資安卓越中心規劃建置計畫
資安菁英課程
課程規劃

(一) 惡意程式實務分析_黃昭明(zha0)

1. 課程類型:Malware Analysis
2. 課程日期:110 年 11 月 13 日(六) ~ 110 年 11 月 15 日(一),共三天。
3. 課程總時數 18 小時。
4. 課程介紹:

   本課程注重實際案例,從基礎說起,深入淺出,希望能成為入門的基石課程,從基礎組合語言及 C 中學習,切入作業系統基礎知識,分析惡意程式常見技巧,最後給出分析惡意程式的步驟及完整流程。講師將帶領學員從惡意程式分類、分析環境建置開始,逐步學習靜態分析、動態分析、認識組合語言與反組譯、學習使用 IDA 進行反組譯，了解惡意程式的行為、程式碼注入(Injection)與攔劫 Hooking),透過實際樣本一覽惡意程式常用的迷惑手法。
5. 講師介紹:黃昭明(zha0)

   目前於 TeamT5 杜浦數位安全擔任資安工程師,也為知名資安社群 CHROOT 成員。

   專長 Windows 事件調查及惡意程式分析,專注於 C/C++、x86、漏洞技巧、編譯器實務、與作業系統原理相關研究。也擔任 HITCON Training 多年講師,並曾於 HITCON 研討會發表研究成果:

   - 2006 - Virus Evolution
   - 2010 - Owned Kiosk
   - 2015 - PLEAD the Phantom of routers
   - 2016 - Catching the Golden Snitch
6. 課程摘要:

   (1)組合語言

   a. 數碼系統
   b. 暫存器
   c. 指令集
   d. 走入保護模式

   (2)Windows 作業系統

   a. 資料型態
   b. 功能及名詞解譯
   c. API 使用及分類
   d. PE 檔案格式
   e. 使用除錯程式了解系統機制
   f. 工具使用 Windbg/Ollydbg/IDA Pro

   (3)惡意程式常見手法

   a. 磁碟/檔案竄改

b. 記憶体注入
c. 開機啟動方式
d. 偵測與查找
e. 工具使用 Volatility/Windbg/Ollydbg

(4)近期常見樣本分析

a. 深入完整分析

7. 學員先修技能:基本的電腦操作技能,學過程式語言、懂得怎麼撰寫程式尤佳,對分析惡意程式有興趣。
8. 學員自備工具:筆電、VMware。

(二) Office 漏洞魚叉開發實務_馬聖豪(ShengHao Ma, aka aaaddress1)

1. 課程類型:Vulnerability Research / Malware Analysis
2. 課程日期:110 年 11 月 19 日(五),共一天。
3. 課程總時數 6 小時。
4. 課程介紹:

   在各國網軍攻擊行動中,Office 系列辦公軟體一直是第一線釣魚需求的兵家必爭之。而在看似誘人的資料文件中埋入帶有後門的 VBA(Visual Basic forApplication)更是各種攻擊行動相當普遍的技巧。然而在 Office 365 在 2018 年後升級、引入了 Defender ATP(Advanced Threat Protection)引擎作為主動防禦,使得啟用 MACRO 的 VBA 釣魚手法變得難以施行。在本課程中我們將介紹最新版 Office 365 防禦策略與查殺鏈,並從最典型的 VBA 後門開始撰寫起。並以知名的近年攻擊行動與開源套件、新型態 Excel Macro4.0(XL4)攻擊技巧,並以手工撰寫 Excel BIFF8 結構來由深度探索 Office 文件規格。務使學員能在課程中做中學,體驗對當前 Office 多層次防護見招拆招的成就感。
5. 講師介紹:馬聖豪(ShengHao Ma, aka aaaddress1)

   目前於 TXOne Networks 擔任資安威脅研究員,

   專研 Windows 逆向工程分析超過十年經驗,熱愛 C/C++、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。並曾擔任 DEFCON、HITB、BlackHat、VXCON、HITCON、CYBERSEC 等各個國內外年會講者與授課培訓、並著有熱銷資安書籍《Windows APT Warfare:惡意程式前線作戰指南》。
6. 課程摘要:

   (1)Office VBA Basic & Binary 結構

   (2)Office 靜態與主動防禦繞過技巧

   (3)Excel Macro 4.0 (XL4), Binary 結構, 與規格後門
7. 學員先修技能:C++、VB、C#
8. 學員自備工具:筆電、Windows 10、Office(2016 版本以上)。

(三) 實戰執行程式與系統漏洞挖掘_馬聖豪(ShengHao Ma, aka aaaddress1)

1. 課程類型:OS Security / Windows Security / Reverse Engineering / Reversing / hellcoding
2. 課程日期:110 年 11 月 20 日(六)~ 110 年 11 月 21 日(日),共二天。
3. 課程總時數 12 小時
4. 課程介紹:

