耀圖書館主任、  國立新營高級工業職業學校資訊科陳忠謀主任 | | |
| 開課系所 | 國立臺南第一高級中學特色選修課程  國立新營高級工業職業學校資訊科(協同教學) | | |
| 課程特色 | □跨域，應用產業領域：  ▓跨系所 ▓跨校 | | |
| 計畫總經費 | 2,500,000元 | | |
| 申請教育部  補助金額 | 2,500,000元 | 自籌款或其他單位補助金額 | 0 元 |
| 本計畫執行內容是否另已申請或獲得其他機關或本部相關單位補助？  ▓否 □是（申請/補助單位：　　　　　　申請/補助金額：　　　　　　元） | | | |
| 計畫主持人  聯絡電話 | 06-2727175#354  0956327000 | 電子信箱 | 8wingflying@gmail.com |
| 開課教師聯絡資訊(請全列，計畫主持人免列) | | | |
| 姓 名 | 高英耀 | 姓 名 | 陳忠謀 |
| 單位職稱 | 國立臺南第一高級中學/圖書館主任 | 單位職稱 | 國立新營高級工業職業學校資訊科/主任 |
| 聯絡電話 | (06)2371206#600 | 聯絡電話 | (06)6322377#560 |
| 電子信箱 | [joseph.tnfsh@gmail.com](mailto:joseph.tnfsh@gmail.com) | 電子信箱 | [morrischen@hyivs.tn.edu.tw](mailto:morrischen@hyivs.tn.edu.tw) |

計畫主持人：  系所主管： 

1. **資安實務課程相關計畫執行成果**

**(104年~106年度期間曾獲補助新型態資安實務課程計畫或示範課程發展計畫等，請簡述執行成果；如無免填)**

**本計畫計畫主持人於104年~106年度期間曾獲教育部補助底下下各項計畫:**

**(1)104年度新型態資安實務課程計畫**

**(2)105年度新型態資安實務課程計畫**

**(3)106年度資訊安全人才培育計畫子計畫三**

**底下分述各計畫執行成果。**

**(1)104年度新型態資安實務課程計畫**

104年度申請的新型態資安實務課課程包含滲透測試實務、行動裝置資安實務、物聯網IoT資安與資安偵測四大主題。滲透測試實務係透過Metasploit滲透測試實務，讓學生實測駭客模組化工具，並運用工具針對OWASP Web TOP10進行滲透測試實務來加強學生資訊安全能力；行動裝置的普及化後續衍生的安全性問題不斷增長，本課程依據OWASP Mobile Web TOP10進行Android資安檢測、iOS資安檢測及分析並加入Android APP逆向工程與靜態分析，分析惡意APP剖析駭客行為。因應物聯網(IoT)時代的來臨，本課程安排業界講師依業界實務經驗講授IoT安全問題，使學生更能了解物聯網安全性問題亦能了解資安產業的現況；本課程以模擬駭客攻防測試，教導學生撰寫偵測規則，並訓練學生實務演練技術。

本課程目標延續103年本系所資安人力之培養，本課程於課程開始講授99年至104年資安事件發展趨勢，讓學生了解新型態資安攻擊模式與發展；接續說明安全測試方法論OSSTMM及滲透測試工具介紹，本課程強調實務演練，以滲透測試工具軟體Kali Linux、Metasploit帶領學生進行資安攻防實務演練藉此分析駭客攻擊行為，讓學生了解駭客攻擊的手法與如何透過各項工具進行偵測與防禦，以達成強化學生對於資訊系統的安全與防範能力，透過各種演練來增進學生的資安技術面能力，更夠獲得實際偵查與防禦駭客之經驗。有鑑於行動裝置的發展，本課程特別加入行動裝置資安的議題，帶領學生實作Android逆向工程與其靜態分析，有助於加強學生於行動終端的防護能力。

本系所除每學年於高年級與碩士班開設資訊安全相關課程外，亦不定期舉辦資安與雲端講座，曾邀請數聯資安張裕敏副總經理、工研院雲端中心闕志克主任、華碩雲端吳漢章總經理、資安公司vArmour徐千洋資深工程師、安華聯網科技吳東杰資安工程師、法務部調查局周台維專員、國立台灣科技大學林宜隆教授等多位產官學研專家學者演講，以提升本所學生資安知識水平。本系所於資安證照的推動也不遺餘力，本計畫主持人曾龍帶領20位高年級與碩士班學生於103年考取18張國際資安CEH(Certificated Ethical Hacker)證照並持續培訓5位獲取CEH證照的學生於103年暑期完成舉辦六場針對縣市網路中心資安人員開設的暑期資安研習營，研習人數共計201人。隨著行動裝置日漸普及，其安全威脅也愈來愈大，本系所於102年開始積極推動Android、APPLE iOS、Windows Phone Mango之行動技術開發，曾獲得第7屆韓國首爾發明展銀牌、樂活百年搶先大賽聰明隨身秘書系統實作類季軍、台北國際發明展金牌獎與參與Android五零高手選項徵才競賽等Android競賽；100年曾與台灣微軟舉辦中南部首場微軟Windows Phone 7 Mango (WP7)手機程式開發體驗營，101年本系所學生開發Mango系統上架APP數達100隻以上；APPLE iOS開發方面獲廠商贊助人才培育計畫、並開發花園夜市、行腳四草、台南公車行、App評測之APP成果，由此見得本系所在行動設備裝置上可提供學生充裕的實作資源加上豐富的開發經驗，於反組譯逆向工程能夠更深入的剖析。

此課程規畫四大主題，包含滲透測試實務、物聯網IoT資安、行動裝置資安實務與資安偵測。依據最新資安事件規劃課程內容，包括滲透測試方法論(OSSTMM3.0)並介紹相關工具，規劃Metasploit滲透測試實務，讓學生了解駭客模組化工具，運用其工具針對OWASP Web十大風險進行滲透測試實務加強學生資訊安全能力。除以上資訊安全威脅外；因應物聯網(IoT)時代的來臨，其背後網路安全所帶來龐大資訊安全威脅，因此本課程特別規畫業師依業界實務經驗講授IoT安全問題，使學生能更貼切的了解物聯網其網路安全性問題。2015年智慧型裝置的方便性及普及性所衍生的資安事件不斷增長，行動裝置的惡意程式也將突破800萬大關，行動資安防護勢在必行，本課程依據OWASP Mobile十大漏洞風險規劃，包含Android資安檢測、iOS資安檢測及分析，測試開發的APP是否有安全漏洞疑慮，課程並加入Android APP逆向工程與靜態分析，分析惡意APP剖析駭客行為。新形態的網路攻擊事件，例如零日攻擊造成全球網路常受到重大威脅，本課程以模擬駭客攻防測試，教導學生撰寫偵測規則，加強國內資安防護，並訓練學生實務演練技術。

本計畫共舉辦三場講座，分別為IoT security、手機APP安全檢測、資安國際盃技術及心得分享，其中IoT security與手機APP安全檢測講座中，邀請安華聯網科技股份有限公司洪光鈞總經理與行政院國家資通安全會報技術服務中心檢測與評鑑組陳培德組長，講師依據其業界實務經驗分享，讓學生能更了解IoT與手機APP檢測之安全實務，並讓學生能加強掌握資安產業現況，講座中講師帶領學生實機操作，能累積學生資安實務的經驗，充實其自身的資安能量。資安國際盃技術及心得分享講座中，邀請國立交通大學CTF團隊BambooFox陳仲寬博士，講師豐富的資安國際盃參賽經驗與培育CTF團隊心得分享，增加學生參與資安競賽的動力，在技術分享部分，實際操作與學生實機互動教學，除加深學生印象外，也讓學生更能掌握資安攻擊的實務技術。

本計畫主持人有鑑於103年度上學期資訊安全系統設計課程時，曾帶領同學前往國家高速網路中心參訪，課程學生反應熱烈並且成效優越，因此，於本次課程帶領學生前往國家級財團法人電信技術中心與民間企業鈊安資訊科技股份有限公司進行企業參訪，使學生深入了解產業現況，學生參訪後紛紛表示受益良多。

**(2)105年度新型態資安實務課程計畫**

105年度新型態資安實務課程計畫關注於網站安全。本課程於課程開始講授WebSecurity大事趨勢與攻擊事件與類型，包含OWASP TOP 10、SANS/CWE TOP 25、WASC；接續說明WebSecurity測試方法論與工具包含OWASP testing guide 4.0內容、白箱測試與黑箱測試、如何使用Kali Linux進行攻擊測試(滲透測試)，透過建置DVWA來提供學生實務測試環境。

課程中強調實務演練並安排大量的實作課程包含SQL injection攻擊、WordPress攻擊、跨站腳本（XSS）攻擊、跨站請求偽造（CSRF）攻擊、中間人攻擊（MITM）與針對性釣魚攻擊、HTTP DDoS攻擊實務演練、自動化模糊sulley測試，帶領學生進行網站攻防實務演練藉此分析駭客攻擊行為，使學生了解駭客攻擊的手法與如何透過各項工具進行偵測與防禦，以達成強化學生對於資訊系統的安全與防範能力，透過各種演練來增進學生的資安技術面能力，更夠獲得實際偵查與防禦駭客之經驗。

另外，搭配12小時企業講師授課，透過企業講師分享自己的經驗透過交流，提升學員資安的知識和實務技巧。本課程也帶領學生參訪國家高速網路中心、TTC財團法人電信技術中心等實驗室。計畫主持人也鼓勵與協助學生參與相關資安社團、競賽與資安證照考試輔導，並於課後時間提供相關實驗設備與平台給學生進行分組課後進階攻防演練。

本計畫主持人有鑑於104年度上學期資安檢驗與駭客攻防演練課程時，曾帶領同學前往財團法人電信技術中心及鈊安資訊科技股份有限公司參訪，課程學生反應熱烈並且成效優越，因此，於本次課程帶領學生前往國家級財團法人電信技術中心與國家高速網路中心參訪進行參訪，使學生深入了解產業現況，學生參訪後紛紛表示受益良多。

本次實務課程規劃以國家高速網路與計算中心Cyber Defense Exercise(CDX)作為資安攻防演練平台，先製作CDX學生教學手冊讓學生熟悉CDX平台操作流程，並在平台上佈署攻擊平台Kali Linux 2016與漏洞平台Metasploitable 2進行資安攻防演練。

課程進行之攻防測試包含Linux滲透測試與網頁安全攻防測試，並有助教群分享NMAP、Sqlmap、Metasploit工具技術。Linux滲透測試包含利用Nmap掃描Metasploitable 2開啟的服務(Services)、利用TCP埠512、513、514進行rlogin服務的弱點攻擊測試、利用TCP埠2049進行網路檔案系統(NFS)服務的弱點攻擊測試、利用DistCC Daemon Command Execution後門攻擊(CVE-2004-2687) 測試、利用Samba CIFS server 進行漏洞攻擊(CVE-2010-0926) 測試。網頁安全攻防測試使用OWASP Mutillidae、DVWA、WebGoat、Hack This Site網站漏洞平台進行測試其中包含系統指令注入(Command Execution)、跨站請求偽造(Cross-Site Request Forgery)、反射型XSS(XSS reflected)、儲存型XSS(XSS stored)、遠端檔案包含(File Inclusion)、SQL注入(SQL Injection)、SQL盲注(SQL Blind Injection)、數字型SQL注入(Numeric SQL Injection)、字串型SQL注入(String SQL Injection)、任意文件上傳(File Upload Vulnerability)、存取控制(Access Cnotrl)、隱藏表單操作(Hidden Form Field Manipulation)、參數竄改(Parameter Manipulation)、弱點cookie(Weak Session Cookies)、Web服務(Web Services)、認證過程失效(Fail Open Authentication)、HTML危險註解(Dangers of HTML Comments) 。

本課程中積極推動證照輔導，鼓勵學生考取資安相關證照，並針對證照所需技能加以輔導。本計畫主持人於105年09月20日 ~ 105年11月28日期間於課程外對學生進行證照輔導並於105年11月29日考試，共計9位學生取得證照。

**(3)106年度資訊安全人才培育計畫子計畫三**

教育部資訊安全人才培育計畫自106年度開始執行，子計畫三106年度主要內責辦理高中職生資安研習營、資安初學者挑戰活動：MyFirstCTF競賽、資安實務導師之推動以及整合與佈建CTF演練題庫:

**1. 高中職生資安研習營**

高中職生資安研習營主要的目標是藉由辦理資安扎根活動，如高中資安實務研習營/體驗營、資安初學者挑戰活動/競賽等，培育與發掘有潛力的學子，並協助資安認知推廣。106年度總共舉辦下列培訓課程，課程內容與辦理情形說明如下表所示。

|  |  |  |  |
| --- | --- | --- | --- |
| **類型** | **簡稱** | **名稱** | **場次與人次** |
| 高階課程 | 特訓營 | Winter Camp  寒訓營 | 場次：北部+南部各一場(寒假舉辦)  人次：162人次 |
| 進階課程 | 研習營 | 資安實務攻防研習營  (Hacking weekend) | 6場/249人次  27所高中職學生、30所大學學生參與 |
| 基礎課程 | 體驗營 | 高中職學生資安體驗營 (Happy Hacking day) | 預計辨理：12場  實際辦理：25場  59所高中職學生+13所大學學生參與，累計919人次 |

1. 高中職學生資安體驗營(Happy Hacking day)：

* 為推廣資安認知與扎根資安基礎實務人才訓練，以及發掘與培育具潛力學子，針對高中職生的資訊技術能力，規劃與設計具趣味性與動手作的資安實務課程內容。
* 本年度共辦理25場高中職學生資安體驗營，包含東部與離島學校，共計919人次參與，共計59所高中職學生、13所大學學生參與。

**針對所辦理之高中職生資安體驗營，於課程後皆有進行問卷調查，並視學生學習狀況滾動式調整課程內容，高中職生資安體驗營問卷調查結果顯示課程滿意度：94%、教材滿意度：95%、教師上課滿意度：97%、對於資安知識提昇滿意度：93%、教學內容滿意度：95%、課程理解度：77%。**

1. 資安實務攻防研習營(Hacking Weekend)：

* 此為進階課程，以資安實務基礎為主，強調「動手作」的資安實務技術體驗與學習。研習營課程於暑假期間舉辦的稱之為資安實務攻防研習營(Hacking Weekend)。
* 本年度共辦理6場資安實務攻防研習營(Hacking Weekend)，計249人次參與，共計27所高中職學生、30所大學學生參與。

**針對所辦理之資安實務攻防研習營，於課程後皆有進行問卷調查，並視學生學習狀況滾動式調整課程內容，其問卷調查顯示進階課程可有效提昇學生資訊安全的實力。107年度將 從基礎課程、進階課程、高階課程三模式，舉辦高中職資安體驗/研習營，課程規劃從體驗到實作，從年輕學子向下扎根，啟發學生對資安議題的重視。**

1. 2018 Winter Camp 寒訓營

* 本計畫於寒假期間舉辦寒訓營。此次主題為「從程式debug＋reverse到PWN搶旗大賽」，由臺灣好厲駭CTF培訓學生擔任主講，傳承其經驗。其課程表詳細如下：

|  |  |
| --- | --- |
| 時程 | 主題 |
| Day 1 | * Linux 程式開發+編譯與組譯技術 * Gdb(含gdb-peda) debug實務技術 * Linux執行檔分析[Linux Binary analysis] * Readelf+Objdump實務演練 |
| Day 2 | 基礎逆向工程實務演練   * 關鍵組合程式解讀 * CTF的基礎逆向工程解題 |
| Day 3 | PWN!PWN!PWN!   * 從Buffer overflow漏洞到format string attack * CTF的基礎PWN解題 |

* 辦理場次與地點：
* 南部於台南一中舉辦，活動資訊如下:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 時間 | 地點 | 主講人 | 活動人次 | 參與對象 |
| 107年1月25日 | 臺南一中 | 曾龍 | 28人 | 台南一中、新營高工、台南女中、台南附中 |
| 107年1月26日 | 臺南一中 | 林思辰 | 21人 |
| 107年1月27日 | 臺南一中 | 陳憶賢 | 19人 |

* 北部於成功高中舉辦，活動資訊如下:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 時間 | 地點 | 主講人 | 活動人次 | 參與對象 |
| 107年1月30日 | 成功高中 | 曾龍 | 33 | 成功高中、北一女中、明倫高中、麗山高中、大安高工 |
| 107年1月31日 | 成功高中 | 陳廷宇 | 32 |
| 107年2月1日 | 成功高中 | 張元 | 29 |

**2. MyFirstCTF資安競賽與培訓活動**

* 為激發學生資安學習興趣、說明CTF資安競賽內容以及推廣MyFirstCTF資安競賽，辦理7場MyFirstCTF Training活動，共計26所高中職學生、30所大學學生參與，總人次達260人次。
* MyFirstCTF共有62名學生參加競賽，包括有臺灣大學、成功大學、宜蘭大學、暨南大學、屏東大學、淡江大學、中國文化大學、亞洲大學、及臺灣科技大學、台北科技大學、虎尾科技大學、健行科技大學等共34位大專院校學生(男生31位+女生3位)。高中職學校有台南一中、台南女中、成功高中、高雄中學、新營高工、大安高工等共28位學生參與(男生27位+女生1位) 。相關統計數據如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **學校別** | **男** | **女** | **小計** | **註備** |
| 高中 | 27人 | 1人 | 28人 | 台南一中8人  成功高中5人  新營高工4人  大安高工3人  共計13所高中參與 |
| 大學 | 31人 | 3人 | 34人 | 健行科大6人  臺灣大學5人  臺灣科技大學4人  淡江大學3人  宜蘭大學3人  屏東大學3人  共計14所大學參與 |
| 小計 | 58人 | 4人 | 62人 |  |

* 此次競賽分數級距與大學/高中得分人次統計如下表所示，由表得知有52%的人得分1000分~1999分佔最多，其次為21%的人得分2000分~2999分，1000分以下的得分人數佔19%，3000分以上的得分人數佔8%。

|  |  |  |  |
| --- | --- | --- | --- |
| 分數級距 | 大學 | 高中 | 小計 |
| 5490分(滿分) | 0人 | 0人 | 0人 |
| 5000分~5489分 | 0人 | 0人 | 0人 |
| 4000分~4999分 | 0人 | 1人 | 1人 |
| 3000分~3999分 | 3人 | 1人 | 4人 |
| 2000分~2999分 | 6人 | 7人 | 13人 |
| 1000分~1999分 | 23人 | 9人 | 32人 |
| 500分~999分 | 1人 | 3人 | 4人 |
| 250分~499分 | 0人 | 7人 | 7人 |
| 50分~249分 | 1人 | 0人 | 1人 |
| 0分 | 0人 | 0人 | 0人 |

