Course Overview and Tool Installation

黃俊穎 (Chun-Ying Huang)
<chuang@cs.nctu.edu.tw>

交通大學 資訊工程學系

1

Ethical Statement

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。

2

3

Case Study: Yahoo!

On March 15, 2017, US DOJ accuses Russia of hacking Yahoo!

The attackers …

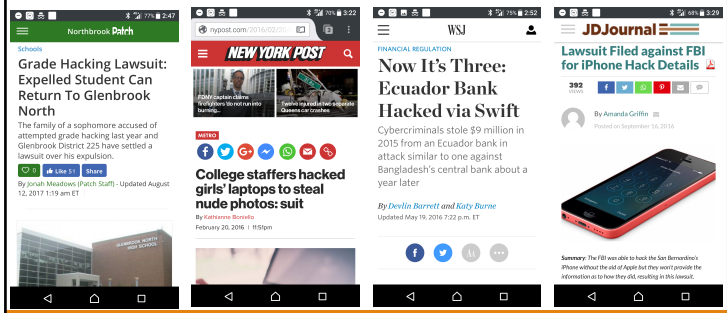
- Stole more then 500M accounts in 2013/2014
- Accessed to stolen accounts in 2015/2016

Source: https://yahoo.tumblr.com/post/158438180334/russian-hackers-and-government-officers-indicted

4

Even More Lawsuit Cases

改成績 偷照片 搶銀行 駭手機



5

IF You Must Hack Something …

Consider BUG BONTY PROGRAMS

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

6

Course Overview

August 28 – September 3

7

Topics

APT

Binary

IoT

Mobile

Network

Web

8

Invited Speakers


Nikolay Akatyev


KG Kim


Quan Heng Lim
林泉亨


Chris Liu


Aaron Luo


Sean Wu


Orange Tsai
蔡政達


Angelboy
楊安傑


Anderson Ni
倪萬昇


Edwin Lu
盧勝榮


Dr. CSC


羅孟彥


許振銘

9

Course Overview (Taipei)

Taipei	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
	8/28/2017	8/29/2017	8/30/2017	8/31/2017	9/1/2017	9/2/2017	9/3/2017
9:30-10:00	Opening	IoT and Car	SSRF -	BLE	Real-life	Mobile	Final CTF
10:00-10:30	課程簡介	Security	從入門到放棄	協定安全	Examples of	Forensics	
10:30-11:00	道德宣導				Web Vul.		
11:00-11:30	工具安裝	Aaron Luo	Orange Tsai	Prof. SC Cha		Nikolay	
11:30-12:00		(TrendMicro)	(DEVCORE)	(NTUST)	QH Lim	Akatyev	
12:00-12:30					(Horangi)	(BoB)	
12:30-14:00	Break	Break	Break	Break	Break	Break	Break
14:00-14:30	Basic	Modern	Binary	IoT Security:	Security in	Web Security	Final CTF
14:30-15:00	Skill	Android	Exploitation	From Cloud to	Real world:	& Hacking	
15:00-15:30	Training	Rooting		Edge	Defending	Hands-on	
15:30-16:00			Angelboy		Web Apps	Practice	
16:00-16:30		Sean Wu	(中研院)	Anderson Ni			
16:30-17:00		(Team T5)		Edwin Lu	Chris Liu	KG Kim	
				(台達電子)	(Rakuten)	(BoB)	
17:00-							Closing

10

Course Overview (Taichung)

Taipei	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
	8/28/2017	8/29/2017	8/30/2017	8/31/2017	9/1/2017	9/2/2017	9/3/2017
9:30-10:00	Opening	BLE	IoT Security:	Real-life	Mobile	SSRF -	Final CTF
10:00-10:30	課程簡介	協定安全	From Cloud to	Examples of	Forensics	從入門到放棄	
10:30-11:00	道德宣導		Edge	Web Vul.			
11:00-11:30	工具安裝	Prof. SC Cha			Nikolay	Orange Tsai	
11:30-12:00		(NTUST)	Anderson Ni	QH Lim	Akatyev	(DEVCORE)	
12:00-12:30			Edwin Lu	(Horangi)	(BoB)		
			(台達電子)				
12:30-14:00	Break	Break	Break	Break	Break	Break	Break
14:00-14:30	Basic	網路攻擊鏈實務	Modern	IoT and Car	Web Security	Binary	Final CTF
14:30-15:00	Skill		Android	Security	& Hacking	Exploitation	
15:00-15:30	Training	許振銘教授	Rooting		Hands-on		
15:30-16:00		(健行科大)		Aaron Luo	Practice	Angelboy	
16:00-16:30			Sean Wu	(TrendMicro)		(中研院)	
16:30-17:00			(Team T5)		KG Kim		
					(BoB)		
17:00-							Closing