   本課程講者以自身逆向工程十年的經驗累積而成,其中結合了編譯器原理、作業系統與逆向工程實務三者混著介紹。將帶領學員由淺入深,從編譯器如何遵照可執行檔案格式(PE)產生出執行檔、系統如何解析執行檔、到將其裝載為 Process 真正執行起來的完整流程。除了介紹扎實的作業系統實現基礎外,並帶以各國網軍(如 CIA、海蓮花、APT41)曾玩轉這些基礎的惡意利用手段,使讀者能一窺網軍如何操作這些奇技淫巧來打擊防毒軟體。課程內容以動手實務的形式盤點近年實用網軍技術:包含 PE 結構完整操作攻擊/繞過手段解析、Windows Shellcode、程式感染、與防毒繞過、系統服務 逆向工程與繞過,無論是網軍、逆向工程愛好者甚至威脅研究員都能以紅隊視角打下對 PE 格式扎實的基礎!
5. 講師介紹:同上「Office 漏洞魚叉開發實務」之講師。
6. 課程摘要:
   (1)文件映射、蠕蟲感染 與 Process Hollowing
   (2)動態運行 PEB/PE 攀爬 & Shellcode 開發實務
   (3)PE2Shellcode(Stager)、CIA 雅典娜計畫 & 加殼設計
   (4)數位簽名規格 Authenticode & 簽名偽造實務
   (5)符號管理、路徑協議 與 NTFS 弱點利用
   (6)UAC 服務逆向工程 & 提權漏洞挖掘
   (7)WOW64 設計 & 天堂之門繞過防毒
7. 學員先修技能:C++、x86、Python、Windows
8. 學員自備工具:筆電、Windows 10、Visual Studio、Python。

(四) 物聯網攻防實戰_鄭仲倫(Mars Cheng)

1. 課程類型:IoT Security
2. 課程日期:110 年 12 月 3 日(五)~ 110 年 12 月 5 日(日),共三天。
3. 課程總時數 18 小時。
4. 課程介紹:

現今的物聯網市場發展快速，製造商以相當快速的週期推出各項產品，小如網路攝影機、路由器、智慧家庭、醫療設備及汽車等，大到智慧城市、智慧工廠等。其應用已成為人們生活中不可缺少的一部分，相對其資安威脅也日益增長。本課程也因應最新的物聯網生態系推出第二版的內容，第二版將涵蓋物聯網與工業控制系統概念與架構、攻擊向量、基礎的 ARM Exploitation、更深入的韌體分析實戰手法及無線射頻相關的攻擊手法，幫助我們以攻擊者的角度思考該如何對其進行防護，一探 IoT/ICS 安全的世界。本課程提供數十個的實作練習，非常適合想要被手把手教學的學員們報名。

5. 講師介紹:鄭仲倫(Mars Cheng)

目前於 TXOne Networks 擔任資安威脅研究員,專注於 ICS / SCADA、IoT 及企業網絡安全的相關資安議題研究;加入 TXOne 之前,曾在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。

(1)至今提交了 10 多個 CVE 編號,並且在三本 SCI 期刊中(JCR Ranking Top 20 %)發表與應用密碼學相關之論文。

(2)國際資安會議演講經歷:Black Hat、DEFCON、HITB、HITCON、SecTor、SINCON, ICS Cyber Security Conference Asia and USA、VXCON、CLOUDSEC 及 InfoSec Taiwan 等。

(3)資安教育活動經驗:曾於國防部、教育部、經濟部、AIS3、民間上市櫃企業均有授課與顧問經驗,目前亦擔任台灣駭客年會 HITCON 2021 的總召集人,也曾為 HITCON 2020 的副總召集人。

6. 課程摘要:

(1)何謂物聯網(IoT)?

(2)OWASP IoT Top 10 2018 剖析

(3)物聯網攻擊向量剖析

(4)體驗物聯網-MQTT 通訊協定模擬

a. IoT 資訊搜集(Lab)

b. MQTT 與物聯網(Lab)

(5)ARM Exploitation (10+ Lab)

a. Basic ARM Exploitation

b. Exploit Mitigation Techniques

c. Bypass Mitigation

(6)物聯網韌體分析與實作

a. 物聯網韌體分析流程

b. 物聯網韌體靜態與動態模擬分析及漏洞挖掘

(7)物聯網惡意程式分析與殭屍網路實作

a. 分析與編譯物聯網惡意程式(Lab)

b. 建置物聯網殭屍網路(Lab)

(8)車聯網通訊分析與實作

a. 建置車聯網模擬環境(Lab)

b. 車聯網攻擊實作(Lab)

(9)無線射頻滲透測試剖析 (Lab)

(10)物聯網安全防護策略

7. 學員先修技能:具備基本 Linux 指令操作能力

8. 學員自備工具:筆電、VMware Workstation、VMware Fusion (請勿使用 M1 Mac),課程預計提供 2 套 VM(ova)、硬碟空間需求 60G 以上,記憶體 8G 以上。

※結業式當天亦將邀請國際資安競賽 Pwn2Own 得獎團隊戴夫寇爾(DEVCORE)執行長翁浩正進行心得分享及經驗交流

報名網址：https://reurl.cc/aN184G