**MyFirstCTF 106年度首度辦理，獲得不錯成效，今年有62名學生報名，參賽獲的學生都能解出CTF題目，顯見已有一些資安認知與技術基礎。於競賽活動辦理之前，透過高中職生資安研習活動、CTF培訓課程以及BreakALLCTF線上體驗活動等，讓高中職生與資安初學者了解CTF競賽模式與解題技巧。107年度本計畫競賽活動，將移由子計畫二統籌規劃辦理，未來子計畫三將關注與擴大高中職生資安扎根之推廣與培訓。**

**3. 建立資安實務導師(mentor)制度與辦理相關培訓課程與活動**

* 資安實務導師(mentor)培訓制度結合國內業界與學界師資，以師徒制的方式傳授資安理論與實務技術，以培育兼具理論與實務能力的資安菁英人才與國際級資安實戰競賽選手。另為培訓後續各階段的學員，本計畫更規劃邀請導師及資深學員開授高階資安實務培訓課程、並與HITCON戰隊選手合作開授CTF高階培訓課程、指定實作、導師與學員面談授課、團體討論等原則進行；期間也透過期中、期末成果發表會等活動，檢視培訓成效。
* 資安實務導師邀請業界導師15名與學界導師7名，共計22位資安實務專家擔任導師，以導師個人或3-4人導師組成團隊進行培訓。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **場次** | **時間** | **地點** | **主題/活動** | **講師** |
| 1 | 106年4月29日 | 成功大學 | 高階資安實務培訓：  IOT security + HitCon CTF | 李倫銓 |
| 2 | 106年5月24日 | 臺灣科技大學 | 高階資安實務培訓(\*\*):  Memory Forensics and Malware Analysis  記憶體鑑識及惡意程式分析 | 邱銘彰 |
| 3 | 106年6月1日 | 成功大學 | 高階資安實務培訓(\*\*):  Memory Forensics and Malware Analysis  記憶體鑑識及惡意程式分析 | 邱銘彰 |
| 4 | 106年9月21日 | 臺灣科技大學 | CTF培訓:  ASIS CTF Final 2017難題神解 | 蔣盛文 |
| 5 | 106年10月15日 | 臺灣科技大學 | CTF培訓(\*):網站安全培訓課程 | 羅煜賢 |
| 6 | 106年10月15日 | 中興大學 | CTF培訓(\*):網站安全培訓課程 | 趙偉捷 |
| 7 | 106年10月15日 | 崑山科技大學 | CTF培訓(\*):網站安全培訓課程 | 曾龍 |
| 8 | 106年10月28日 | 臺灣科技大學 | CTF培訓:  Advanced binary exploitation | 吳哲仰 |
| 9 | 106年11月11日 | 中興大學 | CTF培訓(\*):  Begin Your smart PWNing Life | 吳哲仰 |
| 10 | 106年11月12日 | 崑山科技大學 | CTF培訓(\*):  Begin Your smart PWNing Life | 吳哲仰 |
| 11 | 106年11月19日 | 臺灣大學 | 高階資安實務培訓: Fuzzing 課程 | 蕭旭君 |
| 12 | 106年11月25日 | 中興大學 | 高階資安實務培訓:  Linux安全與Docker 安全 | 徐千洋 |
| 13 | 106年11月26日 | 臺灣大學 | 高階資安實務培訓:  Symbolic Execution課程 | 蕭旭君 |
| 14 | 106年12月08日 | 台北國際會議中心 | CTF培訓:  Attack and Defense CTF培訓 | 劉育全、張亭儀、鄭達群 |
| 15 | 106年12月10日 | 臺灣科技大學 | CTF培訓(\*):破密分析培訓課程 | 林思辰、楊明軒、趙偉捷 |
| 16 | 106年12月16日 | 中興大學 | CTF培訓(\*):破密分析培訓課程 | 林思辰、楊明軒、趙偉捷 |
| 17 | 106年12月17日 | 台南一中 | CTF培訓(\*):  破密分析培訓課程 | 林思辰、楊明軒、趙偉捷 |
| 18 | 106年12月23日 | 臺灣科技大學 | 高階資安實務培訓:  Web Security課程 | 蔡政達 |
| 19 | 107年1月29日 | 奧義智慧科技公司 | 高階資安實務培訓:  入侵鑑識調查經驗分享會 | 邱銘彰、叢培侃 |
| 20 | 107年2月10日 | 奧義智慧科技公司 | 高階資安實務培訓:  入侵鑑識調查經驗分享會 | 邱銘彰、吳明蔚 |

(\*)此活動與高中職生資安研習營合辦。 (\*\*)此活動與子計畫一合辦。

**資安實務導師制度之培訓已逐步發揮其效益，亮點培訓成果如下：**

* 第一屆學員羅煜賢學員持續參加第二屆資安實務導師(mentor)制度之培訓，其優異的表現也使其成為奧義智慧科技服份有限公司實習生，更進一步與資安產業鏈結。
* HITCON Final CTF 2017共有三個臺灣隊伍打進決賽，來自臺灣大學的balsn(王建元、陳威甯)，來自中央大學的DoubleSigma(張元、陳廷宇)以及交通大學的BambooFox(趙偉捷、黃冠智、蔡謦安)這三隊都有參與學生參與資安實務導師制度的培訓。
* 第二屆培訓學員中來自中央大學的DoubleSigma\_Ethereum團隊勇奪106年度AIS3 EOF CTF冠軍。
* 第二屆培訓學員中高雄美國學校的尤同學(高中生)勇奪第一屆MyFirstCTF冠軍。
* 第二屆培訓學員林子婷赴日本東京參加2017 SECCON CTF for Girls資安競賽勇奪第二名佳績。

**4. 配合國網CDX攻防平臺，建置ACTF演練題庫擴建與運用**

* 本計畫配合國家高速網路與計算機中心建置之國網攻防平臺（Cyber Defense Exercise, CDX），並進一步整合各子計畫資安實務演練題目，協助建立教學資源題庫。
* 本年度整合AIS3活動、資安初學者CTF體驗研習營等CTF題目資源，106年擴增題庫50題，另於104年至105年度累計建置25題，故共累計建置75題，並於105年於國網中心平臺CDX進行ACTF (Academic CTF)演練題庫平臺環境之建置。

1. **課程規劃與設計**
2. **課程目標與特色  
   (請簡述課程宗旨、學習目標、課程的特色(如跨域、跨校/系所、產學合作等))**

資安威脅日益龐大，並已擴及到各新興科技領域，從手機、雲端、基礎關鍵設施到物聯網、車聯網與智慧城市都面臨必須加以重視的嚴重地步。世界各國紛紛提出許多資安政策來強化國家層級的資安。我國行政院國家資通安全會報提出「國家資通安全發展方案(106-109年)」，期透過前瞻、宏觀的視野，提出國家級的資通安全上位政策，以因應我國特殊的政經情勢及全球複雜多元的資通訊變革，並作為國家推動資安防護策略與計畫之重要依據。當前重要成果包括2018年5月11日立法院院會中，順利完成《資通安全管理法》三讀，法條經由總統公告後，正式施行日期將由行政院另行公告。在其法條中第四條規範:「為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：

一、資通安全專業人才之培育。

二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。

三、資通安全產業之發展。

四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。

前項相關事項之推動，由主管機關以國家資通安全發展方案定之。」

誠如國安會諮詢委員李德財院士表示: 「…(政府)必須要投入資安人才與人手的培育和培訓，畢竟，世界各國對於資安人才需求孔急，必須有一套培養機制，方能滿足政府及產業的資安人才需求」。李院士更表示「不只公務人員必須面對資安人力缺口的現況，私部門也同樣必須和公部門一樣，以各種方式，設法補足公、私部門的資安人力缺口，而這些面向，也是《資通安全管理法》通過後，從政府部門到產業都必須深刻面對的當務之急」。

為因應國家發展資安需求，配合第五期「(106年至109年)資通安全發展方案」(草案)、行政院科技會報辦公室「數位國家‧創新經濟發展方案（2017-2025年）」、行政院五大產業創新「國防產業－資安」暨資安即國安策略等政策推動策略，以及架構於教育部「推動產學研鏈結與前瞻科技人才培育」科技施政目標下，由教育部與經濟部共同推動「資訊安全人才培育計畫」，以挹注資安培育環境布建，厚植產業資安專業及具跨域資安技能人才為實施重點，配合在地創新聚落，國防資安產業之強化，結合國內大學校院資安教學能量，培養資安實務應用人才，來帶動國內資安產業自主研發氛圍。鑑於國內資安實務教學的師資較為不足，且對於學生資安實務技術的培訓不易與產業應用鏈結，教育部「資訊安全人才培育計畫」推動新型態資安實務暨示範課程，鼓勵大專校院教師發展創新、翻轉及具示範的資安實務課程教學方法，強調資安實務/實戰演練、專題實作、及鼓勵整合相關產業資安實務需求，設計與開設跨域/跨際之資安實務課程示範課程，以期能建立整合產學與跨域的資安實務師資團隊並建立示範教學資源，並擴散與提升國內資安實務教學能量。此外，也配合國網中心CDX (Cyber Defense Exercise)攻防平臺，整合與建立資安實務教學環境與平台，用於資安實務課程教學之中。另外藉由資安實務專題講座課程等配套措施，將示範課程的資安實務教學能量擴散至國內各大學的資安實務課程教學中。

資安人才培育制度不僅需考量不同層級的各種策略，並配合不同階段提出精進作法。在現有的政策架構下，為擴大資訊安全人才培育的長遠目標，宜扎根於更廣大的學生包括非資訊類別的大專生與高中職學生。特別是教育部正在堆動的12年國民基本教育課程綱要。課綱其目的是整合12年國教從國小到高中課程，解決過去國中小9年一貫與高中課綱分開的銜接落差。高中學科的必修時數下降，選修課學分占了1/3。且各高中須以發展特色，增加4到8學分「校訂必修」。課綱要成就每一個孩子，也是第一個以學生為中心的課程綱要，他將學生的學習定位從應付升學考試到學習者為中心。但新課綱大量的選修和跨領域課程，考驗老師的教學與規劃課程的能力。誠如師大教育政策與行政研究所副教授陳佩英所說「過去教學改變都在外圍，靠老師的熱情；但新課綱，把改變變成主流，將會帶來系統性影響」。

本計畫將推動資安認知教育，針對認知層級的資安教育提出相關作法包括教學內容與課程規劃、教學配套環境與示範影片、學習評量與實測。本計畫也將配合教育部資安人才培育計畫舉行高中職生資安種子師資培訓課程，邀請與輔導各高中職教師及各大專校院開設資安通識課程。

**課程宗旨**

本計畫的宗旨在於規劃與設計及製作資安認知層級的模組化課程相關教學環境，規劃不同學習模組提供給非資訊相關的大專院校及各高中職學校進行資訊安全教育。要給非資訊相關的大專院校及各高中職學校的資安認知教育需要考量到上述學生並不具備資訊相關基礎，因此課程設計上必須將相關必要知識以生動活潑的方式讓學生可以掌握基本觀念。本課程模組強調以動手做的精神讓學生從觀念到實作上都能整合，避免枯燥的理論教學。考量到國內學生的學習模式，部分課程將透過搶旗大賽的模式安排學習，透過解題的形式來引領學生掌握依安分析的技術。本課程另外將特別強調資訊安全防禦技術的實測，透過開放原始碼的系統使學生能盡早掌握現今網路環境常用的資訊安全防禦系統包括網路防火牆、網路入侵偵測系統與網站應用程式防火牆的技術。如果只是單純介紹相關理論知識，會過於枯燥乏味，本計畫規劃實際攻擊場景並實際教導學生設計與採用適當規則來加以防禦系統的技術。本計畫更推動培養學生自主學習，因此本課程規劃延伸學習，不僅提供學習資源提供學生自主學習外，還將鼓勵與輔導優秀且有強烈學習意願的學生進一步參加教育部資訊安全人才培育的更多活動，包括參加資安研習營、參與MyFirstCTF及AIS3 CTF等競賽。最後必須強調的是在學生學習資安測試同時須及早引進相關資訊倫理及法律相關主題，特別是我國已經於今年(2018)已經通過資安管理法。有關資訊倫理及法律的主題宜以生動的案例加以呈現，本計畫亦將以個案分析與說明引領學生掌握上述重要的主題。

**課程目標**

本計畫規劃的模組化課程依照不同的範疇有不同的課程學習目標。各課程模組不僅講授相關基本知識外更強調實作學習，基本知識的講授將提供所有上課簡報與部分影片教學，實作學習則供學習環境與配套工具。底下分別論述相關的學習目標。

《從資訊安全到資訊倫理與法律》模組將強調資訊倫理的重要性，將以生動的說明來強調資訊倫理上四大議題(Mason的PAPA模式)。另將以案例的方式說明國內外資安事件與相關的法律(包括我國通過的資通安全管理法與歐盟GDPR等)，以建立學生正確的行為。

《Linux安全測試基礎》模組主要透過動手做的精神來學習開放原始碼最著名的作業系統，為避免枯燥的指令教學本課程設計以CTF解題模式來學習相關指令，從實際解題過程了解與學習到相關指令的用途。此應用導向的學習模式可以快速使學生掌握作業系統所提供的更多工具使用，本課程將引領學生認知作業系統行程管理的觀念與實作，網路指令的使用等主題。

《隱寫術》課程模組將透過CTF平台的解題來訓練學生熟悉隱寫術(Steganography)的觀念與技術。課程將包括文件隱寫術與圖片隱寫術的技術，在文件隱寫術上教導學生網路不明的文件、圖片、音樂與影片不要隨便下載，特別是被不肖人士用來進行社交攻擊的檔案通常都會夾帶木馬及後門程式。為避免學生誤入歧途，本課程將以CTF題目來展示隱藏在檔案及圖片的資訊，此課程可讓學生了解隱寫術的技術及資安分析技術。本課程將訓練學生善用Linux平台上的binwalk 及dd工具來解析檔案隱藏的資訊。

資訊安全課程一定要講解密碼學的相關觀念，但資訊背景的大學密碼學課程以密碼演算法為主的教學並不適用於高中職及非資訊背景的學生學習。《基礎加密/解密與破密》課程模組將以生動的案例學習讓學生學習到密碼學的相關觀念及實作技能，課程主要先以古典密碼學來教導學生了解何謂加密與解密，課程動手做的部分將以CTF題目解題並透過使用網路線上工具來解題。課程包括凱薩密碼、暴力破解法與頻率分析法等技術。

《使用Python進行加解密與破密》課程模組係深化《基礎加密/解密與破密》的內容，在《基礎加密/解密與破密》課程主要係以網路線上工具來解題，本課程則強調使用程式設計的技術來教導學生解題。在眾多程式語言學習上本計畫規劃以python程式作為主要教學主軸，python程式不僅易學且在大數據分析及人工智慧的應用上有著強大的優勢。大部分學校程式設計強調語法學習與演算法設計，本計畫強調應用導向的學習，透過密碼相關主題使學生掌握應用領域的相關技能，如此可開闊學生學習的視野。本課程和上述《基礎加密/解密與破密》組合成獨立學習單元，並可以《Python程式設計與密碼學應用》或《Python程式設計與加解密及破密上的應用》為主題來教導學生。《現代密碼加解密與破密(初體驗)》模組本課程將教授現代密碼學的加密與解密，包括非對稱式的RSA及對稱式DES及AES密碼學的基本觀念。本課程不涉及密碼學演算法的教學，而將先讓學生透過openssl及python程式實測密碼學的加解密。唯有先讓提高學生學習興趣，後續再鼓勵學生後續研究相關演算法及其實作。修完此課程模組的學生將會應用openssl及python程式完成非對稱式的RSA加密與解密實測、DES及AES密碼的加密與解密實測。另外有將於CTF題目中學習到基礎的RSA破密分析。

《編碼與解碼》課程模組將教授資訊科技常用的編碼與解碼技術。在高中職的資訊科技概論課程大都編列章節來說明原理，但卻欠缺實作主題，本課程將以實測的角度訓練學生使用線上工具實際完成不同編碼與解碼技術，修完此課程模組的學生將學會base64/base32/Morse code等編碼與解碼技術，並將完成CTF平台上的題目。

《網路安全與封包分析》模組主要教導學生網路協定分析與攻擊封包分析。本課程模組將實際以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。學生學完基礎課程模組將可使用wireshark /tshark進行封包分析。進階課程模組將 以CTF平台上的攻擊封包分析題目來深刻化學生學習。

《網路安全之防火牆實務》模組主要教導學生網路安全上最基本的防火牆觀念與實務。學生將可學會檢視規則和狀態、配置防火牆的設定、規則分析與撰寫等技術。本課程也將規劃實際的攻擊防禦案例實測使學生了解網路防火牆的用途，課程實作上將使用Ubuntulinux環境的Iptables/ ufw設定防禦規則，來實際進行網路防禦的實際演練。

《網路安全之入侵偵測系統實務》模組主要教導學生網路安全上常使用的入侵偵測系統觀念與實務。不僅教導主機型入侵偵測系統也將實測網路型入侵偵測系統。學生將可學會檢視入侵偵測系統規則、入侵偵測系統的設定、規則分析與撰寫等技術。本課程也將規劃實際的攻擊防禦案例實測使學生了解入侵偵測系統的用途，課程實作上將使用Ubuntu linux環境的snort設定防禦規則，來實際進行網路防禦的實際演練。

《網站安全分析模組》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，課程將以CTF題目來強化學生的安全測試能力。學生學習此課程基礎部分將會使用developer tools、curl、burpsuite等工具來進行基礎的網站安全測試，學生也將學會使用上述工具完成CTF平台上的解題。

進階部分將講授OWASP TOP 10(2017)所揭露的部分常見的網站漏洞，課程將實際演練file inclusion漏洞並實際示範黑名單過濾機制並實測bypass的攻擊技術最後再以完整的技術進行防禦，以一完整的實測案例教導學生網站安全的攻防技術。學生學習此課程進階部分將深刻理解網站漏洞及其可能造成的威脅，同時學生也將學會CTF平台上的解題。

《網站安全防護實務:WAF》模組主要教導學生網站安全防護常使用的網站應用程式防火牆的觀念與實務。課程將以Modsecurity及DVWA漏洞平台進行實測。mod\_security是支援Apache的一個模組，可以提供Web攻擊或Web入侵偵測及防禦，可建構它來抵擋相關的Web攻擊方式，例如資料隱碼攻擊（SQL injection Attacks）、跨網站Script攻擊（Cross-site Scripting）、目錄路徑外洩（Path Traversal Attacks）等相關的Web攻擊。學生學完本課程模組後將可以如何設定網站應用程式防火牆，並將完成實際的網站攻防實務。

《系統安全》模組主要教授系統安全的基本觀念。課程將規劃一攻擊防禦實測案例，學生將實際以kali linux的nmap 及metasploit針對windows系統進行攻擊，課程也將實測如何使用windows系統的工具進行防禦。學生學完本課程模組後將可以熟悉滲透測試的基本技術與系統的安全防禦技術。

