OT # Day 2 - CTF Related Issues

LL ## Making a security alarm for fun and profit - 李倫銓 (Alan Lee)

- 課程投影片: goo.gl/w3r5uu
- Lab 步驟 及 需要的檔案 / 工具: https://github.com/mcsworld/AIS3
- 有興趣的在課程後可以跟老師要晶片來玩

王 Director Traversal Cheat Sheet

- https://pentestlab.wordpress.com/2012/06/

ZL
- Correlation
  - 動手做後面的東西
  - 被打進來的時候會叫
- .htpasswd ==> John the Ripper

CF
- Damn Vulnerable Web Application

C
- MS event id https://support.microsoft.com/en-us/kb/977519 or **http://ppt.cc/rZbEE**

TC
- Windows event log
  - event id 登入成功的代碼 4624

黃 coolterm :http://freeware.the-meiers.org/
options -> port選擇對應的com ,baudrate 設定115200

DH Ubuntu(Linux) -> sudo screen /dev/ttyUSB0 115200

王 MAC -> Terminal 執行 ls /dev/tty.usbserial*，應該可以找到對應的 tty name
-> screen /dev/tty. usbserial[對應的tty name] 115200

HP https://github.com/mcsworld/AIS3/blob/master/Lab/README.md
https://github.com/mcsworld/AIS3/tree/master/API

AL ## The development of CTFs - Tyler Nighswander

ZL 投影片: http://copyfighter.org/ais3/slides/

HP
About

J Tyler 大神

JC 神人物理+計算機科學雙主修，博士研究量子計算

BC 玩了 6 年的CTF (2009 ~ present)

HP

AL
What is a CTF?

HP
- Capture the Flag
  - Jeopardy Style
    - 參賽者打官方主機
J
    - more relaxed
    - variety of challenges
AL
    - more teams(1000+)
HP
  - Attack-Defense style
    - 互相攻擊對方主機取得旗幟
    - fewer teams(30~60)
紀
    - Connecting to AP...
J
    - shorter contests
AL
- Game Format
HP
  - 8 hours - 72+ hours, normally 24hr
林
  - 3-50 problems
HP
  - Usually online, sometimes in person
A
- Categories
  - Cryptography
  - Forensics
  - Binary explotation
紀
  - Web exploitation
林
  - Reverse engineering
J
  - Trivia
A
  - Programming
林
  - Social engineering
林
  - Incident respon
HP
- Why You Should Play CTF!
  - You won't get the experience anywhere else!
A
  - Fastest way to learn computer security
HP
  - It's a lot of fun!
A
  - Make friends in security/CTF community
AL
  - travel to competitions
A
  - Competition for every skill level
  - Taiwan has excellent TEAMS!

Shorter answer is : If you like security, play CTFs!

HP
CTFs vs ...

- CTF vs puzzle hunts
  - CTF skills will help ypu in the real world!
- CTF vs "defensive" competitions
  - CTFs are more fun
H - CTFs have objective scoring
HP - CTFs vs "real security"
  - CTFs are competitive
  - CTFs are (relatively) short and easy

If you run your own CTF competition, keep all of these in mind!

- Before going futher....
  - Downloadable VM with tools!
  - Assumes Linux knowledge...
  - http://copyfighter.org/ais3/ctf

History

- Kriegspiel - 1811
Z - Dice-based war simulation game
AL - enigma - 1930s
  - computers + crypto decisive in war
- Phreaking - 1967
J - Precursor to hacker movement
- Computer viruses/exploits
A - First CTF held at DEFCON 4 in 1996
    - Format is a mystery ...
    - Held every year since
  - UCSB iCTF first held in 2001
  - First Pwn2Own in 2007
  - Old stype contest .... problems list to time ...
AL - forensics + reversing + exploitation + trivia
J - Practice Site: http://copyfighter.org/ais3/ctf

A - Trends
  - Crypto in CTF is roughly in-tune with real world!
CF - differential analysis
    - length extension attack
ZL - power analysis
    - padding oracle { 2010 ASP.NET, 2011 Codegate }

