Course Information

CSIE 7016 Computer Security, Fall 2019

https://edu-ctf.csie.org

課程資訊

課名：計算機安全 Computer Security

時間：9:30-12:10, Fridays 234
(配合各校上課時程，開始時間可能會調整，會再公布)

地點：R204 + 線上直播

課程網站：https://edu-ctf.csie.org

- Allowed IPs: 140.{112, 113, 114, 115, 118, 122}.0.0/16

討論區：https://tlk.io/edu-ctf-2019

Email: ctf@csie.ntu.edu.tw

Today’s Agenda

課程目標與大綱
講師介紹和聯絡方式
Ethics of hacking
成績計算方式（台大only）
加簽原則&處理加簽（台大only）
Basic Tools介紹

課程目標

透過**實務**操作，學習資訊安全的核心概念與技術

提供**合法**的學習和互動平台，給對實務攻防技術有興趣的同學

課程特色

課程內容以實務攻防為主
課堂練習+大量的作業
還要參加課餘競賽 (CTF or bug bounty)
沒有期中考，但有期末競賽

課程特色

跨校連線教學
講師來自臺大、交大、台科大
還有業界邀請演講
黃金陣容!

建議具備以下條件再選修

資安基礎知識

- 如修過密碼學、資訊安全
- 如參加過暑期資安課程、講習

程式與系統基礎知識

- 如修過計算機程式
- 如摸過UNIX / LINUX

這學期時間很多很多

課程大綱（暫定）

Wk.	Date	Topic	Note
1	Sep 13	中秋節放假	
2	Sep 20	Introduction & Basic Tools	
3	Sep 27	Reverse Engineering	
4	Oct 04	Reverse Engineering	Balsn CTF
5	Oct 11	國慶補假	HITCON CTF
6	Oct 18	Web Security	金盾獎競賽
7	Oct 25	Web Security	
8	Nov 1	期中考溫書假	
9	Nov 8	Binary Exploitation	期中考週

課程大綱（暫定）

Wk.	Date	Topic	Note
10	Nov 15	Web Security	台大校慶
11	Nov 22	Binary Exploitation	
12	Nov 29	Binary Exploitation	
13	Dec 06	Binary Exploitation	
14	Dec 13	Cryptography	
15	Dec 20	Cryptography	
16	Dec 27	Cryptography	
17	Jan 03	Guest Lecture	
18	Jan 10	Final CTF Competition	

Final CTF competition: 01/10 (9am) – 01/12 (5pm)

Make sure you can participate!

Teaching Team

台大	交大	台科大	外掛支援
蕭旭君	黃俊穎	鄭欣明	黃詩凱
張元	陳廷宇	馬聖豪	莊秉睿
鄧逸軒	陳憶賢		
楊安傑	林思辰		
趙偉捷	尤理衡		

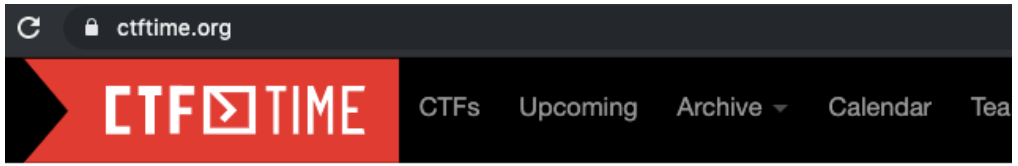
Email: ctf@csie.ntu.edu.tw

線上討論區：https://tlk.io/edu-ctf-2019

Office Hours: Please email to schedule an appointment

Teaching Team

Teaching Team



Team rating

2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

Place	Team	Country	Rating
1	Balsn		847.047
2	Dragon Sector		785.223
3	TokyoWesterns		738.337
4	Plaid Parliament of Pwning		714.125
5	Tea Deliverers		670.862
6	dcua		645.227
7	p4		638.825
8	r3kapig		638.141
9	Bushwhackers		615.464
10	LC↯BC		598.572

Ethics of Hacking


本課程目的在提升同學對資安產業之認識及資安實務能力。所有課程學習內容不得從事非法攻擊或違法行為，以免受到法律制裁。提醒同學不要以身試險。

刑法第36章妨害電腦使用罪

第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條	製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

超級駭客蘇柏榕再犯！盜百萬個資

xC

http://www.tvbs.com.tw/index/

更新日期:2007/09/22 15:18

國內爆發治安史上最嚴重的駭客事件，包括中華電信、無名小站">無名小站以及BBS網站，都遭駭客入侵，3百多萬名會員資料被竊取，而嫌犯就是超級駭客蘇柏榕，他曾在就讀建中期間，入侵總統府及大考中心網站，聲名大噪。現在疑似遭黑幫利用，竊取資料販售牟利。讓他的父母很心痛，說家裡沒有這個人。