《新興資訊安全課題》模組主要將以生動活潑的模式引領學生關注日常生活所常會遇到的資安課題，另將涵蓋《人工智慧與資訊安全》、《行動APP安全》與《雲端安全》等主題。其中《行動APP安全》與《雲端安全》將以學生常使用的雲端服務加以說明宜注意的資安警覺而行動APP安全將以影片展示說明不安全的APP下載會造成的傷害。《人工智慧與資訊安全》則主要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。學生學習此課程後將會使用Google所提供的Google Colaboratory平台作為主要的人工智慧教學平台。Google Colaboratory主要目的是想要幫助機器學習和人工智慧教育的推廣。它是一個提供Jupyter Notebook服務的雲端環境，無需額外設定就可使用，並且還提供免費的GPU使用。Google Colaboratory平台預裝了一些做機器學習與深度學習常用的套件，像是 TensorFlow、scikit-learn、matplotlib、numpy、pandas等，本計畫將使用Google線上人工智慧平台作為”人工智慧與資訊安全”課程模組的實作場域。另外本課程有將教導學生安裝Google　Colaboratory平台未安裝的套件（例如Facebook在 2017年開源的PyTorch）。本課程另外將示範人工智慧在資訊安全分析的應用。

課程的特色(如跨域、跨校/系所、產學合作等):

本計畫提出的課程模組具備下列特色:

1.資安實務導向課程設計，不僅實務教授資安測試的攻擊面手法更提供防禦的主題:

本課程以實測情境模式(攻擊與防禦的實測)使學生動手實測網路防火牆、入侵偵測系統與網站程式防火牆等現階段政府單位及一般企業都在使用的安全機制與設備。透過此實作可以大幅提升學生的學習意願與資安認知(資安素養)。

2.可配合與支援國內十二年國教的課綱設計

我國十二年國教的課綱即將實施，本課程可以配合與支援國內十二年國教的實施。現行高中職生的資訊 科技概論課程有章節教導網路概論，但大部分現行教材幾乎全都是單純的觀念並無任何實作內涵。本計畫的網路安全分析模組以wiershark實測模式透過動手實測的學習模式可以大幅提升學生的學習意願。

3. 跨域、跨校/系所的推動模式

本示範課程計畫將直接與高中職學生合作並採取不同模式進行推廣。

第一種模式採取直接與各高中職直接開設的特色選修模式。

另外第二種模式則是採取在現有課程內(例如資訊科技概論)加入個別模組。

本計畫推薦與規劃推動第二種模式可以提供的教材包括:

加解密等課程模組可以在(Python)程式設計等課程加以運用。

網路分析模組可以在資訊科技概論相關章節直接使用。

人工智慧與資安分析模組可以在新興科技相關章節使用。

4.整合新興科技(人工智慧)的主題

新興科技(人工智慧)是全球及我國國家發展的重大發展政策，聚焦於人工智慧的人才培育是各國激烈競爭的場域。如何在通識與認知課程領域使非資訊類大專學生及高中職學生能盡早了解人工智慧及其在安全的威脅與應用是本課程特色之一。這些課程可在不強調大量數學知識與程式實作上將使學生被GAN、CNN及其應用大為驚豔。另外人工智慧所產生的資安威脅與人工智慧強化的資安防護是各國大幅關注的領域，本課程也將從認知層級規劃部分實作課程並利用google所提供的平台體驗使用python程式來執行簡易的人工智慧主題。為加深學生延伸學習，本計畫更提供錄影教學來示範建置單純使用CPU所建置的平台與深度使用GPU所建置的平台提供學生深入學習。

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:

為避免學生在學習過程及日後就業面臨不當的行為所產生的倫理與法律問題，本課程在授課之初就強調資訊倫理及法律的正確觀念，特別是我推動的資安管理法及其他各資相關法律對所有學生及國民都有所規範。

推動策略

本計畫提出的課程模組將依底下兩大方向推動:

1.配合教育部資安人才培育計畫舉行高中職生資安種子師資培訓課程

為落實國家資安整體計畫，本計畫將配合教育部資安人才培育計畫種辦公室舉行高中職生資安種子師資培訓課程。受訓對象為高中職教師及大專校院的通識課程教師，培訓主題則是通識與認知層級的資安教育教學經驗分享，舉辦過程中也將與各參與學校建立聯繫，並提供相關諮詢管道以建立後續輔導與推動資安認知課程。

2.邀請與輔導各高中職教師及各大專校院開設資安認知課程

透過總計畫所舉辦的各種活動，本計畫將建立各校聯絡清冊，並邀請與輔導各高中職教師及各大專校院開設資安認知課程。就現有課程教學模組上，可以搭配資訊科技概論或計算機概論等課程的開設，將相關主題(例如編碼與解碼、加密與解密、網路)的教學簡報、影音教學與線上評量平台(主要以CTF競賽模式)提供給教師使用。

3. 與現有高中職學科中心合作:

本計畫將與相關高中職學科中心(例如設置於台南二中的「高中資訊學科中心」)合作，推動相關課程模組，以利資安基礎及認知教育課程推廣至全國高中。

1. **課程網要與教學導引**
   1. **課程綱要與導引**

**(建議以模組化設計，說明課程主要內容，並說明課程目的與綱要、教學活動規劃、教學導引與建議等；下表為範例格式，可自行增加/調整欄位說明課程設計)**

|  |  |  |  |
| --- | --- | --- | --- |
| **課程模組名稱** | **教學目的與課程綱要** | **教學活動規劃**  **【註1】** | **教學導引與建議** |
| 從資訊安全到資訊倫理與法律 | 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）。 | 總授課時數2小時，  課程觀念介紹30分鐘、案例分析1小時30分鐘。 | 課程難易度：易  教學方式：先講授資訊安全基本觀念，並以實際資安威脅案例加以說明。接著以案例分析方式說明資訊倫理的主題，最後介紹資安相關法律包括我國剛通過的資安管理法。 |
| Linux安全測試基礎 | 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。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：易  教學方式：先講授linux作業系統基本觀念再以CTF平台使用Linux常用指令進行解題以動手做的方式熟悉Linux作業系統。  教學資源建議：本課程模組需建置linux，本計畫將提供相關教學環境的image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 隱寫術 | 本課程將透過CTF平台的解題來訓練學  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。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：易  教學方式：先講授隱寫術基本觀念再以CTF平台使用binwalk 及dd進行解題以動手做的方式熟悉隱寫術。  教學資源建議：本課程模組需建置linux，本計畫將提供相關教學環境的image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 基礎加密/解密與破密 | 本課程將教授基本古典密碼學的加密與解密，並實際以線上工具完成破密。本課程將使用ＣＴＦ平台上的題目進行實際演練。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：易  教學方式：先講授基本古典密碼學的加密與解密基本觀念再以CTF平台使用以動手做的方式熟悉古典密碼學的破密。  教學資源建議：  課程模組將利用網路線上工具講授實際基本古典密碼學的加密與解密的作法。本計畫將提供相關教學環境的image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 使用Python進行加解密與破密 | 本課程將教Python程式設計技術，為強化學習，本計畫以進階的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。 | 總授課時數4小時：  課程理論簡介1小時、授課與實習操作3小時。 | 課程難易度：中  教學方式：先講授python程式技術再以解CTF平台的題目作為應用以強化學生的運算思維能力及其實際解決問題的能力。  教學資源建議：本課程模組需建置linux，本計畫將提供相關教學環境的image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 現代密碼加解密與破密(初體驗) | 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。 | 總授課時數2小時，  課程觀念介紹1小時、授課與實習操作1小時。 | 課程難易度：中上  教學方式：先講授現代密碼學的加密與解密，包括RSA及AES密碼學的基本觀念術再以openssl及Python模組進行加解密使學生了解不同密碼學的加解密運用。接著在CTF平台進行解題以動手做的方式熟悉破密分析。  教學資源建議：本課程模組需建置linux，本計畫將提供相關教學環境的image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 編碼與解碼 | 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。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：易  教學方式：先講授不同編碼與解碼，包括ASCII及Base64編碼與解碼的基本觀念再以線上工具實際演練CTF平台上的編碼與解碼題目。  教學資源建議：  本課程模組將利用網路線上工具講授實際編碼與解碼的作法。本計畫將提供相關教學環境的image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 網路安全與封包分析 | 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。  最後再以CTF題目來深刻化學生學習。 | 總授課時數4小時，  課程理論簡介1小時、授課與實習操作3小時。 | 課程難易度：中  教學方式：先講授網路協定基本觀念再以wireshark實作環境搭配實驗情景實際演練網路協定的封包分析，最後再教導學生利用CTＦ平台所建置的攻擊封包進行分析。  教學資源建議：本課程模組需使用wireshark /tshark，本計畫將提供相關教學環境的image檔案與教學手冊。  另外CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 網路安全之防火牆實務 | 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。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：中  教學方式：先講授防火牆基本觀念再以實作環境搭配實驗情景實際演練防火牆規則撰寫與防禦技術。  教學資源建議：本課程模組需建置防火牆的設定，本計畫將提供相關教學環境的image檔案與教學影片及手冊。 |
| 網路安全之入侵偵測系統實務 | 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。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：中  教學方式：先講授入侵偵測系統基本觀念再以實作環境搭配實驗情景實際演練入侵偵測系統規則與防禦技術。  教學資源建議：本課程模組需建置入侵偵測系統的設定，本計畫將提供相關教學環境的image檔案與教學影片及手冊。 |
| 網站安全分析模組 | 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。進階部分將講授OWASP TOP 10(2017)所揭露的部分常見的網站漏洞，課程將實際演練file inclusion漏洞並實際示範黑名單過濾機制並實測bypass的攻擊技術最後再以完整的技術進行防禦，以一完整的實測案例教導學生網站安全的攻防技術。 | 總授課時數6小時，  課程觀念介紹2小時、授課與實習操作4小時。 | 課程難易度：中上  教學方式：先講授並實際演練HTTP協定及其相關測試工具包括developer tools、curl、burpsuite等工具，並配合CTF題目來強化學生的安全測試能力。再以實作環境搭配實驗情景實際演練網站的攻擊與防禦技術。  教學資源建議：  本課程模組需建置DVWA網站安全測試平台，本計畫將提供相關教學環境的image檔案與教學影片及手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 網站安全防護實務:WAF | 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。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：中  教學方式：先講授入侵偵測系統基本觀念再以實作環境搭配實驗情景實際演練入侵偵測系統規則與防禦技術。  教學資源建議：本課程模組需建置入侵偵測系統，本計畫將提供相關教學環境的image檔案與教學影片及手冊。 |
| 系統安全 | 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系統進行攻擊，課程也將介紹如何使用windows系統的工具進行防禦。 | 總授課時數2小時，  課程觀念介紹30分鐘、授課與實習操作1小時30分鐘。 | 課程難易度：易  教學方式：先講授系統安全基本觀念再以實作環境搭配實驗情景實際演練入侵偵測系統規則與防禦技術。  教學資源建議：本課程模組需建置入侵偵測系統的設定，本計畫將提供相關教學環境的image檔案與教學影片及手冊。 |
| 人工智慧與資訊安全 | 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。 | 總授課時數2小時，  課程觀念介紹1小時、授課與實習操作1小時。  另外規劃錄製影片提供學生延伸學習2小時內容，本計畫將提供學生後續研讀的自主學習教材。 | 本課程難易度：中上。教學方式：將採觀念說明與利用Google平台進行實作。另外本計畫也將利用採購的教學設備錄製影片教導學生如何建置人工智慧分析平台與進階教學內容。  教學資源建議:建置人工智慧分析平台宜利用本地端教學環境，後續教學則可利用建置的伺服器與Google雲端平台。 |

**註1**：若有安排參訪、實習或實驗，請於｢參-三、教學方式與課程配套｣補充相關資訊。

* 1. **開課與進度規劃**

**(請說明課程之開課規劃與授課進度規劃)**

本計畫將先行於107學年1學期與試辦學校(台南一中與新營高工)就教材發展上先行試驗部分課程模組。正式試辦課程將於107學年2學期開始。

|  |  |  |
| --- | --- | --- |
| 學期 | 參與學校 | 推廣模式 |
| 107學年1學期 | 台南一中高中3年級選修課程 | 特色課程(詳見後述) |
| 新營高工《程式設計實習》 | 多課程模組(詳見後述) |
| 台南黎明高中《資訊科技概論》 | 單一課程模組  編碼與解碼 |
| 107學年2學期 | 台南一中高中1年級選修課程 | 特色選修課程 |
|  | 崑山科技大學通識課程  資安攻防面面觀 | 通識課程 |
| 108學年1學期 | 各校推廣 |  |

大學通識課程及高中職特色選修課程主題相近，各校可依照其不同的需求規劃與使用不同的課程模組，底下以107學年2學期預計開設的特色選修課程將以呈現:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 課程名稱 | | (中文)資訊安全新體驗  (英文) A Practical Introduction to Security | | | |
| 開課老師 | | 曾龍、高英耀 | | | |
| 課程  基本  資料 | 開課系所 | | | 跨校開課 | |
| 國立台南一中高三特色選修課程 | | | ▓ 無  □ 有，共同開課學校與系所名稱： | |
| 學分數 | 開課時間 | 開課週期 | 課程屬性 | 授課對象 |
| 2 | 107學年  2 2學期 | □每學期  ▓每學年 | ▓新開課程  □原有課程 | ▓高中 1年級  □大學 年級  □碩士班  □博士班 |
| 上課時數 | 實習/實作  時數 | 預估  修課人數 | 本課程有無須搭配先修課程或核心技能 | |
| 40時/20週 | 1~1.5時/每週 | 30 | □有，課名:  □有，核心技能:  ▓無 | |
| 本課程使用之教科書(非新編或編修) | |
| 自編教材 | |

| **授課進度** | | | |
| --- | --- | --- | --- |
| **週數** | **內容** | **授課教師**  **【註2】** | **授課方式** |
| 第一週 | 從資訊安全到資訊倫理與法律 | 曾龍 | 基礎/理論課程授課 |
| 第二週 | Linux安全測試基礎 | 高英耀 | 基礎/理論課程授課/實作 |
| 第三週 | 隱寫術 | 高英耀 | 基礎/理論課程授課/實作 |
| 第四週 | 加密/解密與破密 | 曾龍 | 基礎/理論課程授課/實作 |
| 第五週 | 使用Python進行加解密與破密(1) | 曾龍 | 基礎/理論課程授課/實作 |
| 第六週 | 使用Python進行加解密與破密(2) | 曾龍 | 基礎/理論課程授課/實作 |
| 第七週 | 現代密碼加解密與破密(初體驗) | 曾龍 | 基礎/理論課程授課/實作 |
| 第八週 | 編碼與解碼 | 高英耀 | 基礎/理論課程授課/實作 |
| 第九週 | 期中考 | 高英耀 | 實作/學習評量 |
| 第十週 | 網路安全與封包分析(1) | 曾龍 | 基礎/理論課程授課/實作 |
| 第十一週 | 網路安全與封包分析(2) | 曾龍 | 基礎/理論課程授課/實作 |
| 第十二週 | 網路安全之防火牆實務 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十三週 | 網路安全之入侵偵測系統實務 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十四週 | 網站安全初體驗 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十五週 | 網站漏洞分析(1) | 曾龍 | 基礎/理論課程授課/實作 |
| 第十六週 | 網站漏洞分析(2) | 曾龍 | 基礎/理論課程授課/實作 |
| 第十七週 | 網站安全防護實務:WAF | 曾龍 | 基礎/理論課程授課/實作 |
| 第十八週 | 系統安全初體驗 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十九週 | 人工智慧與資訊安全 | 曾龍 | 基礎/理論課程授課/實作 |
| 第二十週 | 期末考 | 高英耀 | 實作/學習評量 |

**註2**：課程單元如係「搭配外聘專家講課」者，請於｢伍、參與師資-二、外聘專家簡介｣略述外聘人員(如業師)之學經歷背景及講述主題。

另外本計畫也將提出在高中職資訊安全的新型教學模式。由於各高中職學校對於新興科技及資訊科技有龐大教學需求，但卻苦無協助學校。本計畫將推動部分課程融入「資訊科技概論」。底下根據教育部國民及學前教育署網站(<https://www.k12ea.gov.tw/ap/download_view.aspx?sn=e4fde167-fc32-485b-8296-996f58fe3303>) 以高中生為主的必修科目二學分之「資訊科技概論」推薦本計畫所規劃的課程模組:

|  |  |  |  |
| --- | --- | --- | --- |
| **主題** | **主要內容** | **說明** | **推薦之課程模組** |
| 一、導論 | 1.資訊科學簡介 | 1-1資訊科學素養  1-2資訊科學本質與內涵 | 無 |
| 2.資訊科學發展 | 2-1電腦發展  2-2資訊科學發展重要里程碑 |
| 3.電腦基本原理 | 3-1數位化觀念與二進位系統  3-2基本數位邏輯處理※ |
| 二、電腦硬體 | 1.電腦硬體概論 | 1-1電腦基本組成  1-2電腦設備使用 | 無 |
| 2.電腦硬體基本單元 | 2-1處理單元  2-1-1 處理單元功能及結構  2-1-2 處理單元效能  2-1-3 指令運作週期※  2-2記憶單元  2-2-1 記憶單元功能  2-2-2 常見儲存裝置  2-2-3 記憶單元儲存原理  2-3輸入、輸出單元  2-3-1 常見輸入、輸出裝置  2-3-2 輸入、輸出單元工作原理  2-4基本單元間關係  2-4-1 內部連結方式  2-4-2 外部連結方式 |
| 三、電腦軟體 | 1.電腦軟體概論 | 1-1資料數位化  1-2軟體運作原理  1-3軟體分類 | 1-1資料數位化  可搭配之課程模組:  (1)編碼與解碼[2小時]  2-2作業系統功能  可搭配之課程模組:  (2)Linux實務[2小時] |
| 2.系統軟體 | 2-1系統軟體簡介  2-2作業系統功能 |
| 3.應用軟體 | 3-1應用軟體簡介  3-2應用軟體實作 |
| 四、電腦網路 | 1.電腦網路概論 | 1-1網路發展  1-2網路功能  1-3網路運作原理※ | 1.電腦網路概論可搭配之課程模組:  [1]網路封包分析實務  [2小時]  3-2網路安全防護可搭配之課程模組:  [2]防火牆攻防實務[2小時]  [3]入侵偵測系統攻防實務[2小時] |
| 2.網際網路 | 2-1網際網路架構  2-2網際網路服務  2-3網站建置與維護※ |
| 3.網路安全 | 3-1網路安全問題  3-2網路安全防護 |
| 五、電腦與問題解決 | 1.電腦解題概論 | 1-1電腦解題簡介  1-1-1垂直式邏輯思考  1-1-2循序漸進的流程  1-2電腦解題在各領域之應用 | 無 |
| 2.電腦解題程序 | 2-1問題分析  2-2解題方法設計  2-3測試與修正 |
| 3.演算法概論 | 3-1演算法特性  3-2演算法表示方法  3-2-1演算法基本元件  3-2-2演算法基本元件組合  3-3資料結構與演算法※  3-4演算法與電腦解題 |
| 4.電腦解題實作  ※ | 4-1電腦解題工具介紹  4-2解題實作 |
| 六、資訊科技與人類社會 | 1.資訊科技與生活 | 1-1資訊科技與生活的關係  1-2資訊科技的優點與限制  1-3未來的資訊科技 | 1-3未來的資訊科技  可搭配之課程模組:  (1)人工智慧[2小時]  (2)《行動APP安全》[1小時影片教學]  (3)《雲端安全》[1小時影片教學]  3-2資訊倫理與道德  可搭配之課程模組:  (1)《從資訊安全到資訊倫理與法律》模組 |
| 2.資訊科技與學 習 | 2-1電腦輔助學習軟體  2-2電腦網路與學習  2-3電腦輔具與無障礙設計 |
| 3.資訊社會相關議題 | 3-1電腦使用與身心健康議題  3-2資訊倫理與道德  3-3資訊相關法律問題 |