CF
- Duel EC DRBG

AWEIMEOW 感謝大大 <(_ _)>

A
- Many crypto attack months after real world exploit with ..
- CTF getting harder
  - 10 years ago: BOFs with no ALSR nor NX
  - today: ASLR, NX, RELRO, PIE, 1 Byte overwrites
  - to get started, look at **OLD CHALLENGES** !
- CTF are just about ahead of the curve for exploits
- Full PIE + pointer xor + mor in 2012

- Trends Overview
  - Some categories follow trends closely
    - Unlikely that CTF will beat academics in crypto
    - CTFs will likely remain hot on their heels
  - Some categories seems ahead of trends
    - Exploitation and sometimes web can lead real world

黃
- Both influenced by tools and are ....

A
- Trends Lessons
  - Read security news, it will show up in CTFs
  - Follow academics + blogs + tools about security
  - When bug hunting, remember recent trends.

H
- Lessons for real world
  - Practice hard exploitation with CTFs
  - Tools/techniques for CTFs can be used for speed
  - Trends can help your bug hunting real life too!

A
- CTF Recent History
  - Until 2007, CTFs were 'just a games'
  - First pwn2own in 2007
    - almost a CTF, prize is $10k USD
  - Codegate 2008
    - Only Korea
    - USD 100K prize

黃
- 2009 - international

A
- CTFs are not just games!
- Can easily win: money, glory, jobs
- CTFs will get more valuable, also more competitive

ZL FreeBSD 0day and root'ed everyone
- Wiereshark 0day

    - Defcon 20 - DoS's in four separate dissectors: CIP CTDB, XTP, Mongo
黃 - CTF skills and Real World skills overlaps!
    - CTF is an easier place to start
    - CTF are a safe ,legal place to practice hacking
D   - Tricks with scripting and tool will speed up dev time
黃   - Experience can help get jobs in security industry

ZL ## Why tools

- Get rid out of the boring things and do something interesting { do this buffer overflow all the time }
- "Grunt work" can get boring
- "Force multiplier"
D - Stop rewriting the same scripts
ZL - Save you many many hours
- Solve challenges FASTER

Automation in the "Real World"

黃 - This is a huge problem
H - Finite number of skilled computer security researchers
黃 - (nearly) infinte amount of computer....

H ## Tools to discuss

- misc
- IDA
- binary ninja
- GDB/PEDA
- pwntools
ZL - Qira
H - Pin
- Z3
ZL - angr - with a symbolic execution
- afl - cool fuzzer
H - write your own!!

- misc
    - Random tools can automate many tasks!
A   - meta-goal: kill stupid CTF problems

ZL moar history

- 2010 year of the blind SQLi challenges

- writing blind SQLi solver with binary search - not fun
  - writing it in less than 10 minutes -- even less fun
- SQLMap !
  - automated
  - interest over time goes up
- Today blind SQLi is much less common
- This is good: focus on creative gaskss, not menial ones
- Lesson: if you see a task 10 times, automate it
- Also: if you think a challenge is "dumb", automate it

Reverse Engineering and Malware Analysis - Erye Hernandez

- Lecture Structure
  - Day1: Intro to Malware Analysis
  - Day2: Static Analysis
  - Day3: Dynamic Analysis
- Tool
  - http://copyfighter.org/ais3/malware/

- What is malware ?
  - **mal**icious soft**ware**
  - deliverately designed to disrupt computer
- History of Malware
  - 1950s: Von Neumann's approaches to self-reproducting automata
  - 1970s: Creeper and Reaper, Rabbit, Pervading Animal Hunter
  - 1980s: Elk Cloner, Brain, Virden, Morris Worm, CERT
  - 1990s: self-mutating engine, Michelangelo, virus creation kits, selling malware in the underground, BackOrifice
  - 2000s: iLOVEYOU, Pikachu, SQL Slammer, MyDoom, Sony BMG scandal
  - 2010s: Stuxnet, Zeus, Gameover Zeus, CryptoLocker

- Threat Actors
  - Insider threats / Maliciours insider
    - current or former employee, contractor, etc
    - misuse of access
    - goal: revenge or $$$
  - Hacktivists
    - protest or promote political agenda
    - not well resourced

AL
- Cybercriminalist
  - 王 utilize infosetealers and ransomware
  - goal: $$$
- A State-sponsored threat groups
  - lots of resources
  - goal: Militaries, ...