11

Course Overview (Tainan)

Taipei	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
	8/28/2017	8/29/2017	8/30/2017	8/31/2017	9/1/2017	9/2/2017	9/3/2017
9:30-10:00	Opening	IoT Security:	Real-life	Mobile	SSRF -	BLE	Final CTF
10:00-10:30	課程簡介	From Cloud to	Examples of	Forensics	從入門到放棄	協定安全	
10:30-11:00	道德宣導	Edge	Web Vul.				
11:00-11:30	工具安裝			Nikolay	Orange Tsai	Prof. SC Cha	
11:30-12:00		Anderson Ni	QH Lim	Akatyev	(DEVCORE)	(NTUST)	
12:00-12:30		Edwin Lu	(Horangi)	(BoB)			
		(台達電子)					
12:30-14:00	Break	Break	Break	Break	Break	Break	Break
14:00-14:30	Basic	分散式阻斷攻擊	IoT and Car	Web Security	Binary	Modern	Final CTF
14:30-15:00	Skill	的滲透、攻擊與	Security	& Hacking	Exploitation	Android	
15:00-15:30	Training	防禦		Hands-on		Rooting	
15:30-16:00			Aaron Luo	Practice	Angelboy		
16:00-16:30		羅孟彥教授	(TrendMicro)		(中研院)	Sean Wu	
16:30-17:00		(高雄應用科大)		KG Kim		(Team T5)	
				(BoB)			
17:00-							Closing

12

AIS3 Final CTF

AIS3 2017 FINAL CTF將以「隊」為單位進行比賽。

每一隊的學員為三位。組隊方式之後說明。

參與AIS3 2017 FINAL CTF且成績表現優異的同學，經審查及推薦後，未來將有機會接受教育部補助出國參加或觀摩國際資安競賽。

無法完成分組登記的學員，或落單的學員，請儘速連絡當地活動主辦單位以協助辦理登記。

13

AIS3 Final CTF 組隊方式說明

shad0w1yc

14

重點

組隊及上傳功能開放時間:
8/28 9:30 - 8/30 12:30

不可跨區組隊

一旦組隊成功，就無法再更換隊員、更改隊伍名稱，個人隊伍代碼也會失效，在功能關閉前都還可以更新隊伍頭貼

唯有找齊三個人才能組隊，功能關閉後沒有隊伍的人會被隨機配對，並會在 1~2 小時後更新到系統上

常見問題

如果沒有上傳頭貼會怎樣？

- 不會怎麼樣，我們有準備預設圖片給所有沒上傳的隊伍

被隨機配對後可以上傳圖片嗎？

- 為了後續作業所以不開放，如果你有希望用的頭貼，請努力的找尋隊友吧！

此功能只有正式學員可以用，助教、旁聽生該怎麼辦？

助教、旁聽生組隊？

我們會幫其他想參加的人建立帳號，9/3當天請找北區和南區的工作人員登記。

中區旁聽教室因為技術和場地的限制，無法開放給旁聽教室參賽。

其他問題？

在聊天室 @shad0w1yc 找我、實體gank、或寄信 service@ais3.org

22

其他注意事項

~~座位表~~

午餐

無線網路

- AIS3 / AIS3-2G
- 請看名牌後面說明

AIS3共筆/聊天室

23

共筆 & 聊天室

共筆：
https://paper.dropbox.com/doc/AIS3-2017-1RuujJKI3sVe4tRh4dP7c

聊天室：
https://tlk.io/aisss2017

24

List of Tools – Summary

Name	Name
Android Studio, SDK, and NDK	JCE (Java Cryptography Extension)
Android Backup Extractor	Kali Linux
APKtool	objdump
Bee-Box / bWApp	OpenSSL binary
Burp Proxy (free)	OWASP Broken Web Applications VM
Command line	pwntool
GDB and GDB/PEDA	VMware player or workstation
Jadx (dex-to-java compiler)	Virtualbox
Java SDK	Wireshark

25

Course File Server (in LAN)

http://file.ais3.org/

26

Course File Server (Cont'd)

