資安菁英人才培訓課程第三期資訊

課程時間	上午 9 時 30 分至下午 5 時止，中間休息 1.5 小時
課程地點	10/14~11/11 進出口同業公會(捷運行天宮站)

（一） Cloud Security：雲端平台安全攻防

課程日期	112 年 10 月 14 日（六）
NICE Framework	Protect and Defend
ECSF 培訓對象	資安事件工程師、資安威脅情資分析師、資安實務者、資安研究員、數位鑑識調查員、滲透測試工程師
先修技能	具備雲端基礎知識即可
自備工具	筆電（裝有瀏覽器與 ssh client）

1. 課程介紹：

本課程旨在提供學生對雲端攻擊和防禦的深入理解，並透過實作環節培養學生在主要雲端平台（AWS、GCP）上實際應對攻擊和實施防禦措施的能力。課程將涵蓋雲端計算的基本概念、最新的攻擊趨勢，以及依照 NIST Cyber Defense Function（CSF）的五大功能分類進行的雲端防禦實作。

2. 講師介紹：

林殿智(Dange Lin)現為奧義智慧科技的資深資安威脅研究員，專注於汽車安全、雲端安全、機器學習與情資分析等領域，目前於 MIH Working Groups 中負責資訊安全。曾於 HITCON、MOPCON、CYBERSEC 等多個研討會發表演講，也曾擔任 AIS3 講師。

3. 課程摘要：

(1) 導論

- 介紹雲端計算的基本概念和優勢

(2) 雲端攻擊概念與攻擊趨勢

- Coud Security Alliance – Top 11
- Backhat, DEFCON 最新攻擊手法介紹

(3) AWS Lab

- AWS 環境操作
- 雲端攻擊實作
- 雲端防禦實作（依照 NIST CSF 分類）

(4) GCP

- GCP 環境操作
- 雲端攻擊實作
- 雲端防禦實作（依照 NIST CSF 分類）

（二） 社交工程戰略攻防實務

課程日期	112 年 10 月 15 日（日）
NICE Framework	Protect and Defend
ECSF 培訓對象	資安事件工程師、資安威脅情資分析師、資安實務者、資安研究員、數位鑑識調查員、滲透測試工程師
先修技能	網路安全
自備工具	Windows

1. 課程介紹：

資安專家常言要隨時緊覺來自四面方駭客的社交工程攻擊，以絕自身成為攻擊者對企業的破口。然而，若未對社交工程有實務理解，那該如何知道第一線駭客是如何進行攻擊的呢？本課程為此打造了一系列完整的社交攻擊的實務武器化技巧，統整了近期在野正流行的社交工程方法與策略，能幫助學員貼近攻

擊者視角理解這些攻擊行動的原理、而能在第一時間感知並防禦這些新型態濫用知名網路服務而達成的釣魚手段。

2. 講師介紹：

馬聖豪（@aaaddress1）目前為 TXOne Networks 產品資安事件應變暨威脅研究團隊資深威脅研究員，專研 Windows 逆向工程分析超過十年經驗，熱愛 x86、漏洞技巧、編譯器實務、與作業系統原理。此外，他目前為台灣資安社群 CHROOT 成員，並曾任 Black Hat USA、DEFCON、CODE BLUE、HITB、VXCON、HITCON、ROOTCON、CYBERSEC 等各個國內外年會講者與授課培訓，並著有全球熱銷中英資安書籍《Windows APT Warfare：惡意程式前線戰術指南》。

3. 課程摘要：

(1) 常規釣魚信件識別教戰原則

- 識別內文的合法性
- 發送者帳號、Emai 組織、網站域名.
- Googe/M365 頭貼

(2) 社交工程武器化流程

- 標靶對象情報蒐集
- 制定針對個人性的釣魚內容
- 選取並制定適合標靶對象的對應技巧與執行

(3) 3. 多種已被野外開採的知名服務釣魚缺陷

- 竊取帳號密碼-釣魚網站
- 供應鏈下手-Github 開源專案釣魚(*.sn), apt, rpm, pip 套件管理器
- 欺騙與取信策略

- 濫用 0365 Outlook 預覽缺陷執行惡意程式
- 劫持 Teams 設計缺陷達成濫發微軟簡訊技巧
- Google+0365 的 Calendar 竄改發送者技巧
- 濫用 Google Drive 達成竄改文件發送者技巧
- 通殺蘋果全系列郵件客戶端(macOS & iOS)顯示的 Email Account 紀錄
- 低軌衛星竊聽
- Telegram try 電話號碼收 SMS
- 針對工程師的 Visual Studio 供應鏈釣魚法