本計畫將與新營高工合作，善用協同教學模式，在現有程式設計課程中加入資訊安全的應用。本計畫將於107學年第一學期在新營高工合開課程，課程名稱為《程式設計實習》，先由新營高工資訊科陳忠謀主任教授Python程式設計的技術，再由本計畫主持人教授Ｐython程式設計與資訊安全上的應用，相關教材將陸續輔導新營高工使該校能充分從協同教學模式中逐步建立新興科技及資訊科技上資訊安全的教學。底下列出六周的授課內容：

|  |  |  |  |
| --- | --- | --- | --- |
| 週數 | 內容 | 授課教師  【註2】 | 授課方式 |
| 第十四週 | Linux實務演練 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十五週 | 使用python進行編碼與解碼 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十六週 | 加密/解密與破密 | 曾龍 | 基礎/理論課程授課/實作 |
| 第十七週 | 使用Python進行加解密與破密(1) | 曾龍 | 基礎/理論課程授課/實作 |
| 第十八週 | 使用Python進行加解密與破密(2) | 曾龍 | 基礎/理論課程授課/實作 |
| 第十九週 | 現代密碼加解密與破密(初體驗) | 曾龍 | 基礎/理論課程授課/實作 |
| 第二十週 | 期末考 | 陳忠謀 | 實作/學習評量 |

本計畫在107學年第一學期將先與上述兩所學校進行實際示範教學，發展不同模組教材。後續將配合總計畫規畫進行高中職資安種子師資培訓。107學年第二學期將正式試辦課程模組的示範教學，於108學年第一學期再增加輔導不同學校的的資安認知與體驗課程，全部計畫將完成十所學校的實際授課輔導。由於本課程採模組化設計，參與的學校可以利用不同的課程加以運用，例如資訊科技概論課程中部分章節如網路概論可以使用本計畫的課程模組及CTF平台的題目來強化學生實際動手做的能力與強化學生學習意願。

1. **教學方式與課程配套**
2. **教學方式說明**

**(請就教學前的課程準備及教案設計等，若為跨域/跨系所/跨校等課程特色如何進行、是否有創新的教學方式導入課程中等教學方式進行說明)**

**教學前的課程準備：**

本計畫規劃與提供課程教學簡報與相關實作環境及線上實習平台，並配合教學影片的錄製及Moocs線上教學，可提供教師授課前的課程準備，也可提供學生課前的預習與課後複習用。相關教學影片及Moocs線上教學說明請參見第四章。

**教案設計：**

本課程特別考量資安認知教育的對象並不具備資訊背景的知識，因此教案設計上特別考量學生如何掌握相關基本背景知識。以網路安全分析為例，大學非資訊科系及高中職學生通常都沒有學習過TCP/IP協定，本課程皆以生動的簡報與圖示並配合wireshark實作，使學生動手實作中了解主要協定的內涵，最後還將以實際的CTF題目講解來使學生深化所學到的觀念與技術«

**跨域/跨系所/跨校等課程特色的進行模式：**

本計畫實際參與各高中職的資安認知教育，並以實際學校課程實施來展示課程模式的運用。本計畫除直接與高中職老師合開資安認知課程(台南一中)外，也協助高中職老師再現有的課程內融入相關的資安教育(新營高工的程式設計實習課程)。初期階段使用新營高工協同教學的模式將可以讓大部分學校快速引入本課程相關模組。例如高中職學校的計算機概論或資訊科技概論課程有網路章節，可以鼓勵與輔導高中職學校教師將本課程網路分析模組納入其現有課程中。部分學校對於網路有特別的教學需求者可以將進階的網路安全之房或搶與入侵偵測系統納入其特色教學上。

**創新的教學方式：**

本課程不同於平常教學模式，特別強調由實作學習模式。平常教學模式通常先講授基本觀念後再實際演練為主，若無實際演練場景的教學，通常學習常會流於枯燥。本課程提出的實作學習模式係先讓學生學會基本工具及使用技術後再配合相關解題使學生充滿學習意願，先知其然後再讓學生知其所以然的教學模式。

1. **資安實務或實戰演練課程的教法與設計**

**(請就實務課程的教法、教學環境設計、課程操作或實務個案等進行說明)**

實務課程的教法

本計畫推動的實務課程教法強調動手實作中學習相關的技能與觀念，以本計畫目標學生而言，都未曾學習過Linux，因此課程教學上將先提供Linux教學環境，讓學生透過現場操作Linux指令來完成CTF題目。每一題目規劃不同指令，從基本的題目到進階題目都以實作方式完成，授課過程中再搭配觀念講解可以使學生快速掌握與

Linux作業系統。若只單純教導指令而缺乏有趣的個案實作將使學生學習低落，因此在隱寫術課程模組將進一步強化使用Linux作業系統的binwalk 及dd等工具，透過解題圖片隱寫術的CTF題目，可再進一步深化學習到的Linux。另外使用Python進行加解密與破密則導引學生使用linux的Python程式開發環境，透過幾周的教學極生動的CTF解題可使學生提升高陽的學習意願。

教學環境設計

不同課程模組會有不同的教學環境，本計畫將提供各校教師相關的教學平台，底下摘錄部份相關內容:

|  |  |
| --- | --- |
| **課程模組名稱** | 教學環境設計 |
| Linux安全測試基礎 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 隱寫術 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 基礎加密/解密與破密 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 使用Python進行加解密與破密 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 現代密碼加解密與破密(初體驗) | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 編碼與解碼 | 使用線上工具實際演練CTF平台上的編碼與解碼題目。  CTF題目將建置於國家高速網路所提供的CDX平台 |
| 網路安全與封包分析 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 網路安全之防火牆實務 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。 |
| 網路安全之入侵偵測系統實務 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。 |
| 網站安全分析模組 | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 網站安全防護實務:WAF | 教學環境使用本計畫將提供的linux image檔案與教學手冊。  CTF題目將建置於國家高速網路所提供的CDX平台。 |
| 系統安全 | 本計畫將提供的linux 與WINDOWS XPimage檔案與教學手冊。 |
| 人工智慧與資訊安全 | 教學環境使用Google平台進行實作。  本計畫也將利用採購的教學設備錄製影片教導學生如何建置人工智慧分析平台與進階教學內容。 |

在課程操作上本計畫將提供各課程模組的教學手冊來提供教室授課及學生學習。為有效學生學習，要在短時間完成實務演練，實務個案必須特別設計。本計畫規劃的實務個案依兩大模式執行。第一種模式採用CTF解題，透過精心設計適合資安初學者的學習需需求，解題過程必須考量資安初學者的學習，這些特殊設計的題目與現階段國內外CTF搶旗大賽的題目不同，必須搭配課程主題，而非以競賽為重心。另外第二種模式則是規畫與建置資安實務攻防案例教學模式。以網路安全之防火牆實務教學為例，本計畫將以所提供的Ubuntu　linux環境教導學生使用Iptables/ ufw設定防禦規則，並配合實際的測試配合Iptables/ ufw的防禦來使學生掌握。特別須說明的是有限時間內完成的實務教學需先設計好攻防演練情境與相關教材與環境，這是本計畫所提供的服務重心。

1. **實作、實習等外部實務學習等配套**

**(參訪、實習、實作或實驗等配套措施的說明(請簡述預定進行之環境/地點及實施內容)，若有其他方式，亦請詳加說明以供審)**

本計畫強調實作學習模式，大部分課程模組皆提供實作相關教材與案例。

底下以幾個課程模組加以說明實作學習的配套措施與環境/地點及實施內容:

|  |  |  |  |
| --- | --- | --- | --- |
| **課程模組名稱** | 配套措施 | 環境/地點 | 實施內容 |
| Linux安全測試基礎 | 於上課教室匯入本計畫提供的linux環境。配合學習手冊與教學簡報進行授課。題目將  建置在國網的CTF平台。  本課程有搭配教學錄影供教師使用。 | 授課地點的網路教室(須裝妥virsual Box)  連線到國家網路中心的CTF平台 | Linux基本指令: ls,cat,find  Linux網路指令:ssh,wget  Linux行程管理指令:ps  本課程模組搭配CTF平台學習，學生於課堂上須動手使用Linux相關指令完成練習。 |
| 隱寫術 | 於上課教室匯入本計畫提供的linux環境。配合學習手冊與教學簡報進行授課。題目將  建置在國網的CTF平台。  本課程有搭配教學錄影供教師使用。 | 授課地點的網路教室(須裝妥virsual Box)  連線到國家網路中心的CTF平台 | 圖片隱寫術的分析技術  Binwalk 與dd 的分析技術  hexdump的分析技術 |
| 基礎加密/解密與破密 | 建置在國網的CTF平台將提供本課程的練習題目。  教師授課可配合學習手冊與教學簡報使用線上工具進行教學。  本課程有搭配教學錄影供教師使用。 | 授課地點的網路教室  連線到國家網路中心的CTF平台 | 古典密碼學:  替換式密碼Substitution cipher  換位加密法Transposition cipher  Scytale cipher密碼棒  本課程模組搭配CTF平台學習，學生於課堂上須動手完成練習。 |
| 網路安全之防火牆實務 | 於上課教室匯入本計畫提供的linux環境。  配合學習手冊與教學簡報進行授課。  本課程有搭配教學錄影供教師使用。 | 授課地點的網路教室(須裝妥virsual Box) | Iptables/ufx基本指令  防禦規則撰寫  實際攻擊測試  防火牆阻擋攻擊情境實務 |

更多課程模的實作學習配套措施與環境/地點及實施內容將分別撰寫於使用手冊與教學手冊。

1. **學習成效評量機制**

**(請說明如何進行資安實務課程內容的學習成效評量機制，以確實了解學生資安實務學習成效)**

**本計畫規劃兩種學習成效評量機制:**

(1) 整合資安證照題型的紙筆測驗

(2) 使用線上CTF平台的實作測驗

整合資安證照題型的紙筆測驗

本課程學習成效評量機制將包括一般傳統的紙筆測驗，但除了相關知識與觀念的評量外，本課程將納入資安專業證照的題型以強化學生學習的動機。另外國家正在推動經濟部產業人才能力鑑定(IPAS)也已經於今年(2018)五月舉辦第一場，相關初級證照考題也將納入本計畫所提供的傳統的紙筆測驗。

使用線上CTF平台的實作測驗

除了紙筆測驗外，本計畫更強調實作的成效評量機制。本計畫將使用國家高速網路與計算中心(國網中心)所提供的CDX雲端資安攻防平台建置線上CTF學習平台及線上CTF評量平台，教師可以在每周上課立即看到學生的學習成果(如下圖所示，學生完成的解題後題目背景將變成綠色的背景)

****

**圖:** 學生完成的解題後題目背景將變成綠色的背景

1. **課程學習互動與回饋機制**

**(請說明課程教學中如何與學生建立學習互動機制，例如共筆、線上討論等；以及課程結束後建立回饋或追蹤機制，了解學習成效或協助學生持續進行資安實務相關議題學習的機制，例如資安證照、資安競賽等)**

課程教學中的學習互動機制：

本計畫鼓勵學生互動教學，由已經解出的同學教導尚未理解的學生完成練習，不僅可以使資優學生獲得更高的成就感以可以培養學生濟弱扶傾的精神。另外對於學習較慢的同學也可以會得好友的幫助完成解題，可增進學生正面的友誼能量。由於是在現場教學且必須當時完成練習，學生的專注度可以大幅提升。

課程回饋或追蹤機制：

本計畫將建立回饋或追蹤機制，在課程結束後，了解學習成效或協助學生持續進行資安實務相關議題學習，底下是相關作法:

[1]在課後我們將建置相關基礎型的題目提供學生課後練習用，考量初學者的學習狀況，本計畫將重新規劃基礎型題目由淺至中，並且鼓勵同學一起研究解題，如此可以建立團隊精神與學習互動。

[2]本計畫將與參與與推動的學校建立追蹤輔導機制鼓勵學生參與適合的資安活動，包括教育部資訊安全人才培育計畫所舉辦的happyWeekend資安研習營、資安特訓營(Summer camp/Winter camp) 、AIS3等活動，本計畫也將鼓勵學員參加HITCON community等資安社團所舉辦的資安講座。

[3]對資安學習強烈的學生，本計畫也鼓勵學生參與教育部資訊安全人才培育計畫的臺灣好厲駭高階人才培育，由業界與學界資安專家組成的輔導師資可以滿足更高需求的資安培育。

[4]另外參與各項資安競賽可以讓學生將所學到的技術用於正確的地方(避免學生誤觸法網)，本計畫將推動與輔導學生參與舉辦的資安競賽[底下是比較適合本計畫學生參與的CTF]:

1.國外著名的 CMU大學舉辦的線上PICO CTF競賽[3-4月間舉辦]

2.由Montgomery Blair High Schoo 所舉辦的Angstrom CTF[3-4月間舉辦]

3.教育部資安人才培育計畫舉辦的MyFirstCTF[寒假期間舉辦]

4.教育部資安人才培育計畫舉辦的AIS3 CTF[暑假期間舉辦]

1. **教學資源**
2. **實務課程教學環境或演練平臺的布建**

**(請簡述實務教學環境或演練平台的設計與布建，包含所需的軟硬體設備、校內外教學資源的配合等。其中，為利未來實務課程的示範與推廣，課程內容的實作環境若可虛擬化(KVM)，則需配合國家高速網路與計算中心(以下簡稱國網中心)提供之Cyber Defense Exercise, CDX平臺，設計實務課程教學環境、模組及其相關操作手冊。**

實務教學環境或演練平台的設計與布建：

不同教學模組需搭配實務教學環境底下說明不同模組教學環境所需的軟硬體設備、校內外教學資源的配合。底下所使用的Linux平台將是使用Virtual box的image，建議使用需求與設定包括CPU:intel i5(含)以上,RAM:8GB[2GB配備給Linux image],網路:需可上網[建議教學學校網路須開放ssh連線]，本計畫將提供使用手冊與操作指南。

| **課程主題名稱** | 所需的軟硬體設備 | 校內外教學資源 |
| --- | --- | --- |
| Linux實務演練 | 本地端教學環境將使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 隱寫術 | 本地端教學環境將使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 加密/解密與破密 | 本地端教學環境:  基礎教學:使用網路線上工具  進階教學:使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 使用Python進行加解密與破密 | 本地端教學環境將使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 現代密碼加解密與破密(初體驗) | 本地端教學環境將使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 編碼與解碼 | 本地端教學環境:  基礎教學:使用網路線上工具  進階教學:使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 網路安全與封包分析 | 本地端教學環境將使用上述Linux平台(含wireshark的軟體模組) | 線上CTF平台: 使用國網中心CDX平臺(本計畫將布建CTF練習平台) |
| 網路安全之防火牆實務 | 本地端教學環境:將使用上述Linux平台(含防火牆的軟體模組) | 使用本計畫提供之Virtual box的Linux image |
| 網路安全之入侵偵測系統實務 | 本地端教學環境:使用上述Linux平台(含snort的軟體模組) | 使用本計畫提供之Virtual box的Linux image |
| 網站安全初體驗 | 本地端教學環境將使用上述Linux平台 | 線上CTF平台: 使用國網中心CDX平臺 |
| 網站漏洞分析 | 本地端教學環境將使用上述Linux平台 | 行動測試平台 |
| 網站安全防護實務:WAF | 本地端教學環境將使用上述Linux平台(包含WAF) | 使用本計畫提供之Virtual box的Linux image |
| 系統安全 | 本地端教學環境:Kali Linux平台與Windows XP 平台 | 使用本計畫提供之Virtual box的Linux image及Windows XP image |
| 人工智慧與資訊安全 | 本地端教學環境:AI Linux平台 | 使用本計畫提供之Virtual box的Linux imag |

國家高速網路與計算中心(以下簡稱國網中心)提供之Cyber Defense Exercise(CDX)雲端資安攻防平台。CDX雲端資安攻防平台為科技部委由國家高速網路與計算中心(國網中心)執行資訊安全開放資料平台研發與惡意程式知識庫維運計畫之一部分，平台採用雲端服務的架構進行規劃與設計,猶如使用私有雲服務例如：Amazon Elastic Compute Cloud (Amazon EC2) 或是 Linode ，主要用以改善傳統攻防平台管理與使用不易的問題，虛擬化的架構提供攻防演練場景快速部署的可行性，也提供了多人多場景同時進行攻防演練環境，以擬真的網路環境提供攻防技術的研究，讓參與的人員能夠熟悉與掌握以往曾經發生過的資訊安全事件,並從中學習資訊安全的檢測與分析技巧。本計畫將使用國網中心CDX平臺布建CTF練習平台，現有CDX平臺布建的ACTF平台主要以資訊類別的大專生為主，為因應本計畫教學實習所需，本計畫將規劃與設計更基礎的題目來搭配教學使用。

另外本計畫也鼓勵實際參與資安競賽，本課程將依照學習的狀況輔導學生參與國內舉辦的MyFirstCTF 及國外著名的 CMU大學舉辦的線上PICO CTF競賽與由 Montgomery Blair High Schoo 所舉辦的Angstrom CTF。對於具有強烈學習的學生本計畫也將輔導他們參與教育部資安人才培育計畫的各項活動，並鼓勵學生參與臺灣好厲駭高階資安人才培育活動及AIS3 CTF與HITCON CTF的競賽。由此可以完成從高中直到高階資安人才培育的整體架構。