蘇柏榕父親：「沒有這個人（蘇柏榕）啦！」記者：「您是蘇爸爸嗎？」蘇柏榕父親：「不是啦。」
轉過頭，不認蘇柏榕就是自己的兒子，蘇爸爸態度冷漠，或許是太過心痛失望。因為國內爆發治安史上，最嚴重的駭客事件，包括中華電話、無名小站以及知名BBS網站，有多達3百多萬名的會員資料，都遭到駭客入侵竊取。

刑法§358+§359

< APT目標攻擊 >冒用健保局名義,攻擊中小企業案,使用惡名昭彰的Ghost遠端存取木馬

POSTED ON 2013 年 07 月 02 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

作者：Maharlito Aquino（威脅研究員）

從逮捕勒索軟體集團的首腦之一，到成功打下Rove Digital(請參考:趨勢科技協助 FBI 破獲史上最大殭屍網路始末)，我們可以時常地看到執法單位和安全廠商間的合作行動，並且有著豐碩的成果。這一次，台灣刑事單位和趨勢科技合作偵破駭客假冒健保局,盜取萬筆中小企業個資案件，解決利用知名的Ghost遠端存取木馬家族所進行的APT-進階持續性滲透攻擊 (Advanced Persistent Threat, APT)目標攻擊。執法單位也逮捕了一名對象。

駭客假冒健保局寄帶有惡意程式的email
刑法 § 359+ § 360

演唱會門票「秒殺」竟是黃牛集團電腦程式搶票

電腦程式搶票流程圖。（記者姚岳宏翻攝）

2017-01-16 15:05

拓元售票網黃牛票案
刑法§360+§362

科技公司董事長及員工扮駭客，入侵高鐵售票系統修改票價自行升等

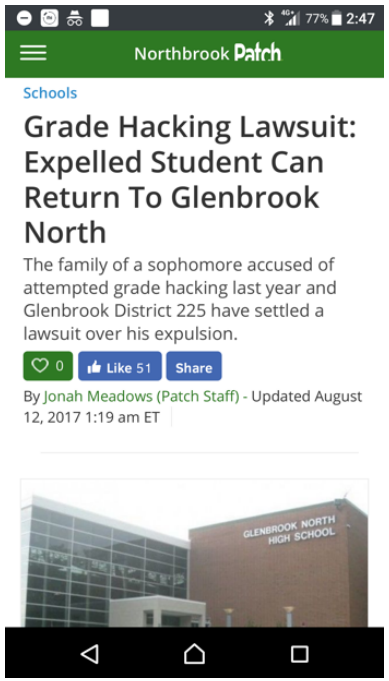
janus 發表於 2015年8月19日 17:05 | 收藏此文

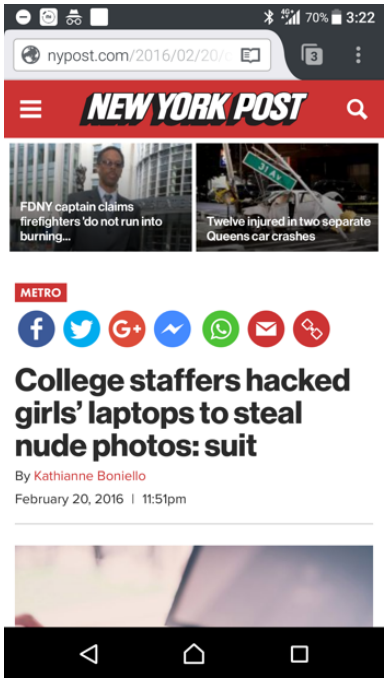
G+1 20 讚 1,497

高鐵公司在今年四月發現，網路購票系統從今年三月底開始，出現了九筆異常的交易狀況。經過鐵路警察局以及刑事局偵九隊調查發現，確認高鐵網站遭到駭客入侵付款系統，駭客竄改了票價的交易金額。而經過三個月的調查，刑事局昨天將駭入高鐵的兩名駭客逮捕。

Even More Lawsuit Cases

改成績　偷照片　搶銀行　駭手機





Respect for Law is the minimum requirement

Principle	Application
Respect for Persons	Participation as a research subject is voluntary, and follows from informed consent; Treat individuals as autonomous agents and respect their right to determine their own best interests; Respect individuals who are not targets of research yet are impacted; Individuals with diminished autonomy, who are incapable of deciding for themselves, are entitled to protection.
Beneficence	Do not harm; Maximize probable benefits and minimize probable harms; Systematically assess both risk of harm and benefit.
Justice	Each person deserves equal consideration in how to be treated, and the benefits of research should be fairly distributed according to individual need, effort, societal contribution, and merit; Selection of subjects should be fair, and burdens should be allocated equitably across impacted subjects.
Respect for Law and Public Interest	*Engage in legal due diligence; Be transparent in methods and results; Be accountable for actions.*

Source: Dr. Shehar Bano

Respect for person

In the name of *good will* and *science*…?

