HACK@10

INTRODUCTION TO CAPTURE THE FLAG

UNIVERSITI TENAGA NASIONAL

The Energy University

$ whoami

Name : Ahmad Hizami (@m4j1d)

University : Universiti Tenaga Nasional (UNITEN)

Course : Cyber Security

Experience: 1 - 2 years

What will be covered today?

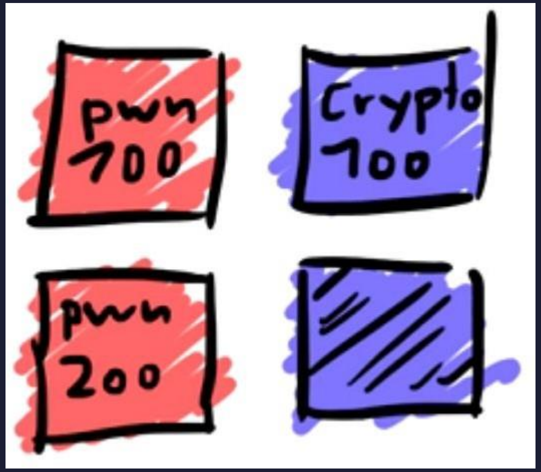
- What is CTF?
- CTF categories
- Challenges Categories
- General tips
- Hack@10 general briefing

Capture the Flag (CTF)

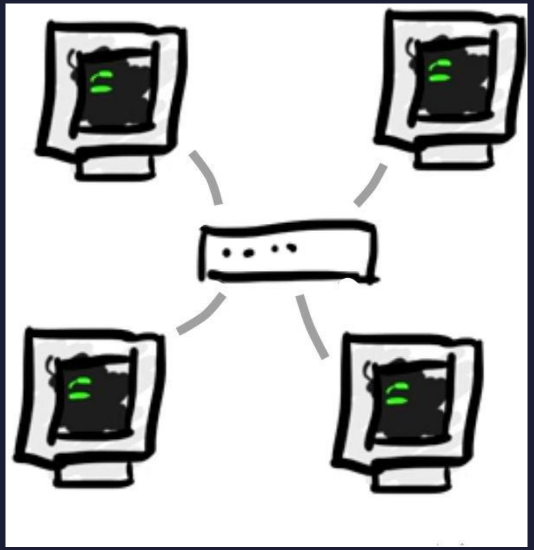
- Nothing to do with shooting games
- computer security competitions
- team based
- end goal = obtaining as many "flag" as possible in limited time
- flag = points/marks
- why join CTF?
  - train you up with cyber security skills
  - not playing in the dark side
  - enjoyment and sharing

CTF Categories

- **Jeopardy**
  - solve multiple questions differs in categories
  - usually question are released periodically (easy->hard)
  - sometimes questions are released based on solved task



- **Attack & Defense**
  - host(PC/VM) running vulnerable daemons & services
  - pwn other teams' box (attack)
  - patch your own box (defense)



Challenge Categories

- cryptography
- steganography
- Networking
- Reverse Engineering
- Web exploitation
- Digital forensic
- Osint
- Miscellaneous

- ideally, you need to master all of them
- but most ctf are group based
- divide jobs between group members
- help to solve faster

Cryptography

Encoding

- transforms data into another format
- using a scheme that is publicly available (no key)
- **ASCII/EBCDIC, base64, hex/binary**

Encryption

- transform data in order to keep it secret
- can only be reversed by knowing the key/algorithm
- **RSA, xor, ciphers (Ceasar/Enigma)**

Hashing

- fixed length string generated based on the input data
- serves the purpose of ensuring integrity
- one way (unless bruteforced)
- **MD5, SHA1, CRC**