1. **實務課程教學設計與操作手冊**

**(請於下表簡列預計可產出做為示範與推廣的教學資源，例如教學設計手冊、實務課程操作手冊、教學環境設計手冊等，並說明實務課程操作手冊與教學內容配合的情形、業師投入情形等，以及後續修訂與維護的機制)**

| **課程主題名稱** | **內容簡要說明(含學習目的)** | **類別** | **業師投入情形** |
| --- | --- | --- | --- |
| 從資訊安全到資訊倫理與法律 | 使學生透過案例分析了解資訊安全的重要性及其威脅，並由個案中深入理解新興科技相關的資訊倫理與法律。 | ▓其他，請說明  認知教學與觀念介紹 | ▓無 |
| Linux實務演練 | 教授學生基礎的linux環境與指令。主要包括網路ssh及wget指令、行程管理常用的ps指令等。本課程模組搭配CTF解題來強化學生學習意願。 | ▓實務課程操作手冊 | ▓無 |
| 隱寫術 | 使學生動手實作文件隱寫術與圖片隱寫術的觀念與技術。 | ▓實務課程操作手冊 | ▓無 |
| 加密/解密與破密 | 使學生動手實作古典密碼學的加密/解密與破密觀念與技術。 | ▓實務課程操作手冊 | ▓無 |
| 使用Python進行加解密與破密 | 教導學生Python程式設計技術與在加解密與破密上的應用。 | ▓實務課程操作手冊 | ▓無 |
| 現代密碼加解密與破密(初體驗) | 教導學生現代密碼的觀念(DES/AES對稱式密碼與RSA非對稱式密碼)及相關的加解密與破密技術。 | ▓實務課程操作手冊 | ▓有  業師姓名：  \_\_郭建邦\_\_ |
| 編碼與解碼 | 使學生動手實作學習不同編碼與解碼，包括base64/ base32/ASCII/Morse。 | ▓實務課程操作手冊 | ▓無 |
| 網路安全與封包分析 | 使學生動手實作學習網路協定的封包分析，及進階的攻擊封包分析技術。 | ▓實務課程操作手冊 | ▓無 |
| 網路安全之防火牆實務 | 透過規劃的攻擊防禦情境使學生動手實作學習網路安全的防火牆實務。 | ▓實務課程操作手冊 | ▓有  業師姓名：  \_\_\_郭建邦\_\_ |
| 網路安全之入侵偵測系統實務 | 透過規劃的攻擊防禦情境使學生動手實作學習網路安全的入侵偵測系統實務。 | ▓實務課程操作手冊 | ▓有  業師姓名：  \_\_\_郭建邦\_\_ |
| 網站安全初體驗 | 使學生動手實作網站安全測試常用的分析工具並以CTF題目深化學生技能。 | ▓實務課程操作手冊  ▓教學環境設計手冊 | ▓無 |
| 網站漏洞分析 | 使學生動手實測OWASP Top 10(2017年版)網站漏洞，並以CTF題目深化學生資安測試技能。 | ▓實務課程操作手冊  ▓教學環境設計手冊 | ▓無 |
| 網站安全防護實務:WAF | 透過規劃的攻擊防禦情境使學生動手實作學習網路安全的網站應用程式防火牆WAF實務。 | ▓實務課程操作手冊  ▓教學環境設計手冊 | ▓有  業師姓名：  \_\_\_郭建邦\_\_ |
| 系統安全 | 透過規劃的攻擊防禦情境使學生動手實作學習滲透測試與系統安全防護的技術。 | ▓實務課程操作手冊  ▓教學環境設計手冊 | ▓有  業師姓名：  \_\_\_**吳哲仰**\_\_ |
| 人工智慧與資訊安全 | 透過規劃的學習情境使學生體驗人工智慧的重要性並配合Google平台實際演練。最後再示範教學人工智慧在資訊安全上的應用。 | □教學設計手冊  ▓實務課程操作手冊  ▓教學環境設計手冊 | ▓無 |

**註：**

1. **本補助計畫上述所產出之教學資源，將免費提供國內大專校院資安實務課程使用。**
2. **計畫之研發成果及其智慧財產權，除經認定歸屬本部所有者外，歸屬受補助單位所有。但受補助單位對於研發成果及其智慧財產權，應同意無償授權本部及本部所指定之人為不限時間、地域或內容之利用，著作人並應同意對本部及本部所指定之人不行使著作人格權。各該著作如有第三人完成之部分者，受補助單位應與第三人簽訂授權本部利用著作之相關契約。其他著作授權、申請專利、技術移轉及權益分配等相關事宜，由受補助單位依政府科學技術研究發展成果歸屬及運用辦法及其他相關法令規定辦理。**
3. **計畫之研發成果不得侵害他人之智慧財產權及其他權利。如有涉及使用智慧財產權之糾紛或任何權利之侵害時，悉由受補助單位及執行人員自負法律責任。**
4. **結合網路、影音等多媒體教學資源**

**(一)實務課程示範教學影片**

**(請於下表簡列預計可產出的實務課程示範教學影片，至少2個單元。另鼓勵錄製MOOCs教學影片，或課程設計搭配影音多媒體，提供線上教學環境使用。)**

本計畫不僅提供正常教學與解題的影音教學，更提供鼓勵學生自主學習的影音教學。為提供學生進一步學習資安技能，本計畫規劃部分課程的影音教學，鼓勵推動學校用來輔導學生自主學習。這些課程將由學生自行學習，推動學校的教學課程上將以輔導腳色提供相關資源，本計畫將提供教學環境的image與使用手冊，並提供諮詢服務。這些課程主要都是需要長時間的測試(例如漏洞掃描技術需要較長的過程時間及示範及解說也需要大量時間)，因此以線上影音教學不僅可以避免上課時數過少，且可以鼓勵學生主動學習。另外上課課程也將提供影音多媒體讓教師可以減輕教學負擔，使老師可以專注於學生實測的學習過程。影音教學的上課時間以十分鐘為主，避免過長的時間會使學生失去注意力。影音多媒體不僅可以使學生課前先預習，也可以讓學生課後複習。

| **課程主題名稱** | **內容簡要說明(含學習目的)** | **影片預定長度** | **類型** |
| --- | --- | --- | --- |
| 認識密碼學 | 古典密碼學的加密/解密與破密觀念與技術。 | 10分鐘 | ▓MOOCs教學影片 |
| 頻率分析法實務演練 | 古典密碼學的破密分析的觀念與技術。 | 10分鐘 | ▓一般影音影片 |
| 使用python加解密實務 | 使用python進行古典密碼學的破密分析 | 10分鐘 | ▓一般影音影片 |
| 認識RSA現代密碼學 | RSA現代密碼學的觀念與 | 10分鐘 | ▓MOOCs教學影片 |
| 使用openssl加解密實務 | 使用openssl進行RSA/DES/3DES/AES的加解密實測課程 | 10分鐘 | ▓MOOCs教學影片 |
| 認識CTF搶旗大賽 | CTF搶旗大賽的類型與學習 | 10分鐘 | ▓一般影音影片 |
| ascii編碼原理及解碼 | 使用線上工具實測ascii編碼及解碼 | 10分鐘 | ▓MOOCs教學影片 |
| base64編碼原理及解碼 | 使用線上工具及Linux base64指令實測base64編碼及解碼 | 10分鐘 | ▓MOOCs教學影片 |
| binwalk實務演練 | 使用binwalk實務分析圖片隱寫術的實務教學 | 8分鐘 | ▓一般影音影片 |
| Wireshark實務演練 | Wireshark實務演練中認識TCP/IP協定並學習網路封包分析技術基礎 | 10分鐘 | ▓一般影音影片 |
| HTTP協定分析 | 使用Wireshark分析HTTP協定 | 10分鐘 | ▓一般影音影片 |
| 網路攻擊封包分析實務 | 使用Wireshark分析網路攻擊封包實務教學 | 10分鐘 | ▓一般影音影片 |
| 認識網路防火牆 | 說明網路防火牆的原理及部屬模式 | 10分鐘 | ▓一般影音影片 |
| 網路防火牆案例實測 | 以規畫的攻擊防禦情境教導網路防火牆的防禦技術 | 10分鐘 | ▓一般影音影片 |
| 建置網站漏洞測試平台 | 建置DVWA網站漏洞測試平台的實務教學 | 10分鐘 | ▓一般影音影片 |
| Developer Tools分析技術 | 透過案例學習網站安全測試常用的Developer Tools分析技術 | 8分鐘 | ▓一般影音影片 |
| curl技術實務演練 | 透過案例學習網站安全測試常用的curl分析技術 | 8分鐘 | ▓一般影音影片 |
| burpsuite技術實務演練 | 透過案例學習網站安全測試常用的burpsuite分析技術 | 10分鐘 | ▓一般影音影片 |
| 漏洞掃描實務 | 本課程主題將介紹漏洞掃描  的基本觀念及Nikto漏洞掃描實務。我國各級政府單位按照不同等級需委外進行漏洞掃描，本課程主題將引領學生認識漏洞掃描的重要性。 | 10分鐘 | ▓一般影音影片 |
| 認識滲透測試 | 本課程主題將介紹滲透測試  的基本觀念及常用工具介紹。我國各級政府單位按照不同等級需委外進行滲透測試，本課程主題將引領學生認識滲透測試的重要性。 | 10分鐘 | ▓一般影音影片 |
| Nmap NSE資安檢測技術 | 透過案例學習系統安全測試與滲透測試常用的Nmap NSE檢測技術 | 10分鐘 | ▓一般影音影片 |
| Ｍetasploit資安檢測技術 | 透過案例學習系統安全測試與滲透測試常用的Ｍetasploit檢測技術 | 10分鐘 | ▓一般影音影片 |
| 建置CPU運算的人工智慧分析平台 | 本課程主題將介紹CPU運算模式的人工智慧分析平台建置方案 | 5分鐘 | ▓一般影音影片 |
| 建置GPU運算的人工智慧分析平台 | 本課程主題將介紹GPU運算模式的人工智慧分析平台建置方案 | 5分鐘 | ▓一般影音影片 |
| 人工智慧個案分 | 本課程主題將人工智慧個案分析 | 10分鐘 | ▓一般影音影片 |

**註：教學影片需配合放置在教育部指定之線上教學資源網站，影片製作人/開課教師亦可依其需求放置相關公開網站中。**

**(二)網路教學工具、多媒體教學資源的使用**

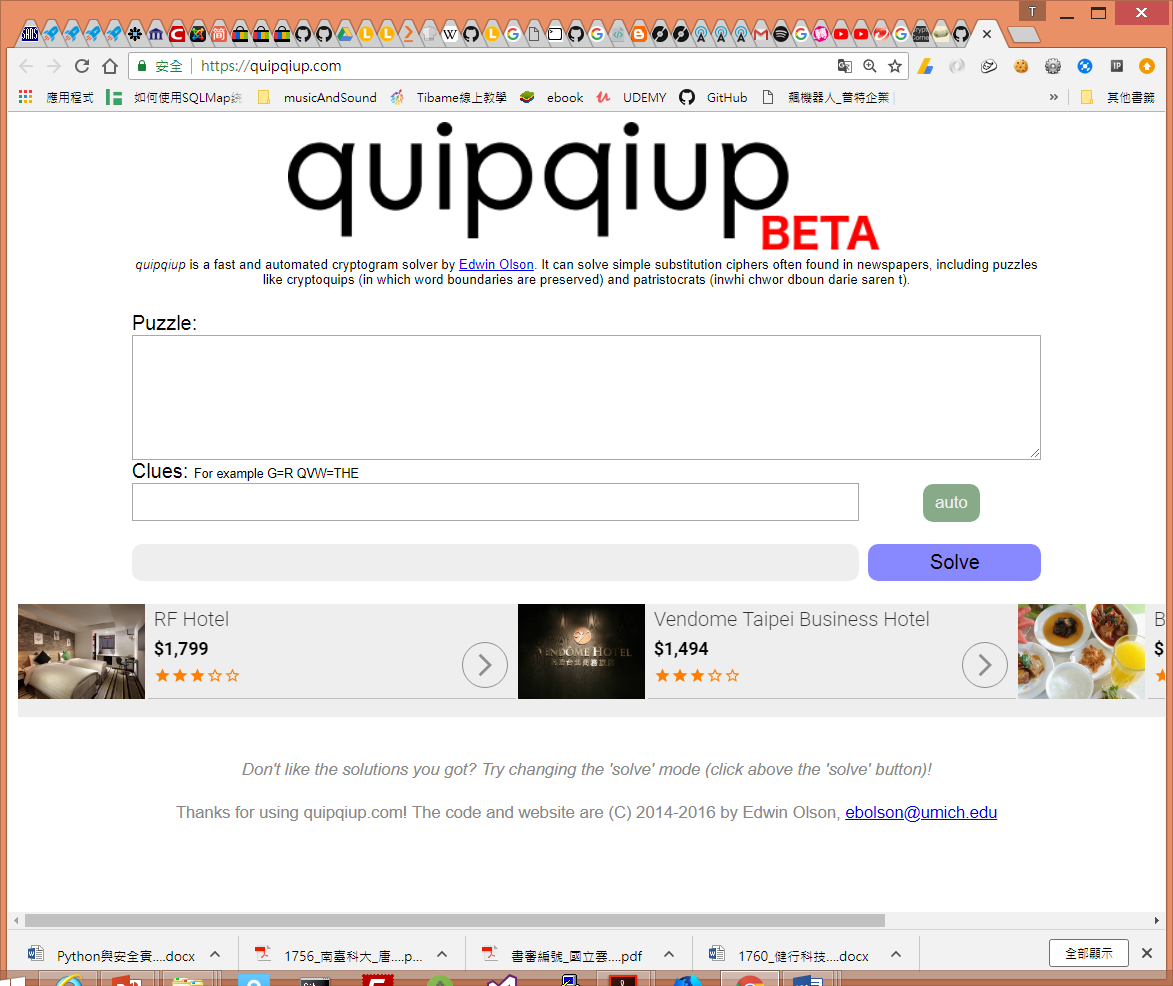
**(說明課程教學預計搭配使用線上實務教學工具、網路影音多媒體教學資源等)**

線上實務工具

本計畫將教導學生學習許多線上實務工具，底下列出部分相關工具與平台：

替換式密碼(Substitution cipher)的頻率分析法線上工具：

在教導替換式密碼(Substitution cipher)的頻率分析法時，本計畫將使用底下線上工具進行教學：http://quipqiup.com/，學生也將學會使用此工具解答Pico CTF 2014 : Substitution 50的題目。



