課程資訊 及 課程大綱

<table>
<tr><td>課程名稱（中文）</td><td>電腦攻擊與防禦</td></tr>
<tr><td>課程名稱（英文）</td><td>The Attack and Defense of Computers</td></tr>
<tr><td>授課教師</td><td>張文村</td></tr>
<tr><td>科號</td><td>11220IIS 500100</td></tr>
<tr><td>上課時間
class time</td><td>Rn56(週四 12:10-15:10)</td></tr>
<tr><td>開課年級</td><td>電資院碩士班</td></tr>
<tr><td>學分數</td><td>3</td></tr>
<tr><td>人數限制</td><td>40</td></tr>
<tr><td>先修科目</td><td>建議選課同學修過「 Linux 作業系統核心」(或「Linux 作業系統」)、「網路安全」兩者或至少其一為佳</td></tr>
<tr><td></td><td></td></tr>
<tr><td>課程簡述
Brief Course Description (required)</td><td>本課程旨在結合與實務，以常見的惡意程式為出發點，介紹駭客常見攻擊手法，與如何透過縱深防禦的架構，進行事前檢測、偵防、事中鑑識等方式；此外亦安排相關資安工具的操作演練，協助同學體驗攻防實務技巧，進而養成在軟體開發上的資安意識，進入資安攻防世界。</td></tr>
<tr><td>關鍵字</td><td>＃IT 偵查與防禦 ＃OT 偵查與防禦 ＃零信任 ＃資安事件鑑識
＃弱點掃描 ＃資安檢測 ＃ICS 滲透測試</td></tr>
<tr><td>課程大綱
Detailed Course Syllabus</td><td>一、課程說明(Course Description)
本課程結合理論與實務操作。將邀請資策會資安所多位不同領域之專家，介紹 IT、OT、IoT 等領域之資安偵防、鑑識、檢測、滲透測試技術，建立事前防禦、事中偵測、事後應變等完整面向的資安攻防知識；此外，亦透過理論、實務交錯搭配模式，由專家們帶入各種業界實務經驗，幫助學習跨領域資安攻擊與防禦技術。
<table>
<tr><td colspan="2">一、資安偵防與鑑識</td></tr>
<tr><td>1,資安偵防與零信任實務應用</td><td>以零信任基礎概念，介紹近年廣被運用之 APT 攻擊事件及其偵防，並透過 MITRE ATT&CK 與 D3FEND 攻擊與防禦框架解說，透過實際 APT 資安攻擊事件為情境進行攻擊手法與緩解措施分析，讓同學對 APT 攻擊事件的偵防有所瞭解。
■ 零信任基礎概念介紹
■ 零信任之元件與運作方式介紹
■ 介紹 ATT&CK 與 D3FEND 框架
■ 以 ATT&CK 與 D3FEND 框架解析真實攻擊事件</td></tr>
<tr><td>2.XDR 系統介紹與</td><td>以開源工具 Wazuh 進行說明，透過系統功能介</td></tr>
</table></td></tr>
</table>

		實務應用	紹、系統架構介紹、資安規則介紹等，讓同學有一 XDR 概觀。 課綱如下： ■ 資安工具概論 ■ 介紹 XDR 的概念及功能 ■ 介紹 Wazuh 的組成元件及應用 ■ 架設 Wazuh，透過設定規則及觸發規則進行觀察、驗證 ■ 結合 AI 的應用
		3.資安事件鑑識分析實務(一)	數位鑑識為當資安事件確實發生時，針對事件相關證據(如：日誌紀錄、網路軌跡等)之完整蒐集、保存及事件根因分析。透過介紹數位鑑識概念、鑑識分析階段、輔助工具等，以 Demo 或帶領同學進行實務操作方式，學習如何進行資安事件鑑識調查。 課程大綱如下： ■ 資安事件應變處置 ■ 何謂數位鑑識 ■ 鑑識流程與輔助工具 ■ 實務練習(Lab)
		4.資安事件鑑識分析實務(二)	經由前一堂課，同學已初步建立資安事件應變處置流程觀念，本堂課將著重於數位鑑識採證後之事件根因分析實務操作，包含鑑識工具實務應用、日誌分析及惡意程式分析等。 本課程將介紹： ■ 鑑識工具包（如：SIFT、FlareVM） ■ 事件分析實務 ◆ 稽核日誌分析 ◆ 磁碟映像分析 ◆ 記憶體分析（消逝型資料） ◆ 惡意程式分析
		二、資安檢測與實務	
		1.資安探險家：弱點掃描實務(一)	■ 資安之門：認識弱點掃描 ◆ 目的和重要性 ◆ 資安探測流程 ■ 敵人剖析：揭密弱點家族 ◆ 關於弱點 ◆ 常見類型 ◆ 影響力與防禦機制 ■ 武器庫解析：探索弱點掃描工具 ◆ 主機弱點掃描工具概述 ◆ 主機弱點掃描工具實務