27

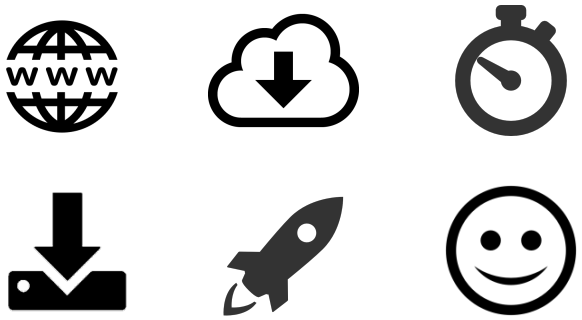
Additional Tools

Windows VM
- IF you are working with a Linux system or Mac OS X
  -- or --
- IF you do not want to analyze malware in your daily working Windows OS

IDA Pro
- Eh … We don't have licenses
- Maybe you can try IDA evaluation
- https://www.hex-rays.com/products/ida/support/download_demo.shtml

28

Standard Installation Steps



29

Some More Notes …

Ensure that you are familiar with (any) VM environment
- Network setup
- Import images to your VM, e.g., bee-box VM image

Command lines

Working with GIT

Leverage package management system

objdump

OpenSSL binary

Wireshark

30

Virtual Machines

Courses that require virtual machines

Consider installing a Linux for yourself!!!
- Ubuntu
- Kali
- Bee-Box / bWApp

31

Virtual Machines

Free choices: VMware Player and VirtualBox

VMware Player: Play with VMs created by VMware Workstation
- Free version only available on Windows and Linux (!?)

VirtualBox: Full featured virtual machines (create, export, import, run)

You may need both – depends on the VM image from the instructors!!

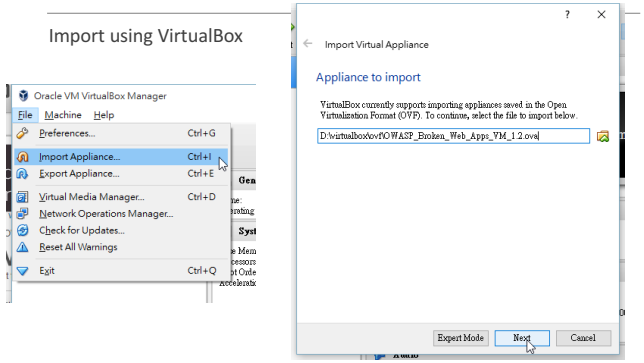
VMware: .vmx files

Open format: .ova and .ovf files

32

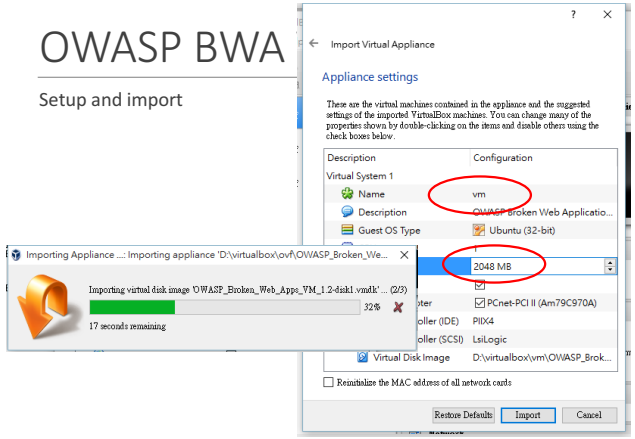
OWASP BWA VM

Import using VirtualBox



OWASP BWA

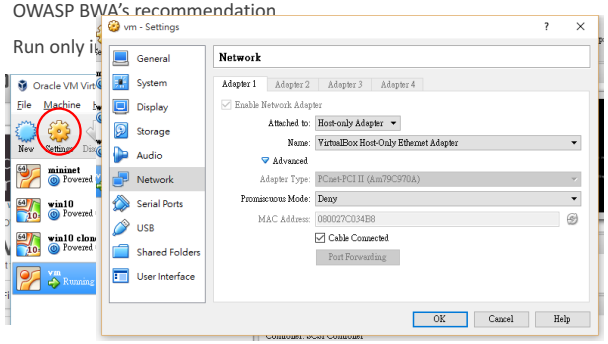
Setup and import



OWASP BWA VM – Networking

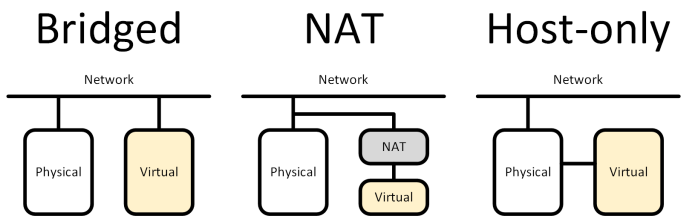
OWASP BWA's recommendation

Run only i



More on VM Networking

An illustration for VirtualBox networking



More on VM Networking (Cont'd)