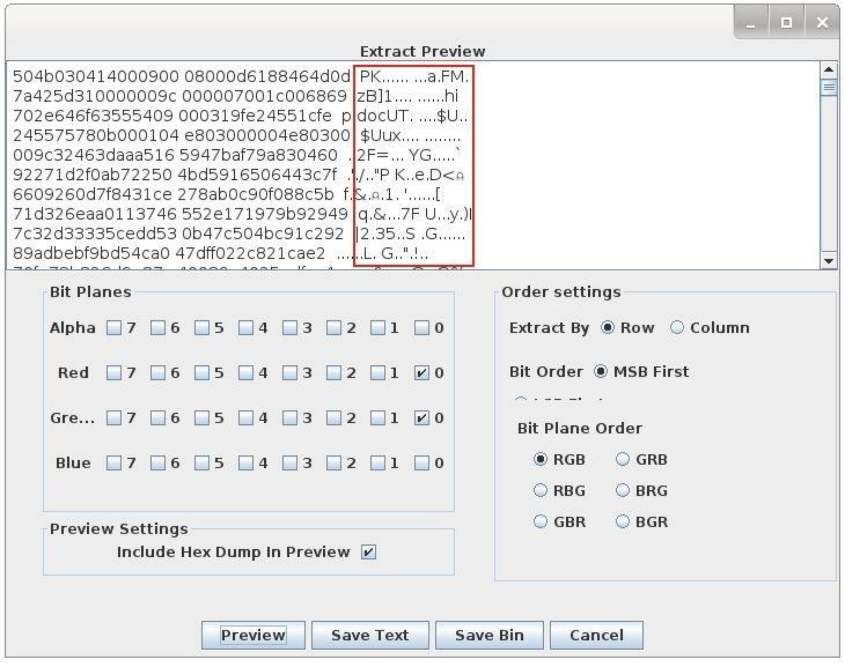
Obfuscation

- make something harder to understand
- obstacle to reverse engineering
- **jsf*ck (javascript), proguard (apk)**

Steganography

the art of concealing information within another data

- **audio**
  - spectrogram
  - filter pass
  - **audacity**
- **others**
  - text stega
  - video frame
  - pdf stream
  - office documents
- **image**
  - lsb insertion
  - color(hex) -> string
  - **stegsolve & etc**



Extract Preview

```
504b030414000900 08000d6188464d0d  PK...... ...a.FM.
7a425d310000009c 000007001c006869  zB]1.... ......hi
702e646f63555409 000319fe24551cfe  p docUT. ....$U..
245575780b000104 e803000004e80300  $Uux.... ........
009c32463daaa516 5947baf79a830460  ..2F=... YG.....`
92271d2f0ab72250 4bd5916506443c7f  .'./.."P K..e.D<
6609260d7f8431ce 278ab0c90f088c5b  f.&...1. '......[
71d326eaa0113746 552e171979b92949  q.&...7F U...y.)I
7c32d33335cedd53 0b47c504bc91c292  |2.35..S .G......
89adbebf9bd54ca0 47dff022c821cae2  ......L. G..".!..
```