		2. 資安探險家：弱點掃描實務(二)	◆ 網路探測與資訊蒐集實務 ◆ 網站弱點掃描工具概觀與實務 ◆ 原始碼弱點掃描工具概述 ◆ 原始碼弱點掃描工具實務
		3. 探索未知的 IoT：IoT 設備檢測實務	■ IoT 世界的隱藏危機：威脅與挑戰揭秘 ◆ 常見的 IoT 安全威脅 ◆ 實際 IoT 攻擊案例分析 ■ IoT 安全之道：解讀國際 IoT 安全弱點 ■ IoT 護衛者之路:探索與實踐 IoT 設備檢測的奧秘 ◆ IoT 設備檢測的基本流程 ◆ 工具和技術的概述
		4. 晶片的資安確保之道：晶片資安標準的現況與未來發展趨勢	■ 硬體攻擊的本質 ◆ 知己知彼~瞭解可用的元件 ◆ 硬體威脅建模 ◆ 初始攻擊面 ■ 侵入式攻擊 ■ 非侵入式攻擊 ◆ 旁通道攻擊 ◆ 錯誤注入攻擊 ■ 台灣晶片安全標準 ◆ 晶片安全標準發展策略 ◆ 系列標準 ■ 晶片資安檢測要點
		三、工控資安偵防與滲透測試	
		1. 工業控制系統(ICS)資安挑戰及防護通識介紹	■ 工控系統及網路架構概觀 ■ 工控聯網資安威脅演進 ■ 工控資安攻擊面向解析 ■ 工控設備主機資安防護 ■ 工控網路環境資安防護
		2. 工控聯網分析技術	■ Modbus 通訊協定介紹 ■ Modbus 封包格式/功能定義 ■ Modbus 模擬環境及工具運用 ■ 封包分析與鑑識工具實作 ■ Modbus 範例解析實作
		3. ICS 網路滲透測試分析技術	■ ICS 實體 Testbed 環境與操作 ■ 控制情境流程介紹 ■ Testbed 各式滲測案例演練 ■ Testbed 攻擊封包解析實作

4.ICS 入侵偵測防護技術	■ 入侵偵測防護工具 Snort 介紹 ■ 偵測規則設計習作 ■ 實例攻擊與偵防演練
四、安全軟體發展生命週期	
SSDLC	■ SSDLC 簡介 ■ 安全軟體設計五大階段：需求、設計、開發、測試與部署

二、指定用書(Text Books)

無

三、參考書籍(References)

1.The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks

2. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions

四、教學方式(Teaching Method)

講述：以講述方式，介紹 IT、OT、IoT 等領域之資安攻擊、偵測與鑑識運作。
實作：透過相關偵測、弱掃、鑑識與滲透測試工具，實機演練。

五、教學進度(Syllabus)

週次	授課內容
1	課程介紹
2	資安偵防與零信任實務應用
3	XDR 系統介紹與實務應用
4	資安事件鑑識分析實務(一)
5	資安事件鑑識分析實務(二)
6	資安探險家：弱點掃描實務(一)
7	資安探險家：弱點掃描實務(二)
8	期中考
9	探索未知的 IoT：IoT 設備檢測實務
10	晶片的資安確保之道： 晶片資安標準的現況與未來發展趨勢
11	工業控制系統(ICS)資安挑戰及防護通識介紹
12	工控聯網分析技術
13	ICS 網路滲透測試分析技術

14	ICS 入侵偵測防護技術
15	安全系統發展生命週期(SSDLC)
16	期末考

六、成績考核(Evaluation)

No.	項目	百分比	說明
1.	期中考試	45%	考試範圍 1~7 周課程內容
2.	期末考試	45%	考試範圍 9~15 周課程內容
3.	課程參與	10%	上課參與和討論

七、可連結之網頁位址 相關網頁(Personal Website)

核心能力 Core capability

請勾選	此科目對應之系所課程規畫所欲培養之核心能力 Core capability to be cultivated by this course	權重（百分比） Percentage
	具有設計與操作實驗以及分析、解釋數據的能力。 To be able to design and perform experimentation as well as analyze and explain the experiment data.	30%
	具有發現問題、定義問題、並設計程式以解決問題的能力。 To have the ability to discover problems, define them, and design computer programs to solve problems.	20%
	具有資訊、數學及科學的基礎知識。 To have fundamental knowledge of computer science, mathematics, and science.	20%
	具有分析、設計、開發、整合、測試、與評估資訊系統、元件、或演算法的能力。 To be able to analyze, design, develop, integrate, test, and evaluate systems, components, and algorithms of computer science.	10%
	具有良好的溝通技巧與跨領域團隊合作的能力。 To have good communication skills and be able to cooperate with others in interdisciplinary teams.	%
	瞭解與資訊相關之產業脈動與最新的資訊科技進展。 To understand the most recent technological and industrial advancements regarding computer science.	10%
	瞭解資訊科技對於全球性社會、經濟、文化等層面的影響與責任。 To understand the social, economical, cultural effects of computer science and related technologies on the global level.	%
	瞭解國際視野及終身學習的重要性。 To understand the importance of international view as well as lifelong education.	%
	尊重學術、工程倫理、及智慧財產權。 To respect academics, engineering ethics, and intellectual property.	10%