Read VirtualBox manual …

https://www.virtualbox.org/manual/ch06.html

	VM ↔ Host	VM1 ↔ VM2	VM → Internet	VM ← Internet
Host-only	+	+	–	–
Internal	–	+	–	–
Bridged	+	+	+	+
NAT	–	–	+	Port forwarding
NAT Network	–	+	+	Port forwarding

37

Notes from One Speaker: Quan Heng Lim (1/3)

On host machine,
Install: Vmware player
Download: bee-box(bWAPP)
Download: Kali Linux
Ensure bridged mode works for both, and machines can ping each other

Update instructions for Kali:
Install: python, pycharm if GUI is prefered
Perform apt-get update, apt-get upgrade

Update instructions for bee-box:
With bee-box, ensure that you have it set up in bridged mode. (Or the same as your kali machine)
Click Update bWAPP, it doesn't work, edit /home/bee/Documents/Scripts/WAPP_update_script.sh

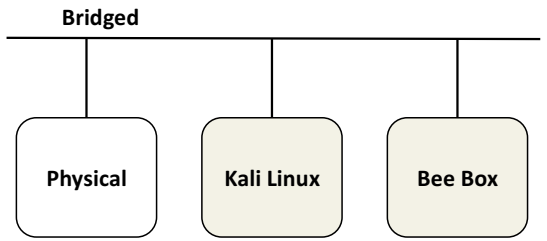
wget --no-check-certificate "http://downloads.sourceforge.net/project/bwapp/bWAPP/bWAPP_latest.zip

Click install bWAPP and click on the generated link.

Also, check keyboard input settings are correct, (Probably US keyboard) and delete all others

38

Notes from One Speaker: Quan Heng Lim (2/3)



39

Notes from One Speaker: Quan Heng Lim (3/3)

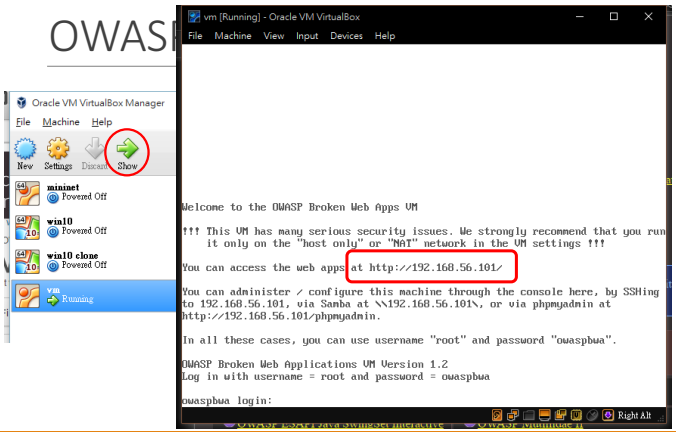
For Buffer Overflow:
Vulnerable app (https://github.com/stephenbradshaw/vulnserver) has been tested on windows 10, however, would recommand to download a windows VM from window's internet explorer or developer's program (90 day trial).

https://developer.microsoft.com/en-us/windows/downloads/virtual-machines

Immunity Debugger
Download immunity debugger with mona.py

40

OWASP



41

OWASP BWA VM – Web UI

42

Create a New Virtual Machine

You will need an OS installation ISO image

Choose your target operating system

Setup virtual CPU, RAM, HDD, …

- More number of CPUs is better
- Larger RAM is better

Try it by yourself!!