　　　　base64編碼與解碼線上工具：https://www.base64decode.org/

　　　　Base64是一種基於64個字元來表示二進位資料的表示方法，通常用於編碼二進制訊

　　　　息，這些訊息透過編碼後進行儲存和傳輸，能保證數據在傳輸過程中保持不變而無

　　　　需修改。Base64通常用於許多應用程式，包括通過MIME的電子郵件，以及將複雜

　　　　的訊息保存為XML。www.base64decode.org線上編解碼網站可迅速將字串進行

　　　　Base64編碼及解碼動作。



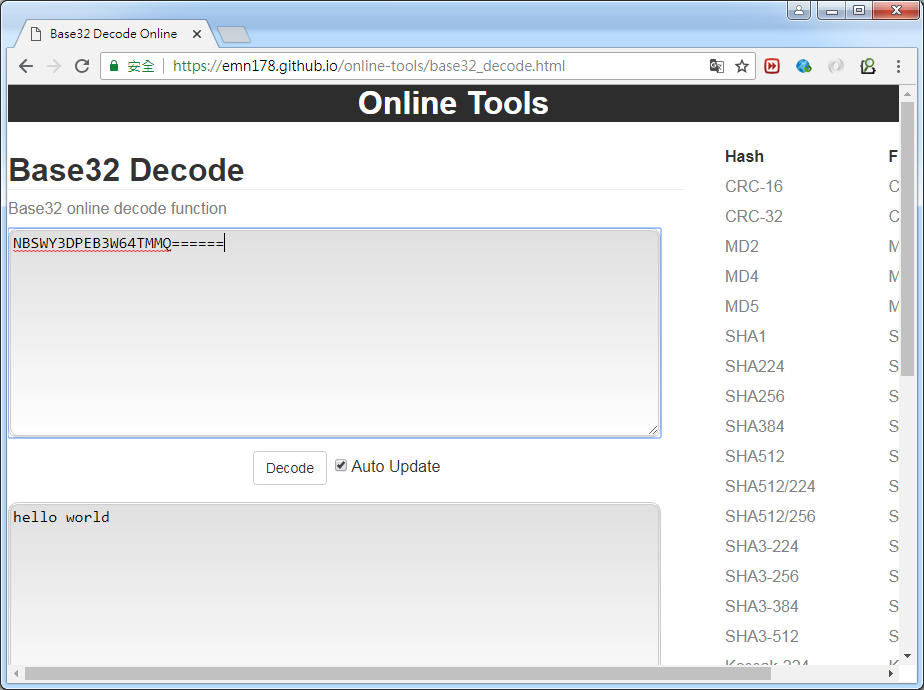
　　　　Base32編碼與解碼線上工具：

網址: https://emn178.github.io/online-tools/base32\_decode.html

　　　　Base32包含一個由32個不同字串組成的字串集，以及一個將任意8個字元序列編碼到

Base32字母表中的演算法。線上編解碼網站除了可進行Base32字串編解碼，甚至還

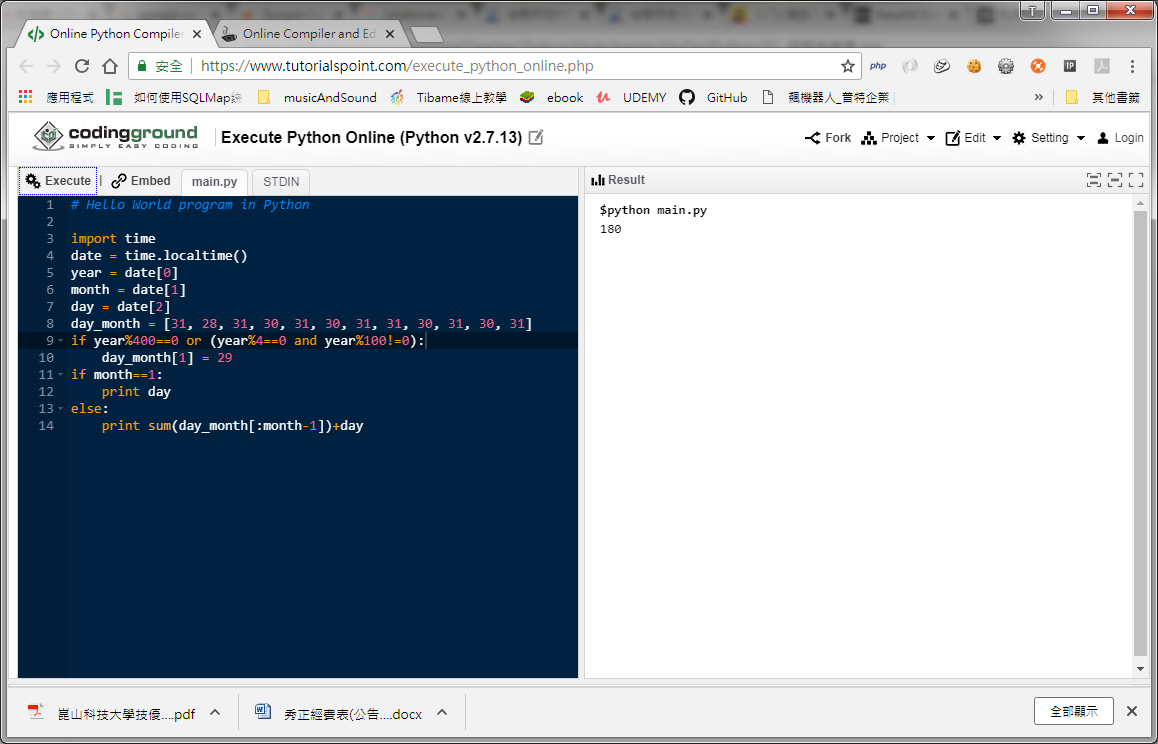
支援Base64、URL等線上編解碼。



　　　　使用線上程式開發平台

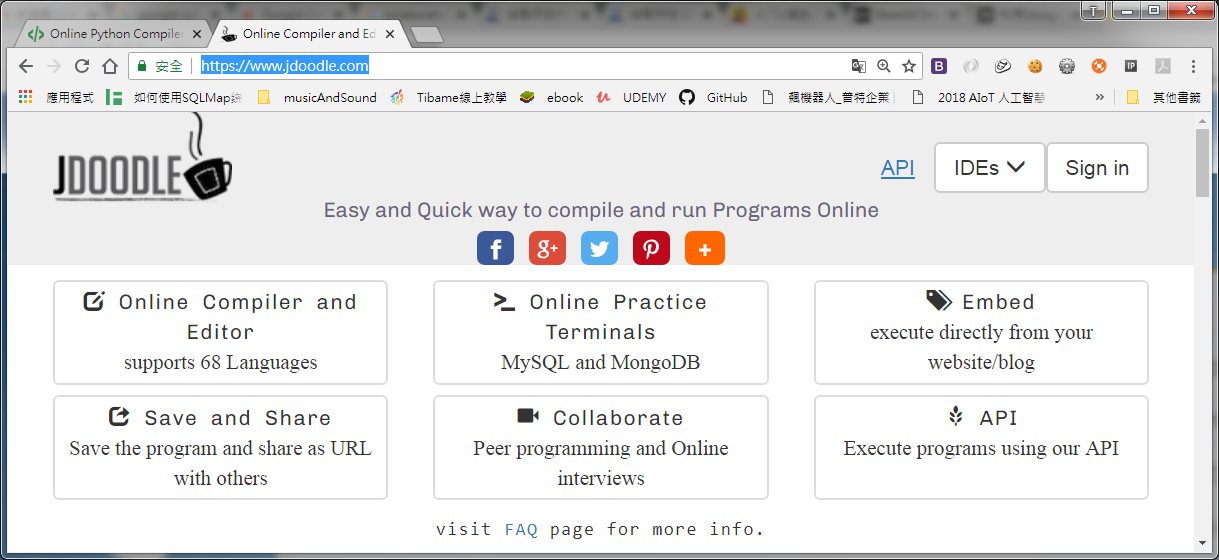
網址:<https://www.tutorialspoint.com/execute_python_online.php>

　　　　本計畫也將教導學生善用線上程式學習，底下所列為python線上程式開發平台



　　　　另外本計畫也將教導學生善用jdoodle線上程式開發平台：

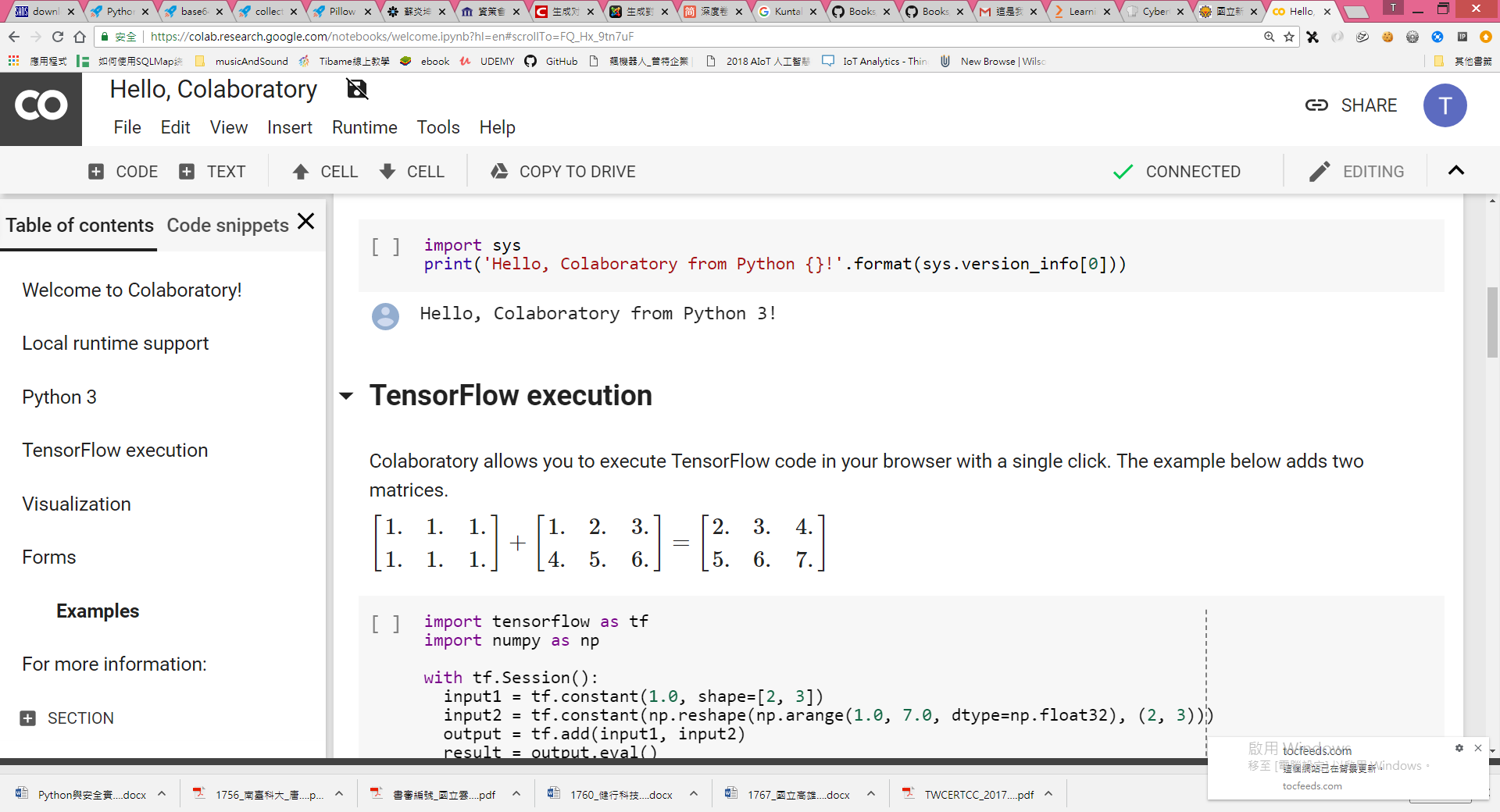
網址:https://www.jdoodle.com/



jdoodle線上程式開發平台支援許多程式開發，包括C/C++/C++14/C#/PHP/

Ruby/Python2/Python3/ GCC/ NASM等

使用Google線上人工智慧平台:



本計畫將以Google推出的Google Colaboratory平台作為主要的人工智慧教學平台。

Google Colaboratory主要目的是想要幫助機器學習和人工智慧教育的推廣。它是一個提供Jupyter Notebook服務的雲端環境，無需額外設定就可使用，並且還提供免費的GPU使用。Google Colaboratory平台預裝了一些做機器學習與深度學習常用的套件，像是 TensorFlow、scikit-learn、matplotlib、numpy、pandas等，對於使用一般公用資料的機器學習與深度學習可以無痛上手。本計畫將使用Google線上人工智慧平台作為”人工智慧與資訊安全”課程模組的實作場域。另外對於未安裝的套件也可以自行安裝，例如Facebook在 2017年開源的PyTorch就可以以底下方式在Jupyter Notebook上安裝:!pip3 install <http://download.pytorch.org/whl/cu80/torch-0.3.0.post4-cp36-cp36m-linux_x86_64.whl>。

**網路影音多媒體教學資源:**

為鼓勵學生自主學習，本計畫將提供相關優質網路學習資源給要深入研讀的學生， 使學生能強化資安技能。底下列出部分網路資源（如youtube及slideshare平台上的許多相關教學資源），完整的清單列表與輔導閱讀將於後續提供，實際授課時將鼓勵學員自主學習：

圖像隱碼術(Steganography)與惡意程式：原理和方法

<https://blog.trendmicro.com.tw/?p=12510>

Steganography: Hiding information in past, present and future.

<https://www.slideshare.net/Alberce/steganography-hiding-information-in-past-present-and-future?qid=c0c0804b-0694-473d-91d1-aec31de599c0&v=&b=&from_search=5>

Wired and Wireless Network Forensics

https://www.slideshare.net/wildpackets/wired-and-wireless-network-forensics?qid=bcfcf521-217e-4e80-86c9-495333a5d0bd&v=&b=&from\_search=6

【HITCON FreeTalk 2018 - Spectre & Meltdown 漏洞原理說明與 POC 剖析】

<https://www.slideshare.net/HacksInTaiwan/hitcon-freetalk-2018-spectre-meltdown-poc?qid=7d30eb36-56ef-49cc-8f06-2d245b08894c&v=&b=&from_search=3>

TrendMicro: 從雲到端，打造安全的物聯網

<https://www.slideshare.net/AmazonWebServices/trendmicro-76989531?qid=7e84024f-cc27-4873-a4a6-59a8e47b29fd&v=&b=&from_search=23>

AI and Security

<https://www.youtube.com/watch?v=ojTz7bOjT6o>

Machine Learning for Cybersecurity

<https://www.youtube.com/watch?v=cpCKhhV1wQU>

A Machine Learning Approach to Log Analysis - Ianir Ideses - DevOpsDays Tel Aviv 2016

<https://www.youtube.com/watch?v=PJ_kx9-OPgc&t=255s>

Server Log Analysis with Pandas

<https://www.youtube.com/watch?v=MbflVr-MBm0&t=37s>

Deep Learning in Security—An Empirical Example in User and Entity Behavior Analytics UEBA

<https://www.youtube.com/watch?v=aAhAJFk1OVc&t=70s>

1. **校內外教學資源之配合**

**(請說明校內外教學資源之配合，例如企業提供軟硬體或線上之實驗或模擬環境、協助教學、企業專題、企業實習（有薪或無薪）及輔導業師等)**

線上之實驗或模擬環境:

本計畫為有效運用有限經費及提供更多服務，因此規劃使用眾多網路教學工具(詳如上述第二節網路教學工具、多媒體教學資源的使用說明)。另外本計畫為因應不同課程模組教學所需也將實際建置不同的教學環境提供各校使用(詳如上述第二節實務課程教學設計與操作手冊說明)。為有效提供教師教學服務本計畫提供多媒體教學資源的使用(詳如上述第三節結合網路、影音等多媒體教學資源之實務課程示範教學影片之說明)。在實作與實習平台上本計畫更將於國家高速網路與計算中心所提供的CDX雲端資安攻防平台建置線上CTF學習平台及線上CTF評量平台，教師可以在每周上課立即看到學生的學習成果。

協助教學:

本計畫將充分配合教育部資安人才培育計畫總計畫辦公室規劃舉辦高中職生資安種子師資培訓課程，舉辦過程中將與各參與學校建立聯繫，並提供相關諮詢管道以建立後續輔導與推動資安認知課程。為鼓勵學生自主學習與進階延伸學習，本計畫將推動與教育部資安人才培育計畫子計畫二與子計畫三之合作，輔導優量學習學生及教師參與更多資安講座與活動。透過整合教育部資安人才培育計畫整體資源來提供更多教師與學生學習所需。

輔導業師

針對參與本計畫各高中職教師及各大專校院所開設資安認知課程，本計畫也將建立追蹤輔導措施，於各校授課過程中邀請各教師提供資優學習名冊，協助建立跨校的學習輔導，並主動推薦至臺灣好厲駭進行更多及更深的培訓。臺灣好厲駭包括底下眾多資安專家學者:

 趨勢科技公司洪偉淦總經理

 趨勢科技公司張裕敏資深協理

 資策會資安科技研究所技術研發中心 毛敬豪經理

 戴夫寇爾翁浩正執行長

 戴夫寇爾蔡政達工程師

 威瑞特公司吳明蔚總經理

 台灣威瑞特公司邱銘彰技術長

 安連網路公司徐千洋資深工程師

 聯發科技公司/李倫銓經理 ( HITCON總召 )

 HITCON蔡松廷理事長

 臺灣大學電機工程系鄭振牟副教授

 臺灣大學資訊工程系蕭旭君助理教授

 交通大學資訊工程系黃世昆教授

 交通大學資訊工程黃俊穎副教授

 臺灣科技大學資訊管理系查士朝副教授

 臺灣科技大學資訊工程系鄭欣明副教授

透過分層的專責服務與主動協同輔導將可有效建立我國資訊安全人才培育制度與教育部政策的成果。

1. **參與師資**
2. **參與教師簡介**

**(1.請簡述所有開課教師主要參與本課程資源發展主題或課程教授主題等、以及其主要曾從事與本課程相關之計畫、論文、實作專題等經驗2.請檢附教師於過去3年內曾開設與本計畫徵件須知第六點第一款所列主題領域相關之資安課程證明。)**

(1)崑山科技大學曾龍副教授

(1.1)經歷

1. 崑山科技大學雲端大數據分析與資通安全研發中心|主任|2011年10月至迄今

2. 崑山科技大學教務處|副教務長|2012年08月至2014年07月

3. 崑山科技大學資工系|系主任|2011年08月至2014年07月

4. 崑山科技大學數位生活科技研究所|所長|2011年08月至2014年07月

5. 崑山科技大學資工系|副教授|2008年02月至迄今

6. 崑山科技大學資工系|助理教授|2006年08月至2008年01月

(1.2) 證照

1. EC-Council CHFI駭客技術專家證照

2. EC-Council CEH駭客技術專家證照

3. BS7799 Lead Auditor證照

(1.3) 獲獎

100年度教育部臺灣網際網路傑出貢獻人員獎

(1.4) 研究領域

1. 駭客攻防技術

2. 大型資安監控中心(SOC)開發

3. 雲端大數據分析

4. 深度學習|人工智慧|機器學習|資料探勘

(1.5) 研發成果

1. [2007]6IDS(IPv6 Intrusion Detection System)v3.5獲得IPv6 Ready Logo Phase-2認證(2007/05/07) <https://www.ipv6ready.org/db/index.php/public/logo/02-C-000190/>

2. [2006]行政院國家資訊通信發展小組(NICI) IPV6推動工作小組研發計畫 A6NSOC(Agent-Oriented Intelligent IPv6 Network Security Operation Center) IPv6安全監控中心

3. [2005]行政院國家資訊通信發展小組(NICI) IPV6推動工作小組研發計畫 W6SGW(Wireless IPv6-Enabled Security Gateway) 適用於無線IPv6網路之安全閘道器

4. [2004]行政院國家資訊通信發展小組(NICI) IPV6推動工作小組研發計畫

6IPS(IPv6-Enabled Intrusion Prevention System) 適用於IPv6網路之入侵防禦系統

5. [2003]行政院國家資訊通信發展小組(NICI) IPV6推動工作小組研發計畫

6IDS(IPv6-Enabled Intrusion Detection System) 適用於IPv6網路之入侵偵測系統

(1.6) 產學合作計畫

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **計畫名稱** | **補助機構** | **起訖時間** | **擔任工作** | **計畫經費** |
| 107年度資訊安全人才培育計畫之子計畫3：實務導師制度與資安扎根 | 教育部 | 2018/04/01~2019/03/31 | 主持人 | 3,500,000 |
| 106年度資訊安全人才培育計畫之「子計畫3：資安扎根與認知推廣計畫」 | 教育部 | 2017/04/01-2018/03/31 | 主持人 | 3,500,000 |
| 105年度教育部新型態資安實務課程計畫--網頁與網站安全駭客攻防實務 | 教育部 | 2016/02/01-2017/01/31 | 主持人 | 160,000 |
| 104年度教育部新型態資安實務課程計畫--資安檢測與駭客攻防演練 | 教育部 | 2015/09/01~2016/01/31 | 主持人 | 160,000 |
| 103年度教育部資訊軟體人才培育推廣計畫--行動終端應用(A類) | 教育部 | 2014/02/01~2015/01/31 | 主持人 | 625,000 |
| 以雲端技術為基礎之跨縣巿協同聯合防禦miniSOC暨AISAC分享平臺建置 | 教育部 | 2014/01/01~2015/04/30 | 主持人 | 4,850,000 |
| 以雲端為基礎兼具分流機制的A-ISAC分享平台暨協同聯合防禦縣市網miniSOC建置專案 | 教育部 | 2013/01/01~2013/12/31 | 主持人 | 6,050,000 |
| A-ISAC擴充平台與縣市網MiniSOC開發建置專案 | 教育部 | 2012/01/01~2012/12/31 | 主持人 | 11,000,000 |
| 自動化縣市網監控、資安分享平台與miniSOC建置 | 教育部 | 2010/03/01~2011/12/31 | 主持人 | 16,500,000 |
| 教育部ISAC教育學術資安資訊分享與分析中心研發專案 | 教育部 | 2009/02/01~2010/2/28 | 主持人 | 7,816,364 |

(1.7) 服務

|  |  |
| --- | --- |
| **單位** | **職稱** |
| 國家資通安全會報技術服務中心 | 107年政府機關(構)資通安全稽核委員 |
| 國家資通安全會報技術服務中心 | 106年政府機關(構)資通安全稽核委員 |
| 國家資通安全會報技術服務中心 | 106年資安服務廠商評鑑委員 |
| 國家資通安全會報技術服務中心 | 105年資安服務廠商評鑑委員 |
| TWCERT/CC | 審稿委員 |
| TANET2011研討會 | 審稿委員 |
| 金融監督管理委員會 | 演講講師 |

(1.8) 技術報告

1. 林政頴、黃亦銘、曾龍，RFID安全性議題，RUN\_PC，(2007/11)