(4) 4. 攻擊彈頭實務策略

- .SCR
- .LNK & PIK
- .ISO + DLL Side-Loading
- Office, Macros, XLS + Bypass MOTW
  - ISO, ZIP, OneNote File

（三） 枕戈待旦，網站應用程式安全實戰

課程日期	112 年 10 月 21 日（六）、10 月 22 日（日）
NICE Framework	Protect and Defend
ECSF 培訓對象	資安事件工程師、資安威脅情資分析師、資安實務者、資安研究員、數位鑑識調查員、滲透測試工程師
先修技能	具備網頁基礎知識即可
自備工具	課程題庫將使用 Docker 環境，因此需具備可執行上述環境之筆電

1. 課程介紹：

本課程首先會讓學員理解網站應用程式常發生的漏洞及原因，並在其基礎上帶出近年來企業最常遇到的網站漏洞威脅及些許較為複雜的情況。另外，除了提供模擬練習環境讓學員練習曾經發生過的資安事件，也會有題目讓學員上手近年發表的資安攻擊手法及 Bug Bounty 案例中的奇技淫巧，並在最後討論如何避免相關問題發生。

2. 講師介紹：

蘇學翔（Boik Su）為知名資安社群 CHROOT 成員，並專精於 Web 滲透測試。其曾於 OWASP AppSec/HITCON/ROOTCON 等國際知名資安研討會發表研究成果，並在 HITCON 及中小企業等擔任講師。

3. 課程摘要：

- 導論網頁應用程式安全從入門到進階
- 企業網頁應用程式常見攻擊手段
- 真實資安事件模擬題練習及檢討
- 網頁應用程式攻擊手法奇技淫巧

（四） 無冕防禦-藍隊核心工法剖析

課程日期	112 年 10 月 28 日（六）、10 月 29 日（日）
NICE Framework	Analyze、Investigate
ECSF 培訓對象	資安事件工程師、資安威脅情資分析師、資安實務者、資安研究員、數位鑑識調查員
先修技能	具備基本 Windows 與 Linux 操作能力即可
自備工具	VMware Workstation、VMware Fusion（Mac User 請使用非 M1/2 晶片之 Mac），課程預計提供 4 套 VM（ova），硬碟空間需求 60G 以上，記憶體 16G 以上

1. 課程介紹：

駭客威脅的猖獗，使得企業防禦方需要花費許多時間與資源，應對攻擊者所造成的損害。但多數企業對於完善的事前、中、後的概念與思維，甚至需要的資安解決方案也不盡然了解。因此本課程以藍隊思維為出發點，進行探討藍隊所需的所有概念與技術。課程內容預計包含事件應變處理、數位鑑識、惡意程式分析、威脅監控等藍隊日常所需的一切，涵蓋理論與實作。學員將具備藍隊相關的知識與技術，為企業資安貢獻一份力！

2. 講師介紹：

鄭仲倫(Mars Cheng), TXOne Networks 產品資安事件應變暨威脅研究團隊經理/台灣駭客協會 常務理事

Mars 負責協調 TXOne 產品安全與團隊威脅研究事宜。過去曾於行政院國家資通安全會報技術服務中心（NCCST）擔任資安工程師，負責物聯網設備與工業控制環境之安全研析，強化政府機關與關鍵基礎設施資安防護能量。

Mars 在我國與國際資安會議中發表演講與授課培訓超過 40 場次，這些會議包括 Black Hat USA/Europe/MEA、RSA Conference、DEFCON、FIRST、TROOPERS、CODE BLUE、HITB、HITCON、SecTor、SINCON、ICS Cyber Security Conference Asia and USA、CYBERSEC、CLOUDSEC、VXCON 及 InfoSec Taiwan 等。並致力於分享各類型資安知識，於資安卓越中心（CCoE）計畫、國防部、經濟部、教育部、HITCON Training 及多間上市櫃企業均有授課經驗。

Mars 專注於 ICS/SCADA、IoT 及企業網絡安全的相關資安議題研究，至今提交了 10 多個 CVE 編號，並於三本 SCI 期刊中（JCR Ranking Top 20%）發表與應用密碼學相關之論文。此外，Mars 同時還是台灣駭客協會產業與政策委員會召集人與行政院資通安全稽核計畫稽核委員，亦曾擔任台灣駭客年會 HITCON 2022/2021 的總召集人與 2020 的副總召集人。