- Hack in vulnerable devices and patch them?
- Hijack spam botnets for research purposes?
- Infiltrate the administration team of an underground market to study sales of illegal drug and weapon?

IF You Must Hack Something …

Consider BUG BONTY PROGRAMS

https://www.bugcrowd.com/bug-bounty-list/

Ethics of Hacking

任何實務的操作練習皆應獲得明確的許可

修習這門課不構成任意存取別人的系統或資料的藉口

最重要的是要保護好自己，不要觸犯法律

任何未經允許的攻擊行為（包括針對教學團隊），除了學期成績為F，還可能有法律刑責

以下**評分方式**與**加簽原則**
只適用於台大修課的同學

Grading Components

Homework assignments (65%)

Final CTF competition (25%)

Other CTF or bug bounty participation (10%)

Other bonus

- 課堂表現
- 課餘競賽表現優異
- 上台報告分享
- ...

如有困難請儘早跟老師和助教聯絡

Final grade: criteria

百分數		等第	定義	等第績分
90-100	95	A+	All goals achieved beyond expectation 所有目標皆達成且超越期望	4.3
85-89	87	A	All goals achieved 所有目標皆達成	4.0
80-84	82	A-	All goals achieved, but need some polish 所有目標皆達成，但需一些精進	3.7
77-79	78	B+	Some goals well achieved 達成部分目標，且品質佳	3.3
73-76	75	B	Some goals adequately achieved 達成部分目標，但品質普通	3.0
70-72	70	B-	Some goals achieved with minor flaws 達成部分目標，但有些缺失	2.7
67-69	68	C+	Minimum goals achieved 達成最低目標	2.3
63-66	65	C	Minimum goals achieved with minor flaws 達成最低目標，但有些缺失	2.0
60-62	60	C-	Minimum goals achieved with major flaws 達成最低目標但有重大缺失	1.7
≦ 59	50	F	No goals achieved 所有目標皆未達成	0
0	0	X	Not graded due to unexcused absences or other reasons 因故不核予成績	0

Failing grade for grad students

Failing grade for undergrads

Warning: final grade is non-negotiable

http://www.oia.ntu.edu.tw/upload/files/20150616223619.pdf

Grading Component 1: Homework Assignments

CTF（capture the flag）形式

每週講師都會出作業

要在CEIBA上繳交code和writeup

作業不能遲交

鼓勵同學討論和合力找資料，但作業要獨力完成

必要時助教和老師會請同學當面解釋作業

Grading Component 1: Homework Assignments

課堂練習也是作業的一部份

雖然有許多週是同步視訊連線，但鼓勵同學還是來204電腦教室一起上課，因為：

- 可以和其他同學討論
- 課程影片不一定會公布
- 會有課堂練習，隨時可以問在現場的助教

Grading Component 2: Final CTF Competition

CTF = Capture the Flag

Attack & Defense or Jeopardy

預計為期三天: 1/10-1/12

分組人數等確定總修課人數後決定

Grading Component 3:
Other CTF or Bug Bounty Participation

在學期結束前參加至少一次資安競賽

- CTF類
- 金盾獎
- HITCON CTF Qual
- (You can find plenty of them on CTFtime)

Bug bounty類

評分方式：寫參賽心得和題目解析

Bonus: 有得獎或獲得獎金，斟酌加分

Bug Bounty （賞金獵人）

List of bug bounty programs

- https://hackerone.com
- https://www.bugcrowd.com/bug-bounty-list/

抄襲行為: zero tolerance

作業抄襲(就算只有一次)：學期成績為F
考試作弊：學期成績為F
複製貼上別人的flag、分享flag也是抄襲

加簽原則

根據HW0的成績來決定加簽的順序
人數上限依教室容量而定

開放實體/線上旁聽，但不要佔到有選到課同學的座位

Homework 0x00 (上星期五已公告)

目的：透過HW0讓同學評估是否要修這門課，也作為加簽依據

今天加簽上的同學，請於**9/27前**在CEIBA上繳交HW0的code和說明，作為評量的依據之一

＊＊＊作業只會越來越難，請審慎評估是否要修這門課＊＊＊

請欲加簽的同學登入課程網站，出示帳號和HW0的分數

加簽完先不要離開，下節課助教會介紹這門課推薦使用的工具

Basic Tools介紹 (by張元)

Questions?