2. 林政頴、黃培軒、曾龍，Web Application Security Framework and Assessment (1)，RUN\_PC，(2007/1)

3. 林政頴、陳家銘、曾龍，Web Application Security Framework and Assessment (2)，RUN\_PC，(2007/2)

4. 黃永銘、黃亦銘、曾龍，滲透測試之OSSTMM標準（一），RUN\_PC，(2005/4)

5. 傅若涵、黃亦銘、曾龍，滲透測試之OSSTMM標準（二），RUN\_PC，(2005/4)

6. 李崇誠、黃亦銘、曾龍，滲透測試之OSSTMM標準（三），RUN\_PC，(2005/5)

7. 林偉穎、陳麒元、曾龍，IPS Testing 入侵防禦系統之測試，RUN\_PC，(2005/3)

8. 黃亦銘、羅大權、曾龍，對企業滲透測試應有的認識，RUN\_PC，(2005/3)

9. 王慶豐、陳麒元、曾龍，IPv6網路之安全性威脅 (上)，RUN\_PC，(2005/1)

10.王慶豐、陳麒元、曾龍，IPv6網路之安全性威脅 (下)，RUN\_PC，(2005/2)

11.林偉穎、陳麒元、曾龍，Intrusion Prevention System入侵防禦系統 (1)，RUN\_PC，(2004/11)

12.林偉穎、陳麒元、曾龍，Intrusion Prevention System入侵防禦系統 (2)，RUN\_PC，(2004/12)

13.林偉穎、陳麒元、曾龍，Intrusion Prevention System入侵防禦系統 (3)，RUN\_PC，(2005/1)

(1.9) 期刊論文

1. 曾龍、王元俊、官大智 量子秘密分享之研究發展,Communications of the CCISA，04/2005

2. 曾龍、王元俊、官大智 量子攻擊及量子密碼協定之安全性證明, Communications of the CCISA，04/2005

3. 曾龍、王慶豐、陳麒元 量子密碼協定之與最新研究發展, Communications of the CCISA，04/2005

4. 曾龍、黃亦銘、賴溪松 量子密碼學之研究領域與最新發展, Communications of the CCISA，04/2005

5. Hai-Yang Cheng and B. Tseng Exclusive Hadronic D Decays to $\eta'$ or $\eta$: Addendum on Resonant Final-State Interactions Chin.J.Phys. 39 (2001) 28-40 (SCI, 2006 Impact Factor =0.238) 被引用次數(SLAC/Spires Citations):4

6. Yaw-Hwang Chen, Hai-Yang Cheng, B. Tseng and K.C. Yang Charmless Hadronic Two-Body Deacys of B\_u and B\_d Mesons Phys.Rev. D60 (1999) 094014 國科會計畫編號:NSC88-2112-M001-006 (SCI, Times Cited:38 , 2006 Impact Factor =4.896) 被引用次數(SLAC/Spires Cita-tions):202

7. Yaw-Hwang Chen, Hai-Yang Cheng and B. Tseng Charmless Hadronic Two-Body Deacys of B\_s Mesons Phys. Rev. D.59, 074003 (1999). 國科會計畫編號:NSC88-2112-M001-006 (SCI, Times Cited: 9 , 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citations):37

8. B. Tseng Exclusive charmless $B\_s$ hadronic decays into $\eta'$ and $\eta$ Phys. Let. B.446, 125 (1999). 國科會計畫編號:NSC87-2112-M006-018 (SCI, Times Cited: 2, 2006 Impact Fac-tor =5.043) 被引用次數(SLAC/Spires Citations):11

9. Hai-Yang Cheng and B. Tseng Exclusive Hadronic D Decays to eta' and eta Phys. Rev. D.59, 014034 (1999). 國科會計畫編號:NSC87-2112-M006-018 (SCI Times Cited: 3, 2006 Impact Factor =4.896) 被引用次數(SLAC/Spires Citations):9

10.Hai-Yang Cheng and B. Tseng Nonfactorizable Effects in Spectator and Penguin Amplitudes of Hadronic Charmless B Decays Phys. Rev. D. D58:094005,1998. 國科會計畫編號:NSC86-2112-M002-010-Y (SCI Times Cited: 35, 2006 Impact Factor =4.896) 被引用次數(SLAC/Spires Citations):89

11.Hai-Yang Cheng and B. Tseng CHARMLESS B DECAYS TO ETA-PRIME AND ETA. Phys.Lett.B415:263-272,1997 國科會計畫編號:NSC86-2112-M002-010-Y (SCI Times Cited: 22, 2006 Impact Factor =5.043) 被引用次數(SLAC/Spires Citations):58

12.Hsiang-nan Li and B. Tseng NONFACTORIZABLE SOFT GLUONS IN NONLEPTONIC HEAVY MESON DECAYS. Phys.Rev.D57:443-451,1998 國科會計畫編號:NSC86-2112-M002-010-Y (SCI Times Cited: 12, 2006 Impact Factor =4.896) 被引用次數(SLAC/Spires Cita-tions):39

13.Wei-Shu Hou and B. Tseng ENHANCED B ---> S G DECAY, INCLUSIVE ETA-PRIME PRO-DUCTION, AND THE GLUON ANOMALY. Phys.Rev.Lett.80:434-437,1998 國科會計畫編號:NSC86-2112-M002-010-Y (SCI Times Cited: 48, Impact Factor =7.072)被引用次數(SLAC/Spires Citations):139

14.Ling-Lie Chau , Hai-Yang Cheng and B. Tseng ANALYSIS OF TWO BODY DECAYS OF CHARMED BARYONS USING THE QUARK DIAGRAM SCHEME. Phys.Rev.D54:2132-2160,1996 (SCI, 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citatations): 5

15.Hai-Yang Cheng and B. Tseng 1/M CORRECTIONS TO BARYONIC FORM-FACTORS IN THE QUARK MODEL. Phys.Rev.D53:1457-1469,1996, Erratum-ibid.D55:1697,1997 (SCI, 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citatations): 37

16.Hai-Yang Cheng and B. Tseng EXTRACTION OF A1 AND A2 FROM B ---> PSI K (K\*), D (D\*) PI (RHO) DECAYS. Phys.Rev.D51:6259-6266,1995 (SCI, 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citatations): 33

17.Hai-Yang Cheng and B. Tseng CABIBBO ALLOWED NONLEPTONIC WEAK DECAYS OF CHARMED BARYONS. Phys.Rev.D48:4188-4202,1993 (SCI, 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citatations): 34

18.Hai-Yang Cheng and B. Tseng NONLEPTONIC WEAK DECAYS OF CHARMED BARYONS. Phys.Rev.D46:1042-1059,1992, Erratum-ibid.D55:1697,1997 (SCI, 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citatations): 43

19.Ling-Lie Chau , Hai-Yang Cheng, W.K. Sze , Benjamin Tseng and Herng Yao CP VIOLATION IN RARE B DECAY. Phys.Rev.D45:3143-3152,1992 (SCI, 2006 Impact Factor =4.896)被引用次數(SLAC/Spires Citatations): 16

20.Ling-Lie Chau , Hai-Yang Cheng, W.K. Sze , Herng Yao and Benjamin Tseng CHARMLESS NONLEPTONIC RARE DECAYS OF B MESONS. Phys.Rev.D43:2176-2192,1991, Erratum-ibid.D58:019902,1998 (SCI, 2006 Impact Factor =4.896)被引用次數(LAC/Spires Citatations): 212

21.C. Lee, B. Tseng, Y.W. Yang CURRENT DECOMPOSITIONS AND CURRENT ALGEBRA. Mod.Phys.Lett.A6:1833-1838,1991 (SCI, 2006 Impact Factor =1.564

(1.10) 研討會論文

1. 曾龍,周志學,王英傑,陳柔伊,蔡龍佑,”BigSA:巨量資料分析為基礎的資安分析平台開發與設計”,UHC2014第八屆優質家庭生活研討會/2014

2. 曾龍、郭堯彰、蔡龍佑、陳柔伊,”以雲端服務結合區域性主動式iBeacon推播系統設計與實作”，萬能科技大學2014工程與電資科技應用學術研討會/2014

3. 曾龍,鄭郁翰,陳柔伊, “雲端運算與智慧行動終端結合的架構與新趨勢”, International Journal of Advanced Information Technologies (IJAIT), Vol. 7, No.1/2013

4. 曾龍,鄭郁翰,陳柔伊,郭堯彰,”整合Web Service技術之互動式服務平台設計與開發”,NST2012 全國電信研討會/2012

5. 曾龍,鄭郁翰,吳祥鳴,郭堯彰，以雲端架構為基礎之IPv6數位監控中心設計與實作，WCE2012 民生電子研討會 ，2012

6. 曾龍,鄭郁翰,陳柔伊，多層次的雲端應用系統開發架構，UHC2012第6屆優質家庭生活關鍵技術研討會 ，2012

7. 曾龍,吳祥鳴,鄭郁翰,王慶豐，ASAP: 自動化資安分析系統，UHC2012第6屆優質家庭生活關鍵技術研討會 ，2012

8. 曾龍,鄭郁翰,郭堯彰,陳柔伊，基於推播訊息機制之居家安全監控中心設計與實作，UHC2012第6屆優質家庭生活關鍵技術研討會，2012

9. 曾龍,鄭郁翰,陳柔伊,顏惠敏,林芳白,張宏明，分析與防禦協同運作之MiniSOC：架構設計與實作，TANET2011網際網路研討會，2011

10. 第一作者(A), “MiniSOC:新的大型網路安全架構”, u-Home 第五屆優質家庭生活科技關鍵技術研討會.

11. 第一作者(A), “Design and implementation of a web-service based Security Information Shar-ing and Analysis Center”, UHC2010.

12. 第一作者(A), “以流程導向與高可用性架構設計與開發之資安通報平台”, Ubiqitous-Home Conference 2010 (UHC2010).

13. 第一作者(A), “以服務導向設計之教育學術資安資訊分享與分析中心”, TANET 2010台灣網際網路研討會.

14. 第二作者(B), “Adaptive Reduction of Redundant and Invalid Alerts traffics for Large Scale Network Security Center via Correlation algorithm ”, U-Home Conference 2008 .

15. 第一作者(A), “Detection of Malware Attack via IDS Proxy Correlation Algorithm ”, U-Home Conference 2008 .

16. 第一作者(A), “Development of U-Message Platform (Notification) for IPv6 U-Home Net-work ”, U-Home Conference 2008 .

17. 第一作者(A), “Design and Development of Ipv6 Digital Surveillance System (6DSS) for IPv6 U-Home ”, U-Home Conference 2008 .

(1.11) 學生競賽獲獎

|  |  |  |  |
| --- | --- | --- | --- |
| **競賽名稱** | **參賽項目組別** | **名次** | **活動日期** |
| 2013校園瘋雲榜App創意競賽 | Android-校園應用組 | 佳作 | 2013/10 |
| 2013全國大專院校資訊盃 | 慢速壘球賽 | 第一名 | 2013/1/29~31 |
| 2012全國大專院校資訊學院盃賽 | 壘球錦標賽 | 冠軍 | 2012/2/6~7 |
| Android「五零」高手選秀活動 | 無 | 第27名 | 2011/9/24 |
| Android「五零」高手選秀活動 | 無 | 第60名 | 2011/9/24 |
| 創業週末高雄/Startup Weekend Kaohsiung | 無 | 冠軍 | 2012/6/29~7/1 |
| 創業週末臺南/Startup Weekend Tainan | 無 | 季軍 | 2013/1/25~27 |
| 2014三校園APP之星 | 創新創意 | 三星校園APP之星獎 | 2014/10/23 |

(2) 國立臺南一中高英耀主任

**(2.1)個人資料**

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名  職 稱 | 高英耀老師 | 電 話：  傳 真：  e-mail： | (06)2371206#600  (06)2741661  joseph.tnfsh@gmail.com |

**(2.2)主要學歷**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 畢業學校 | 國別 | 科系別或主修學門 | 學位 | 起 迄 年 月 |
| 國立中山大學 | 臺灣 | 資訊工程所 | 碩士 | 2000年08月  至2002年07月 |
| 國立臺灣師範大學 | 臺灣 | 資訊教育系 | 學士 | 1992年08月  至1996年07月 |

**(2.3)現職及與專長相關之經歷(按時間先後順序由最近經歷開始填起)**

|  |  |  |  |
| --- | --- | --- | --- |
| 服　務　學　校 | 服　務　部　門 | 職　稱 | 起　迄　年　月 |
| 國立臺南一中 | 圖書館 | 主任 | 2017年08月至迄今 |
| 國立臺南一中 | 資訊科 | 教師 | 2000年08月至迄今 |
| 經歷： | | | |
| 國立臺南一中 | 圖書館 | 資訊組長 | 2011年08月  至2017年07月 |
| 國立臺南一中 | 學務處 | 社團活動組長 | 2010年08月  至2011年07月 |
| 國立臺南一中 | 進修部 | 註冊組長 | 2009年08月  至2010年07月 |
| 國立臺南一中 | 進修部 | 教學組長 | 2000年08月  至2006年07月 |
| 國立恆春工商 | 教務處 | 教學組長 | 1999年08月  至2000年07月 |

**(2.4)近五年內曾講授過之課程**

資訊科技概論、Android App程式設計、軟硬整合--Arduino自造、C++程式設計、進階程式設計。

(3)國立新營高級工業職業學校資訊科陳忠謀科主任

**(3.1)主要學歷**

|  |  |  |  |
| --- | --- | --- | --- |
| 時間 | 畢業學校 | 畢業科系 | 獲得學位 |
| 100.09-102.06 | 南榮科技大學 | 工程科技研究所 | 碩士 |
| 90.09-93.06 | 國立高雄師範大學 | 工業教育學系資訊技術組 二技 | 學士 |
| 81.09-86.06 | 建國工商專校 | 電機工程科 | 專士 |

**(3.2)現職及與專長相關之經歷(按時間先後順序由最近經歷開始填起)**

|  |  |  |
| --- | --- | --- |
| 時間 | 任職處室 | 職稱 |
| 102.08-迄今 | 實習處 | 資訊科主任 |
| 100.08-101.07 | 進修學校 | 教務組長 |
| 99.08-100.07 | 技術教學中心 | 幹事(網管) |

擔任學校的網管的職務，深覺得資訊安全的重要。且目前正值新課綱發展之際，除了部定的課程之外，更發覺目前群科中心所發展的IOT、介面電路控制及智慧機械等相關議題都與資訊安全都有密切的關係，因此有構想將資訊安全相關技術導入新營高工資訊科的課綱之中。

近年來，因與崑山科技大學資訊工程系簽定資訊向下紥根計畫合作同意書，透過此計畫讓資訊科的學生透過邏輯運算思維及程式先修檢測（APCS）讓資訊科的學生近年來在有關程式設計的比賽中獲得佳績：

|  |  |  |  |
| --- | --- | --- | --- |
| 學年度 | 工科技藝競賽 | 科展 | 全國技能競賽 |
| 104 | 電腦修護工 金手獎第一名  電腦軟體設計 優勝第十九名 | 分區科展  電腦與資訊學科 佳作  工程學科員（一）佳作 | 機器人職種  分區賽　佳作第五名  佳作第八名  決賽 全國第三名 |
| 105 | 電腦修護工 金手獎第十一名  電腦軟體設計 金手獎第三名 | 電腦與資訊學科 優勝  　　　　　　　　佳作  工程學科員（一）佳作 | 機器人職種  分區賽 第三名 |
| 106 | 電腦修護工 優勝第十六名 |  | 機器人職種  分區賽 第三名  佳作第六名  佳作第十一名  佳作第十八名 |

本校逐步導入資訊安全相關課程，將透過大專協同教學由崑山科技大學資工系曾龍博士協助資訊安全課程的導入。

1. **外聘專家簡介**

**(除上述參與教師外，請簡述本課程預計再另外聘請專家(如業師)，並略述外聘人員之學經歷背景、專業、主要負責協助發展課程模組主題、授課內容與時數以及預期可對本課程產生之貢獻等)**

| 姓名 | 公司／職稱 | 最高學歷 | 專長 | 在本課程主要協助發展課程模組主題或授課內容與時數、預期可對本課程產生之貢獻等 | 備註 |
| --- | --- | --- | --- | --- | --- |
| 吳哲仰 | Team T5/Senior Researcher | 臺灣大學資訊工程系碩士 | 應用程式安全、逆向工程、漏洞利用 | 協助發展課程模組主題(系統安全)及主題講座(應用程式安全: 從逆向工程到漏洞利用)  。預期可對本課程產生之貢獻包括完成系統安全之教材發展與啟發學生對資訊安全的熱情。 | 已徵詢業師同意 |
| 郭建邦 | 鈊安資訊科技股份有限公司/專案經理 | 成功大學電機工程學系碩士 | 資訊安全、公開金鑰基礎建設、專案管理、虛擬化/網路系統整合 | 協助發展課程模組主題(現代密碼之家解密與破密分析、網路安全之防火牆實務、  網路安全之入侵偵測系統實務、  網站安全防護實務:WAF) 。  預期可對本課程產生之貢獻為協助完成課程模組主題教材。 | 已徵詢業師同意 |

(請於備註欄註記，是否已徵詢業師協助授課之意願，以及是否獲得同意)

1. **經費與進度規劃**

**一、進度規劃及相關行政配置**

**(請簡述相關行政配套及相關資源投入的情形，並於下表簡述計畫執行進度規劃甘特圖)**

**進度規劃甘特圖 (計畫期程規劃請依徵件公告中四、計畫期程為主並自行調整)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 年月份  工作項目 | 107年 9月 | 107年 10月 | 107年 11月 | 107年 12月 | 108年 1月 | 108年  2月 | 108年  3月 | 108年  4月 | 108年  5月 | 108年  6月 | 108年  7月 | 108年  8月 | 108年 9月 | 108年 10月 | 108年 11月 | 108年 12月 | 109年 1月 |
| 設備採購與安裝 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 教學與實習環境系統開發 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 教材編纂  八月編撰第  一至四周教材  九月編撰第  五至八周教材十月編撰第  10至14周教材十一月編撰第  15至19周教材 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 台南一中示範教學 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 九月編撰期中實測題庫 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 十月召開第一次業界專家檢討會議 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 十一月開始新營高工協同教學 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 十二月編撰期末實測題庫 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 一月問卷調查與分析 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 一月召開第二次業界專家檢討會議 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 107學年第二學期示範課程推廣 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 六月底召開第三次業界專家檢討會議 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 高中職生種子師資培訓 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 108學年第一學期示範課程推廣 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 十二月底召開第四次業界專家檢討會議 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 系統統整與功能修正 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 期末報告撰寫 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 預估累計工作進度(%) | 6% | 11% | 16% | 22% | 28% | 30% | 35% | 45% | 50% | 55% | 60% | 65% | 70% | 75% | 80% | 90% | 100% |