Bit Planes

Alpha □7 □6 □5 □4 □3 □2 □1 □0

Red □7 □6 □5 □4 □3 □2 □1 ☑0

Gre... □7 □6 □5 □4 □3 □2 □1 ☑0

Blue □7 □6 □5 □4 □3 □2 □1 □0

Preview Settings

Include Hex Dump In Preview ☑

Order settings

Extract By ● Row ○ Column

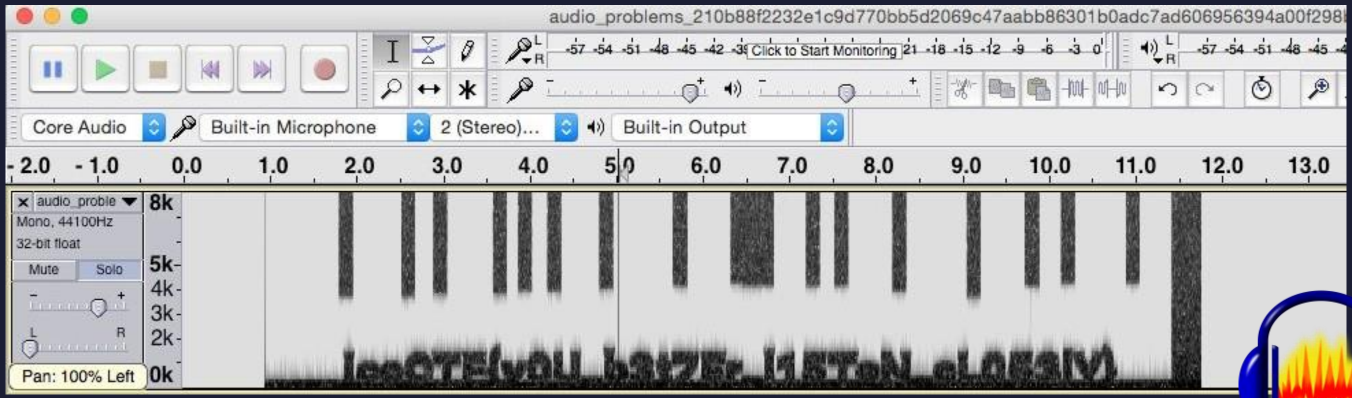
Bit Order ● MSB First

Bit Plane Order

● RGB ○ GRB

○ RBG ○ BRG

○ GBR ○ BGR



audio_problems_210b88f2232e1c9d770bb5d2069c47aabb86301b0adc7ad606956394a00f298

Core Audio | Built-in Microphone | 2 (Stereo)... | Built-in Output

audio_proble

Mono, 44100Hz

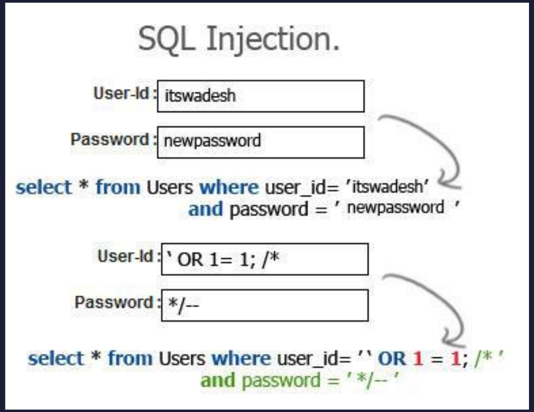
32-bit float

Pan: 100% Left

Web exploitation

- common cause
  - bug in website implementation
  - interpreter bug (php, python, etc)
  - unsanitized user input
  - server misconfiguration

- sql injection
  - inject sql query
  - tool: **sqlmap**
  - bypass waf (manually)



SQL Injection.

User-Id : itswadesh

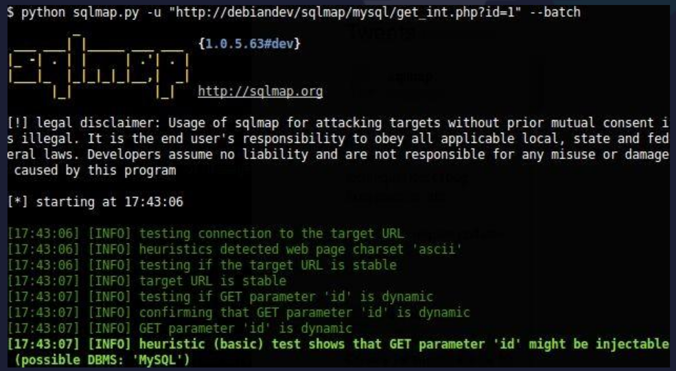
Password : newpassword

select * from Users where user_id= 'itswadesh'
and password = ' newpassword '

User-Id : ' OR 1= 1; /*

Password : */--

select * from Users where user_id= '' OR 1 = 1; /* '
and password = ' */-- '

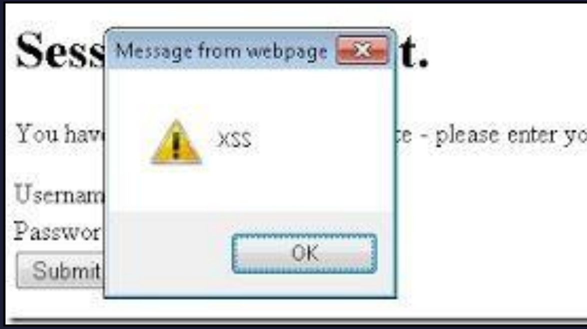


```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
    _
 ___ ___| |_____ ___ ___  {1.0.5.63#dev}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent i
s illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
 caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
 (possible DBMS: 'MySQL')
```

- local file inclusion
  - include webshell
  - view source code

- header manipulation
  - bypass authentication
  - disguise referrer/user-agent
  - tamper cookies
  - tools: **ZAP proxy, chrome devtools**

- others
  - injection
  - xss/csrf
  - web 0days



Sess t.