- Types of Malware
  - Worm, Backdoor, Infostealer, Ransomare
  - Downloader, Keylogger, RootKits, Launcher
  - Botnets, POS, ATM, Mobile
- Malware vs CTF Binanries
  - AL different goals when analyzing
  - analysis requires similar skills
- A malware vs CTF (malware / CTF)
  - AL respond to network intrusion / find flag
  - figure out what binary does / what a binary does
  - find a way to detect and contain / find flag
- A Methods of Analysis
  - Basic Triage
    - 'assign degrees of urgency' - Webster's Dictionary
    - is it malicious ?
    - understand
  - Dynamic
    - observing the executables be
    - AL using a debugger to examine ...
  - A Static
    - examining binary without viewing actual instructions(file, exiftools ,...)
      - AL reverse engineering via disassembler
- A Lab Environment
  - 禹黃 Physical
    - resource intensive
  - Virtual
    - does not require physical hardware
    - easy to revert back to snapshots
  - Automated
    - A CucKoo Sandbox (http://cuckoosandbox.org/)
    - Anubis (https://anubis.iseclab.org/)

YNYCHEN *講者表示 virustotal不錯，但是沒有偵測到不代表沒毒xD*

C
Environmental Setting

(Hard Disk storage <= 2Gb)

楊鎮銘 *是RAM還是HardDisk?*

Network Configuration

Windows

IP: 10.1.1.2
Mask: 255.255.255.0
Gateway: 10.1.1.1
DNS: 10.1.1.1

Linux

IP: 10.1.1.1
Mask: 255.255.255.0
Gateway: None

Windows VM 的網路設成內部網路(internal network) (原本預設是NAT)

ZHEMIN L *export VISUAL=/usr/bin/vim*

sudo vim /etc/inetsim/inetsim.conf

password：aisss

vim tips:
/regular\sexpres{2}ion ?here
[n] for next occurrence

service_bind_address 192.168.1.1->10.1.1.1
/dns_default_ip 192.168.1.1->10.1.1.1
/dns_default_domainname h4x0r.com
:wq

Take a Snapshot
After all setting

Basic Triage

- Goals

Hashes

- Use MD5 or SHA1

- file identification
  - Search online
  - share with other researchers

C Strings

- ASCII and Unicode format
- Provide clues to the functionality of the binary
- IPs, URLs, functions, error messages, etc

PEiD

- Identifies common packers, crypters, compilers
- Outdated butstill useful

Dependency Walker

- Bundled with MS development tools
- Provides hierarchical view of funcitons and odules
- Show only dynamically linked

D PEView

- Displays PE header and sections
- Image_File_Header
- contains compile time
- Image_Section_Header
- contains size on disk and in memory

CFF Explorer

- PE editor

Resource Hacker

- Dispalys the .rsrc section of the file
- View, modify and delete resource

Dynamic Tools

Process Explorer

- Sysinternals suite
- Similar to Windows Task Manager
- Displays currently active processec(parent and child)
- Shows open handles and loaded DLLS

Process Monitor

- Sysinternals suite
- Real-time file system, registry, process.thread activity

Wireshark

- Open source network protocol analyzer

FakeNet

- Network simulator
- Supports DNS,HTTP, SSL, SMTP

INetSim

- Internet services simulation
- Easy to customize and confiure

Lab

Lab1-0.exe

- What is its hash?
- When was the binary compiled?
- What can you tell about the binary?
- What does it do?
- What are some of the functions that the binary imports?

Lab1-1.exe

- What is its hash?
- When was the binry compiled?
- What can you tell about the binary?
- What are some of the functions that the binary imports?

AIS3.exe

- What is its hash?
- When was the binary compiled?
- What can you tell about the binary?
- What does it do?

王 map_setip.exe.zip

- pwd: infected

王 • run as admin

-> md5hash, strings , virtual tools

Ans:

- Lab0-1.exe: cpoy & google its hash , and you will find it is nc
- Lab1-1.exe: Strings, SysinternalSuite - Procmon