**二、經費規劃**

**(本計畫教育部經費以補助人事費、業務費以及設備費為原則)**

單位：新臺幣/元

| **擬向其他機關與民間團體申請補助：▓無 □有** | | | | |
| --- | --- | --- | --- | --- |
| **經費項目** | | **細部經費明細(請條列算式)**  1.灰字為編列原則及基準，詳閱後請刪除。  2.填寫時，範例請移除，無規劃支用之項目也請刪除。 | 金額 | **用途說明** |
| 人事費 | 計畫主持費 |  | 138,598 | 計畫主持人負責計畫整體方向擘畫、監督計畫執行、進度管控、結案報告及成果發表等。 |
| 計畫協同主持費 | (1)6,000元/月× 17月× 1人= 102,000元  (2)補充保費（雇主負擔）102,000×1.91%=1,948元 | 103,948 | 計畫協同主持人協助計畫督導與執行、各活動之執行、協調與支援。 |
| 專任行政助理 | 學士級第1年薪資：  (1)薪資：26,780元/月×16月× 1人=428,480元  (2)107年年終：26,780元/月×1.5月×3÷12 =10,043元  108年年終：26,780元/月×1.5月=40,170元  (3)雇主負擔勞健保：(2,028元+1,250元)×16月=52,448元  (4)勞工退休金(以每月薪資投保級距6%為編列上限)：  27,600× 6%×16月=26,496元  (5)年終之補充健保費（雇主負擔）:50,213× 1.91%=959元 | 558,596 | 1. 由具備學士級學歷者擔任，薪資與年資採計由進用學校認定。 2. 如未依核定學歷聘用，所剩餘經費不得從人事費流用至業務費，全數繳回。 3. 擔任教育部不同計畫項下之專任助理，如同年12月份仍在職者，不論其在職月份是否銜接，均可依實際在職月數合併計算後，按比例發給年終獎金。 4. 依據「教育部人文及科技教育先導型計畫預算經費支用原則」編列。 |
| 兼任行政助理 | * 編列基準：3,000元至5,000元/人月   例：  (1)5,000元× 16月＝80,000元  (2)補充健保費（雇主負擔）80,000元×1.91%= 1,528元 | 81,528 | 依勞基法相關規定編列雇主負擔之健保補充保費(1.91%) |
| 勞僱型兼任助理人員勞健保費及勞工退休金(雇主負擔) | (1)雇主負擔勞健保：5,000元×7.45%×16月 = 5,960元  (2)勞工退休金(以薪資投保級距6%為編列上限)：**(投保級距4500~6000)**  6,000× 6%×16月= 5,760元 | 11,720 | 依勞基法相關規定編列雇主負擔之勞保費負擔(10.5%×0.7+0.1%=7.45%)、勞工退休金(6%) |
| 人事費小計 |  | 894,390 | 1. **各計畫人數以不超過4名為限，並以不超過計畫總經費之50%為原則**。請於所聘用之人事，說明負責之工作內容。 2. 上開人員聘任月數上限，依據計畫實際核定期程為主。 |
| **業務費** | 出席費/諮詢費 | (1) 2,500元×15人次＝37,500元  (2)補充健保費（雇主負擔）: 37,500元×1.91%=716元 | 38,216 | * + - 1. 依「中央政府各機關學校出席費及稿費支給要點」。       2. 核實報支。 |
| 主持費 | (1)2,000元×10場=20,000元  **(2)補充保費(雇主負擔)**：  20,000元×1.91%=382元 | 20,382 | 會議主持費用。核實報支。 |
| 講座鐘點費 | (1)專家學者2,000元× 35人次＝70,000元  (2)補充健保費（雇主負擔）: 70,000元×1.91%=1,337元 | 71,337 | 1. 依「講座鐘點費支給表」支給表核實報支。 2. 計畫邀請校外產學研專家專題講授，發予講座鐘點費，不另發予撰稿費。 |
| 稿費 | (1)CTF題庫出題費：100題，1,000元×100題=100,000元  (2)競賽題庫:25題×3場=75題，1,000元×75題=75,000元  (3)**補充保費（雇主負擔）**：  175,000元×1.91%=3,343元 | 178,343 | 1. 依教育部補助及委辦經費編列基準編列各教材發展所需稿費，並詳列計算式。 2. 命題(含解答)部分，**依考選部建立題庫各項費用支給要點，命題費(申論題700元/解答300元) 1,000元/題。**   (3) 核實報支。 |
| 資料蒐集費 | 20,000元×1式=20,000元 | 20,000 | 1. 圖書之購置以具有專門性且與研究計畫直接有關者為限。 2. 擬購圖書應詳列其名稱、數量、單價及總價於計畫申請書中。 3. 檢附廠商發票核實報支並列入該管機關之財產目錄。 4. 核實報支。 |
| 臨時人員工讀費 | (1)薪資：  140元/時×8時×150人=168,000元  (2)補充保費(雇主負擔)：  168,000元×1.91%=3,209元 | 171,209 | 1. 依勞基法相關規定編列雇主負擔之健保補充保費(1.91%)。 2. 核實報支。 |
| 勞僱型臨時人員勞健保費及勞工退休金(雇主負擔) | (1)雇主負擔勞健保：(以薪資7.45%編列)  168,000元×7.45% =12,516  (2)勞工退休金(以薪資6%編列)：  168,000元× 6% = 10,080元 | 22,596 | 1. 依勞基法相關規定編列雇主負擔勞保費(10.5%\*0.7+0.1%=7.45%)、勞工退休金(6%)。 2. 核實報支。 |
| 交通費(校外專家) | 交通費高鐵臺南-臺北來回2,700 元/人次。2,700元×20人次=54,000元 | 54,000 | 校外專家學者來校之交通費依「國內出差旅費報支要點」辦理，核實報支。 |
| 國內差旅費(計畫成員) | (1)交通費：高鐵臺南-臺北來回2,700 元/人次：2,700元×20人次=54,000元  (2)雜費：400 元× 20人次 ＝ 8,000 元 | 62,000 | 1. 計畫內相關人員參加計畫內工作會議、協助辦理各項培訓課程、成果發表會等計畫相關活動所需之交通費、雜費。 2. 依「國內出差旅費報支要點」辦理。 3. 核實報支。 |
| 膳費 | (1) 研習營  160元×60人次×2場=19,200元  (2)競賽  80元×40人次×3場=9,600元  (3)工作會議  80元×6人次×6場=2,880元 | 31,680 | 1. 午、晚餐每餐單價須於80元範圍內供應 2. 工作坊、研討、研習等活動：半日者，上限120 元/人日(1次誤餐1 次茶點)；1 日者，上限200 元/人日(2 次誤餐1 茶點)； 3. 計畫內部工作會議、座談、諮詢等非對外公開會議，以80 元/人次為原則。 4. 依據「教育部及所屬機關(構)辦理各類會議講習訓練與研討(習)會管理要點」核實報支。 |
| 宿費 | 1,600元×20人次= 32,000元 | 32,000 | 依國內出差旅費報支要點核實報支。 |
| 印刷費 | 100,000元×1式=100,000元 | 100,000 | 1. 辦理相關會議資料、各項報告、徵件資料、期中/末報告印製、教材等文件、活動手冊、海報及文宣等相關文件或資料之影印與裝訂費用。 2. 核實報支。 |
| 實驗材料費 | 100,000元×1式=100,000元 | 100,000 | 1. 請說明實驗材料費之用途 2. 單價未達1 萬元之物品。 3. 核實報支 |
| 場地使用費  (含設備租用及場地佈置) | 研習營：10,000元× 1式×5場=50,000元 | 50,000 | 1. 依「教育部及所屬機關(構)辦理各類會議講習訓練與研討(習)會管理要點」辦理。 2. 專家諮詢會議等活動場地費、影音設備租用費、場地佈線、海背板與大圖輸出及佈置費，檢據核實報支。 3. 不補助內部場地使用費。 |
| 雜支 | * 156,847× 1式=156,847元 | 156,847 | 1. 凡前項費用未列之辦公事務費用屬之。如文具用品、紙張、碳粉匣、光碟片、資料夾、郵資，如文具用品、紙張、光碟、資訊耗材、錄音筆、資料夾、郵資、事務性用品、電腦週邊用品、開會用品(紙杯、茶壺、茶葉、咖啡、糖包、奶精、紙巾…等)，以及執行計畫之其他相關雜項費用等。 2. 核實報支。 |
| **業務費小計** |  | 1,108,610 |  |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **設**  **備**  **費** | 設備項目名稱 | | 使用年限 | | 規格 | 單價 | 數量 | 總價 | 用途說明 | | | IDA pro逆向工程工具 | | 5 | | (1)可編程的、可擴展的、多處理器的、交叉Windows\*1、Linux\*1平臺主機分析程式  (2)支援數十種CPU指令集其中包含Intel x86,x64,MIPS等  (3)Windows含x86、x64、ARM32及ARM64 Decompiler\*1。  (4)Linux含x86、x64、ARM32及ARM64 Decompiler\*1。  (5)伺服主機(含同等級或以上規格)： (5.1)處理器Intel® Xeon® E3-1230 v6  (5.2)記憶體8G DDR4 2400 ECC UDIMM  (5.3)硬碟機2TB\*2 SATA3 6Gb 7200 rpm | 170,000 | 1 | 170,000 | 課程所需之工具，windows Floating、Linux Floating授權及license server | | 人工智慧平台 | | 5 | | (1)處理器Intel Xeon®處理器E3-1240 v6  (2)記憶體32G (含)以上。  (3)硬碟機2TB 2顆(含)以上  (4)運算顯示卡: GTX1070K-08G \*2 (含)以上 | 140,000 | 1 | 140,000 | 課程示範教學所需之系統,使用GPU運算。提供種子師資培訓使用及示範教學使用。 | | 行動CTF平台 | | 4 | | (1)處理器：Intel Core i7 (含)系列以上等級。  (3)記憶體：16GB (含)以上。  (3) 硬碟：1TB HDD(含)以上。 | 60,000 | 1 | 60,000 | 課程教學與示範使用。網站安全課程因教育部網路佈署各式安全偵測系統，為避免造成資安事件單產生，將以區域的行動CTF平台作為演練與示範使用之平台。 | | 行動示範平台 | | 4 | | (1)處理器：2.3GHz 4 核心 Intel Core i5(含)系列以上等級。  (2)記憶體： 8GB (含)以上。  (3)硬碟：256GB(含)以上。 | 60,000 | 1 | 60,000 | 課程示範教學使用，主要用途在系統安全課程模組上。 | | CTF測試與備援平台 | | 4 | | (1)處理器：Intel Core i7(含)系列以上等級。  (2)記憶體：16GB (含)以上。  (3)硬碟：512GB(含)以上。 | 67,000 | 1 | 67,000 | CTF競賽出題與測試時使用，內部測試與示範解題完成後再上傳到國家高速網路中心所提供的CDX平台。後續課程所舉辦的競賽及相關教學實作將使用國家高速網路中心所提供的CDX平台。 | | **設備費小計** | |  | **497,000** | | | | | | | |  | 1.計畫推動所需設備經費：以採購本專案相關教學設備為主，不得使用本部補助款採購一般事務性及個人教學設備(如單槍投影機、實驗桌椅、印表機及個人電腦等)；以不超過計畫總經費之20%為原則。  2.核實編列。 | | | | | | | | | | | | | |
| **合計** | | 2,500,000 |  |  |
| 1. 依行政院99年3月4日院授主忠字第0990001184號函頒對民間團體捐助之規定，為避免民間團體以同一事由或活動向多機關申請捐助，造成重複情形，各機關訂定捐助規範時，應明定以同一事由或活動向多機關提出申請捐助，應列明全部經費內容，及擬向各機關申請補助經費項目及金額。 2. 本計畫執行內容如經查證重複接受補助者，應繳回該項補助經費。 3. 相關經費編列及支用，請依「教育部補助及委辦經費核撥結報作業要點」（請至教育部網站 http://www.edu.tw/ 下載）相關規定辦理。 4. 行政管理費一律不予補助。 | | | **補助方式**：全額補助 | |
| **餘款繳回方式**：依據教育部補助及委辦經費核撥結報作業要點第11點規定辦理 | |

|  |  |  |  |
| --- | --- | --- | --- |
| **主持人** | **單位主管** | **會計單位** | **校長** |
|  |  |  |  |

**柒、預期成效**

**一、預期質化效益**

**(請說明計畫目標達成之情形及其效益，請參考審查重點項目自訂質化成效進行說明。例如，例如資安人才培育的效益、課程設計的創新性、例如資安人才培育的效益、課程設計的創新性、示範教學資源的擴散效益等)**

1.資安人才培育的效益

資安人才培育是國家發展資安非常重要的一環，特別是我國國家政策已將資安發展列入，值此嚴重欠缺資安人才的時代，必須有更多的資源投入。本計畫首度深耕非資訊相關學生的資安認知教學，更特別扎根高中職生，將進一步深化現有整體資安人才培育計畫。現整體計畫下大多著眼於大專以上資訊類別的學生為主體，在教育部資安紮根子計畫三則以體驗營模式推廣資安教育。本計畫關注於非資訊類大專生及高中職學生的資安認知教育，也是首度以課程模式推動的資安人才培育計畫。預計將為教育部資安人才培育計畫資安向下紮根奠定更深遠的影響與建立更長遠的效益，有進一步強化整體資安人才培育計畫。

2.課程設計的創新性

非資訊類別的學生及高中職學生由於尚未具備相關資訊技術背景，因此現有以大學專業資訊課程難以施教於上述學生，本計畫全新規劃課程內容，更以生動的實務教學取代枯燥的理論教學模式，透過動手做的實作教學模式帶動學生的學習熱情。本計畫不僅提供相關教學簡報還包括教學影片與相關演練image，另外也提供MOOCs教學影片供學生是前預習與事後複習用。本計畫學習評量不僅提供一般紙筆測驗模式更提供線上實務解題模式可立即觀察學生學習狀態。

3.示範教學資源的擴散效益

本計畫將配合總計畫規劃推動高中職資安種子師資培訓，將相關教學經驗與教學資源分享給參與的學校。另外本課程也先以兩個學校進行不同模式的示範教學，在台南一中教學模式上採用全新開設的學期課程，在新營高工模式上則採用現有課程搭配協同教學模式。本計畫更特別將協助與輔導學校開課列入計畫重點項目，預計將會吸引更多學校的參與，帶動國家資安人才培育的整體亮眼成效。

**二、預期量化指標**

| 項 目 | 預期目標 |
| --- | --- |
| 教學資源數 | * 課程教案手冊：\_\_\_\_1\_\_\_冊 (以整合成1冊為原則)   【註：手冊應含項目請參考徵件須知第七點(推動重點(2)】   * 實務課程設計與操作手冊：\_\_\_14\_\_\_\_份文件 * 實務課程教學環境設計手冊：\_\_\_10\_\_\_份文件， * 國網中心CDX平台(CTF平台使用與解題手冊)：\_\_\_\_9\_\_份文件 * 示範教學多媒體影片： * \_\_\_\_20\_\_\_個課程主題錄影教學，長度共\_\_\_186\_\_\_\_分鐘 * \_\_\_\_5\_\_\_ 個課程主題Moocs，長度共\_\_\_50\_\_\_\_分鐘 |
| 示範課程  推廣程度 | * 示範課程至他校授課數：\_\_\_10\_\_\_\_間共\_\_\_10\_\_\_\_次   學校及系所名稱：[本計畫將配合總計畫動態調整學校及系所]  宜蘭高中，中興附中，虎尾高中，嘉義高中，台南女中，台南二中  宜蘭高工， 嘉義高工， 新營高工，新化高工，   * 授課主題數：\_\_\_18\_\_\_\_主題數 * 辦理示範課程研習營數：\_\_\_10\_\_\_次 * 辦理校際課程演練次數：\_\_\_6\_\_\_\_次   將配合總計畫在北中南各舉辦二場，  預計舉辦場地:台北--台灣科技大學，台中--中學大學，  高雄--中山大學  預計舉辦時間:寒暑假或周末日 |
| 學生學習回饋 | * 學員參與資安相關競賽： 150 人次，請列出競賽：   BreakallCTF,MyFirstCTF, AIS3 CTF, Pico CTF,Angstorm CTF   * 學員參與資安相關展示活動： 200 人次，請列出活動：happyWeekend資安研習營、資安特訓營(Summer camp/Winter camp) 、AIS3 * 學員報考資安相關證照資格：無 * 其他，請說明： 無 |
| 業師參與  教材程度 | 業師人數： 2 人(業師姓名：\_\_\_吳哲仰\_\_\_\_郭建邦\_\_\_\_\_\_\_\_\_)  業師參與教材編撰主題數：\_\_\_5\_\_\_主題數  業師所屬廠商家數： 2 家(公司名：\_\_\_\_\_\_\_\_\_\_)  吳哲仰:Team T5/Senior Researcher  郭建邦: 鈊安資訊科技股份有限公司/專案經理 |
| 實習(驗)環境或平臺 | ▓自建教學環境或平臺: 簡述實習(驗)環境(資安相關設備、軟體)：    [1]本計畫將建置程式設計安全的環境，利用現有教學環境(電腦教室的PC) ，主要採購IDA Pro軟體及其相關授權，並配合業界師資吳哲仰(Sean Wu)舉辦講座教學(將邀請五位學校教師及示範課程學校資優學生，此五位老師將參與並組成推動小組針對此主題進行規劃與試辦教學)  [2]本計畫將建置以最基礎的設備(PC:8GB RAM須包含GeForce GTX 1060等級以上的 GPU)建置人工智慧平台，並製作相關教材給參與學校推動相關教學與設備建置。  [3]本計畫將將採購行動CTF平台到校實地演練考試與學習用(部分網站安全主題因為教育部學術網路部有多重的資安防禦，難以試辦教學因此使用行動CTF平台可解決此問題)，採購行動示範平台進行示範教學使用。  [4] 本計畫將採購CTF測試與備援平台，將建立以CTFD為基礎的練習平台提供不同學校特殊需求的題型使用，並將利用此平台先行測試新出題目的測試。  ▓使用國網中心CDX平臺  使用(註冊)人數：教師\_50+\_\_ 人；學生\_\_200+\_\_\_人  使用情形說明：  本計畫將於國網中心CDX平臺布建CTF平台作為學生練習與實作解題， 因此會大量使用 國網中心CDX平臺 。 |
| 依計畫性質自行增列指標 | (事件、數字)  1.配合總計畫舉辦高中職資安種子師資培訓營6場，培訓資安種子師資60位。  2.輔導10間高中職學校使用教材模組於相關課程(資訊科技概論、計算機概論、python程式設計、特色選修課程) |

**(接受課程補助後，須配合本部或推動計畫辦公室相關管考措施，不定期或於成果報告中，依授課實況填寫量化成果報告表)**