You hav e - please enter you

Usernam

Passwor

Message from webpage

XSS

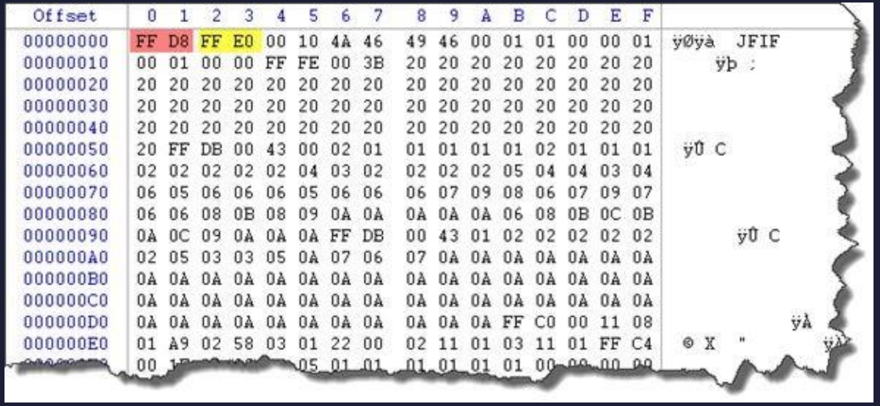
Digital forensic

recovery and investigation of material found in digital devices

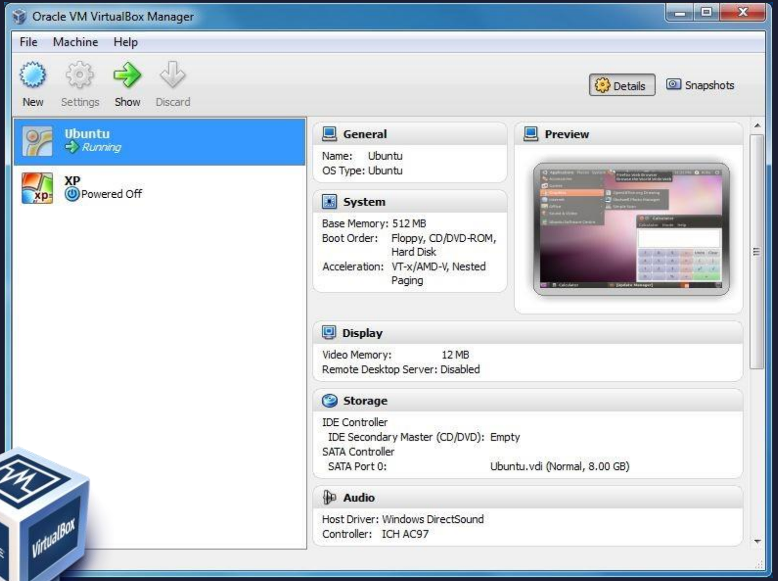
- **extensionless file**
  - magic headers (**hex editor**)
  - www.garykessler.net/library/file_sigs.html
  - **file/binwalk/trickID**

- **data/memory dump**
  - file carving (**scalpel/foremost**)
  - find data (**grep/strings**)
  - **volatility** (memory extraction framework)

- **virtual images**
  - load into virtual machine
  - mount directly (faster)
  - other tools: **encase, ftk**



```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01   ÿØÿà  JFIF
00000010  00 01 00 00 FF FE 00 3B  20 20 20 20 20 20 20 20      ÿþ ;
00000020  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000040  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00000050  20 FF DB 00 43 00 02 01  01 01 01 01 02 01 01 01    ÿÛ C
00000060  02 02 02 02 02 04 03 02  02 02 02 05 04 04 03 04
00000070  06 05 06 06 06 05 06 06  06 07 09 08 06 07 09 07
00000080  06 06 08 0B 08 09 0A 0A  0A 0A 0A 06 08 0B 0C 0B
00000090  0A 0C 09 0A 0A 0A FF DB  00 43 01 02 02 02 02 02        ÿÛ C
000000A0  02 05 03 03 05 0A 07 06  07 0A 0A 0A 0A 0A 0A 0A
000000B0  0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
000000C0  0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A 0A 0A 0A 0A 0A
000000D0  0A 0A 0A 0A 0A 0A 0A 0A  0A 0A 0A FF C0 00 11 08              ÿÀ
000000E0  01 A9 02 58 03 01 22 00  02 11 01 03 11 01 FF C4    © X  "       ÿÄ
          00                05 01 01  01 01 01 01 00 00 00 00
```



Ubuntu
Running

XP
Powered Off

General
Name: Ubuntu
OS Type: Ubuntu

System
Base Memory: 512 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display
Video Memory: 12 MB
Remote Desktop Server: Disabled

Storage
IDE Controller
IDE Secondary Master (CD/DVD): Empty
SATA Controller
SATA Port 0: Ubuntu.vdi (Normal, 8.00 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

General tips

- improve your Google-fu
- learn multiple programming languages
- keep track of recent tech & exploits
- keep practicing & read writeups
  - ctftime.org
  - github.com/ctfs

HACK@10 BRIEFING

- Timing (48 Hours)
  - 24 hours – CTF
    - Start Time: 26 Nov, 10AM
    - End Time: 27 Nov, 10AM
  - 24 hours - Write-Up
    - Submission Open: 27 Nov, 10AM
    - Submission Closed: 28 Nov, 10AM

- Flag Format: *hack10{xxx}*
- Registration Close: 25th November, 11.59PM
- CTF Login Credentials:
  - Each team will be given one login credential
  - will be blasted through email to team leaders on 26th November between 8.00AM - 9.45AM

THANK YOU