第一堂課：
Introduction

講師：sherry
時間：10/06(五) 12:00~14:30
地點：資訊處 215教室
備註：請自備電量充足的筆電

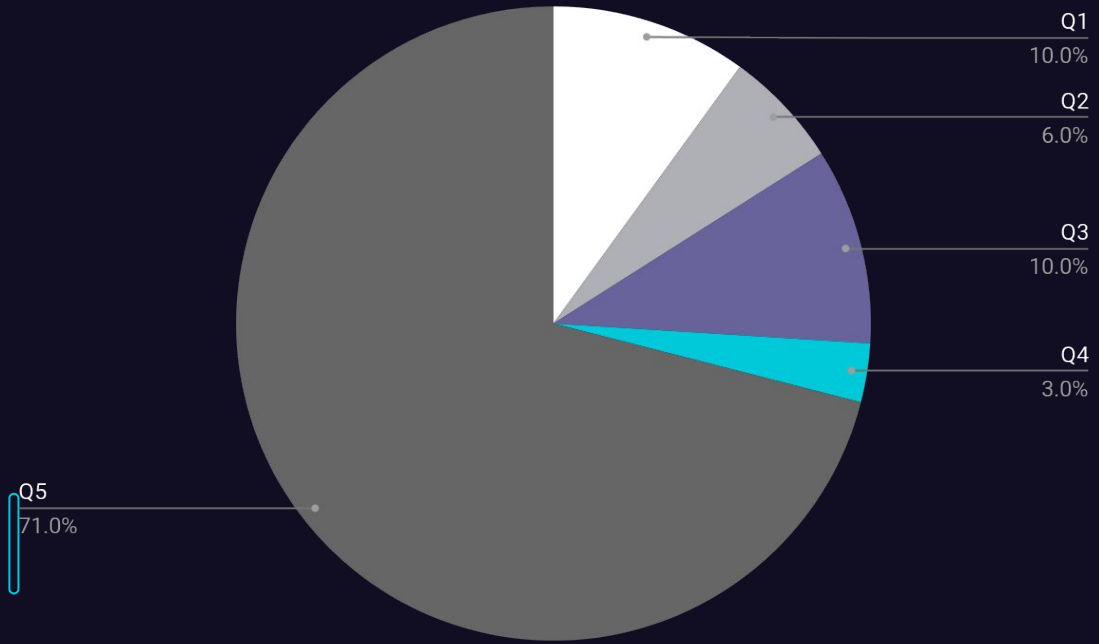
TABLE OF CONTENTS

點名

00

INTRODUCTION 01

TA 分數占比



Q1
Mid Exam(10%)

Q2
Lab Participate(6%)

Q3
Final Exam(10%)

Q4
picoCTF Grade(3%)

INTRODUCTION

Lab participate (6%)

開頭使用 ecourse2 點名+課程實作中選擇一題作為簽到題
→ 題目來源多為 picoCTF 題目，網路上有眾多資訊、詳解可供參考，不用緊張
→ 兩者當天都完成即可獲得 課堂參與*1

請假(僅1次)

如果真的需要請假，可在下次上課前將簡報上的題目都做完，→ 做完同樣可獲得 課堂參與*1

INTRODUCTION

期中／期末(10% / 10%)

使用 CTFd 考試 + 考試後繳交 Write UP

picoCTF 分數(3%)

鼓勵同學自主學習
期末結算 → 1/3-3分、1/3-2分、1/3-1分

INTRODUCTION

1n

Date	Description
11/10	期中考

助教課時間確認！

安裝作業
+ CTFd 註冊

02

虛擬機安裝教學

Click,please

CTFd website

帳號請使用你們的學號
密碼沒有限制(但不要使用太私人的密碼)
Flag Format : CCU_MIS{[\w@]+}

picoCTF

Flag Format : picoCTF{\w+}

What is CTF?

03

CTF

CTF是一種資訊安全競賽，透過參賽者解決各種任務，以奪取 Flag

所以Flag到底是什麼？為什麼要奪取 Flag?

Flag 通常會是文字，但是不限定
其實是模擬現實的漏洞的形式

CTF 類型

- Web
- Crypto
- Reverse
- Pwnable
- Misc

以 picoCTF 來說...

- Web
- Crypto
- Reverse
- Forensics
- General
- Binary

Linux Command 04

> command usage

用法：$ command [OPTION]

範例：ls -al

apt

套件管理器

- 用法
  - 安裝
    - apt install <package>
  - 移除
    - apt remove <package>

su

切換到root身分

sudo

以高權限執行指令

- 用法 : sudo command

ls

列出資料夾下的檔案

- 用法 : ls <dir>
- 選項
  - -a
    - 列出隱藏檔案
  - -l
    - 列出檔案的詳細資訊

cd

切換當前資料夾

. / : 當前資料夾

~ : 家目錄(/home/<USER>)

cd .. : 切換回上一個資料夾

- 用法
  - cd <dir>

mkdir

建立資料夾

- 用法 : mkdir <dir>

rmdir

刪除空的資料夾

- 用法 : rmdir <dir>

clear

清空當前 Terminal 上的所有文字(不刪除紀錄)

類似的功能為`history -c`(會刪除紀錄)

wget

下載檔案

- 用法 : wget < url >
  - 選項
    - -O　想取的檔案名稱

cat

顯示檔案內容

- 用法 : cat <file>

Lab

touch

建立檔案

- 用法 : touch <file>

rm

刪除檔案

- 用法 : rm <file>
- 選項
    - -r　遞迴刪除(刪除資料夾下的所有內容)
    - -f　強制刪除(危險!)

mv

移動檔案

- 用法 : mv <file> path_route

cp

複製檔案

- 用法 : cp <file> path_route

u :

chmod

更改檔案的權限

- u : 針對使用者
- 用法 chmod +權限名稱 filename
- 權限
  - r : 可讀
    - chmod +r <file>
  - w : 可被寫入
    - chmod +w <file>
  - x : 可執行
    - chmod +x <file>

不要隨意使用`chmod 777 <file>`

```
:~/CTF$ chmod u+x wave
:~/CTF$ ./wave
 Pass me a -h to learn what I can do!
:~/CTF$ ./wave -h
```

執行檔案

- 用法 ./<file>

```
:~/CTF$ ./wave
 Pass me a -h to learn what I can do!
:~/CTF$ ./wave -h
```

Lab

unzip

解壓縮zip檔案

- 用法 : unzip <file>.zip

tar

打包、解包檔案

各種各樣打包指令整理:

https://project.zhps.tp.edu.tw/ethan/2009/09/compress/

Lab

grep

搜尋關鍵字

- 用法 : grep keyword <file>

- 搭配 pipe = ‘|’
  - ls ./ | grep ‘flag’
    - 列出當前資料夾中，檔名含有“flag”的檔案

Lab

strings

- 用來檢視二進位檔案中可視字元的工具
- 幫助我們從目標檔案、庫或可執行檔案中找出有用的資訊
- 用法：
  - strings <filename>

- 搭配 pipe = '|'
  - strings ./ | grep 'flag'
    - 列出當前資料夾中，檔名含有"flag"的檔案

Lab

Netcat

多功能的好用工具

可用來遠端連線、掃描 port 是否有開啟等

用法：

- nc server port

整理：

nc(1): arbitrary TCP/UDP connections/listens - Linux man page (die.net)

Lab

Lab

ssh

離開：exit

用法：

- ssh 連線 -p <port number>

Lab

THANKS!

中正資安社連結~歡迎想更進一步學習、交流的人掃描加入!