43

Command Lines

Windows

- You may have to install CYGWIN, or you may work with a Linux VM

Linux

- You already have the built-in shell
- IF you are working with Ubuntu desktop, try gnome-terminal

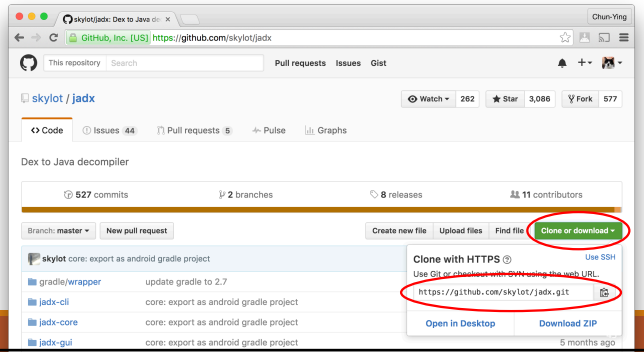
Mac OS X

- You already have the built-in shell
- Application -> Utility -> Terminal

44

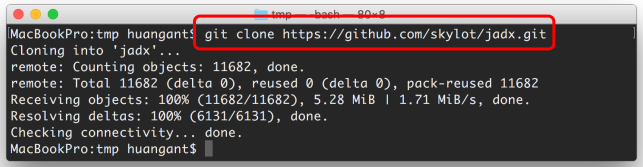
Working with GIT

For example: jadx @ https://github.com/skylot/jadx



Working with GIT (Cont'd)

```
git clone {url}
```



46

Leverage Package Management System

Windows
- Eh ... Work with installers
- CYGWIN software: run the CYGWIN setup program

Linux
- Depends on your Linux distribution …
- Redhat/Fedora based: yum
- Debian/Ubuntu based: apt-get

Mac OS X
- homebrew, fink, macports, ...
- You will need Xcode (installed from AppStore)
- My favorite one is homebrew: http://brew.sh/

47

objdump

Part of GNU assembler, linker and binary utilities (binutils)

Install a Linux VM and you will have it!

Windows: CYGWIN has the package – Install from the installer

Ubuntu Linux – You must be able to ***sudo***

```
$ sudo apt-get install binutils
```

Mac OS X
- By default Mac OS X has **otool** – similar to objdump, but for Mach-O only
- You may install binutils, and then work with **gobjdump**

```
$ brew install binutils
```

48

OpenSSL Binary

Website:
https://www.openssl.org/

Windows:
CYGWIN has the package

Ubuntu Linux

$ sudo apt-get install openssl

Mac OS X
- Built-in **openssl** binary (may be outdated)
- You may install your own via your preferred package management system

```
$ /usr/bin/openssl version
OpenSSL 0.9.8zh 14 Jan 2017          # The built-in version
$ brew install openssl               # Install via homebrew
$ /usr/local/Cellar/openssl/1.0.2h_1/bin/openssl version
OpenSSL 1.0.2h  3 May 2017           # That built using homebrew
```


Wireshark

Read this: Platform-Specific information about capture privileges

https://wiki.wireshark.org/CaptureSetup/CapturePrivileges

Key point
- Packet capture requires putting a NIC into **promiscuous mode**
- Usually it requires super user permission to do that

Windows: The installer should have done everything for you

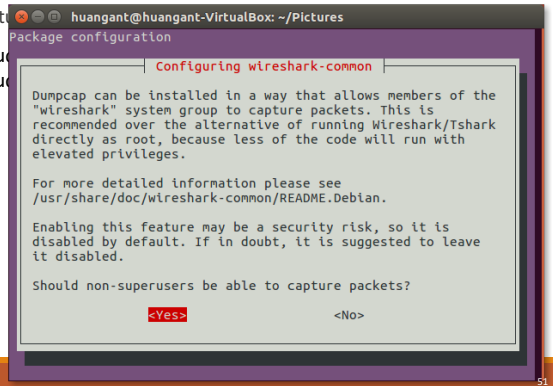
Linux: You may need root privileges or special setups for non-root users

Mac OS X: The latest version does not require X11 nor permission setup
- Otherwise, try "`chmod 777 /dev/bpf*`"

Wireshark for Non-Root Users (Linux)

Ubunt

$ su
$ su



Q & A

問卷調查

53

第二屆 台灣好厲駭 培訓 徵選活動

報名日期::
即日起**至 9 月 8 日(五)下午 5 點截止**

報名方式::請參閱

趕快用手機照

https://isip.moe.edu.tw/?page_id=368

報名網址：https://goo.gl/**2Z6d6C**

服務熱線::

教育部資安人才培育計畫推動辦公室專任助理
陳小姐
0928-155-602 happyhacking2017@gmail.com

網址

報名方式

報名網址