3. 課程摘要：

(1) 藍隊的前世今生

(2) 資安威脅監控-端點與網路偵測

- 資訊安全監控中心簡介
- 閘道及應用程式威脅事件分析
- 端點威脅事件分析
- 網路威脅事件分析
- OSINT 威脅情資應用分析

(3) 資安事件應變流程與數位鑑識實務

(4) 惡意程式分析實務

（五） 王者歸來-網域 AD 的善惡法則(基礎、進階及雲端篇)

課程日期	112 年 11 月 4 日（六）、11 月 5 日（日）、11 月 11 日（六）
NICE Framework	Protect and Defend
ECSF 培訓對象	資安事件工程師、資安威脅情資分析師、資安實務者、資安研究員、數位鑑識調查員、滲透測試工程師
先修技能	具備基本 Windows 與 Linux 操作能力即可
自備工具	VMware Workstation、VMware Fusion（Mac User 請使用非 M1/2 晶片之 Mac），課程預計提供 4 套 VM（ova），硬碟空間需求 70G 以上，記憶體至少 20G 以上（建議 32G 為佳)；學員 Client 需具備 RDP 連線功能

1. 課程介紹：

微軟所提供的 Active Directory (AD)被企業廣泛用作身份和訪問管理的骨幹。AD 也因作為企業最為關鍵的資產而不斷地遭到

攻擊者覬覦，儘管防禦方深知 AD 是企業運營的關鍵，但攻擊者仍然可以藉由濫用 AD 服務提供的這些機制來破壞企業網路運作達成各種惡意目的，甚至搭配了勒索軟體進行組合式的攻擊，進而對企業造成運營影響與財損。

本課程將深入探討本地、混合和 Azure AD 的完整運作架構，探索不同類型的 AD 服務、攻擊及防禦技術。 我們將通過濫用關鍵元件的機制來介紹各種 AD 攻擊技術。本課程預計將是需要學員動手實作的一門課程，對於每個實作，都會有一個作為核心概念的深入討論，使學生能夠理解理論背景並有效地實施攻擊技術。 對於介紹的每一種攻擊技術，我們還將介紹防禦方使用的偵測指標，學員將了解該如何以防禦方的角度發現並偵測攻擊，以建構高度韌性的企業環境。

2. 講師介紹：

陳星羽(Dexter Chen), @chen hsing yu

Dexter Chen 目前於 TXOne Networks 擔任資安威脅研究員，專注於滲透測試、紅隊手法及網域(Active Directory)安全。Dexter 於 HITB、CODE BLUE、Black Hat MEA、HITCON、CYBERSEC 等國際資安會議均發表過研究。加入 TXOne 前，服務於 Trend Micro 紅隊，擅長橫向移動和紅隊的 Operation Security，是一個整天專注於漏洞研究、各種攻擊手法分析及 CTF 的資安愛好者。此外 Dexter 曾多次擔任資安課程講師，包含 HITCON Training 2022/2021/2020、資安卓越中心(CCoE)計畫及國防部等單位。

鄭仲倫(Mars Cheng)

TXOne Networks 產品資安事件應變暨威脅研究團隊經理/台灣駭客協會 常務理事。Mars 負責協調 TXOne 產品安全與團隊威脅研究事宜。過去曾於行政院國家資通安全會報技術服務中心（NCCST）擔任資安工程師，負責物聯網設備與工業控制環境

之安全研析，強化政府機關與關鍵基礎設施資安防護能量。Mars 在我國與國際資安會議中發表演講與授課培訓超過 40 場次。

3. 課程摘要：

(1) 網域（Azure/Active Directory, AD/AAD）背景知識概述

- 網域（AD/AAD）功能說明
- MITRE ATT&CK 映射網域（AD）
- 網域（AD）的資安威脅環境與課程工具簡介

(2) 網域（AD）的攻擊實戰

- 從 PowerShel 進入 AD 環境
- AD 環境中的情資偵蒐
- AD 認證機制 Kerberos 協定剖析
- AD 環境中使用者與電腦憑證盜竊
- AD 環境中的權限提升
- AD 環境中的權限維持

(3) 網域（AD）的偵測實戰

- AD 環境偵測方式剖析
- AD 環境偵測實作

(4) Azure AD 攻擊與偵測實戰

- Azure AD 攻擊手法剖析
- Azure AD 偵測手法剖析