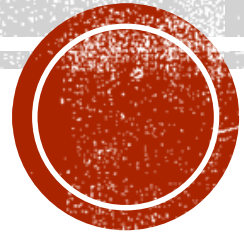
CAPTURE THE FLAG

Thin Ba Shane (Base CTF Myanmar Organization)



ABOUT ME

- Organizer @ Base CTF Myanmar (http://basectf.org/)
- Co-founder @ Creatigon (http://creatigon.com/)
- Admin @ Myanmar Security Forum (http://www.mmsecurity.net/forum/)
- Participant in Cyber Seagame 2015
- Often participant in Cyber Drills

Personal Blog

http://lunam00n.com (LOL Security)

Facebook

https://www.facebook.com/thin.bashane

Twitter

@art0flunam00n

SOME PRACTICE LABS

- Luna File Upload Lab
- https://github.com/LunaM00n/File-Upload-Lab

- Web Obfuscate 101 Lab
- https://github.com/LunaM00n/Web-Obfuscate-Lab

- XVWA (Extreme Vulnerable Web Application) walkthroughs
- https://www.youtube.com/playlist?list=PL62Jkhsty0Fe3LuhFAa-QAmYCcHN1R-BG

WHAT IS CTF?

SCORE BOARD

Rank	Team	Score	First Score	Total Score
1	3Idiots	2900	3	2903
2	Team SSL	2650	10	2660
3	Mdy_L33ts	2650	5	2655
4	h3X	2550	5	2555
5	Root	2100	3	2103
6	Team TUX	1900	4	1904
7	Revolution	1850	2	1852
8	Team_Sylar	1600	1	1601
9	Rpay2	1500	4	1504
10	Team 15	1500	1	1501
11	Surge MNO	1450	2	1452
12	Rango	1350	1	1351
13	NoOb	1100	1	1101
14	Unknown	950	0	950

TOPICS IN CTF

- Web
- Cryptography
- Pwn (Binary Exploitation)
- Steganography
- Network
- Forensics
- Reverse Engineering
- Mobile
- Programming
- Misc.

TODAY TOPICS FOR CTF

- Web
- Cryptography
- Pwn (Binary Exploitation)
- Steganography
- Reverse Engineering
- Mobile

WEB CHALLENGES

- SQL Injection, Cross Site Scripting(XSS), LFI/RFI, Command Execution, Code Injection, etc …
- Web Application Filter Bypass

SQL INJECTION DEMO

```
$input=$_GET['id'];
$query="SELECT username FROM users WHERE id='".$input."'";
```

USER INPUT

- fileame.php?id=<user_input>

WHAT HAPPENED IN SOURCE CODE?

- $query="SELECT username from users WHERE id="".$input."""";

Clear form

SELECT username from users WHERE id='<user_input>'

FUZZING STAGE

- SELECT username from users WHERE id='<user_input>'

- SELECT username from users WHERE id=' 1' or '1'='1 '

Using comment

- SELECT username from users WHERE id=' 1' or 1=1--+ '

WAF BYPASSING DEMO

```php
<?php
        if(isset($_GET['string'])){
            $string=$_GET['string'];
          echo str_replace(" ","",$string);
        }

 ?>
```

NOT ALLOWED WHITE SPACE?

- / (forward slash)
- \t (Tab)
- \n (Line Feed)
- \r (Carriage Return)
- /**/ (Multi lines comment)
- Etc…

HOW TO KNOW THIS?

- Find Bypass methods with googling

```php
<?php
for($i = 0; $i <= 255; $i++) {
    $character = chr($i);
     echo '<div><a'.$character.'href="http://www.google.com/">'.$i.'</a></div>';
}
?>
```

CRYPTO CHALLENGES

- Classic Ciphers, Machine Ciphers, Modern Ciphers, etc…
- PyCrypto (Python Module for Crypto)

ROT13 DEMO (PYCRYPTO)

```
from pycipher import Rot13
print Rot13().encipher('lolsecurity')
print Rot13().decipher('YBYFRPHEVGL')
```

CRYPTO DEMO

- https://www.net-force.nl/challenge/level301/

UGRhIGx3b29za256IGJrbiBwZGEgeWR3aGhhamNhIGx3Y2EgZW86IHludWxwaw==

BASE64 ? HOW TO KNOW THIS?

Base 64 Encoding

- ASCII -> Binary
- Regroup into 6 group quantities
- Convert to Base64 characters

BASE64 CHARACTER TABLE

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

HOW IT WORK?

- Our plain text -> abcde
- Convert into binary ->01100001 01100010 01100011 01100100 01100101
- Regroup into 6 bits ->011000 010110 001001 100011 011001 000110 0101
- 011000 -> 24 (Decimal)
- 24 -> Y (according to Base64 Character Table)
- 0101 -> 010100(filled with 0)
- Base64 maintain 24bit alignment

‘ = ‘ IS NO BINARY REPRESENTATION

- 011000 010110 001001 100011 011001 000110 0101(00)
- Y W J j Z G U =

DECODED BASE64 FOR DEMO

- Pda lwoosknz bkn pda ydwhhajca lwca eo: ynulpk

WHAT THE HELL IS THIS?

- Substitution Cipher (No key)
- Try with classic substitution cipher without key such as ROT13 , Atbash , etc..

Online Cryptogram Solvers

- http://quipqiup.com/index.php

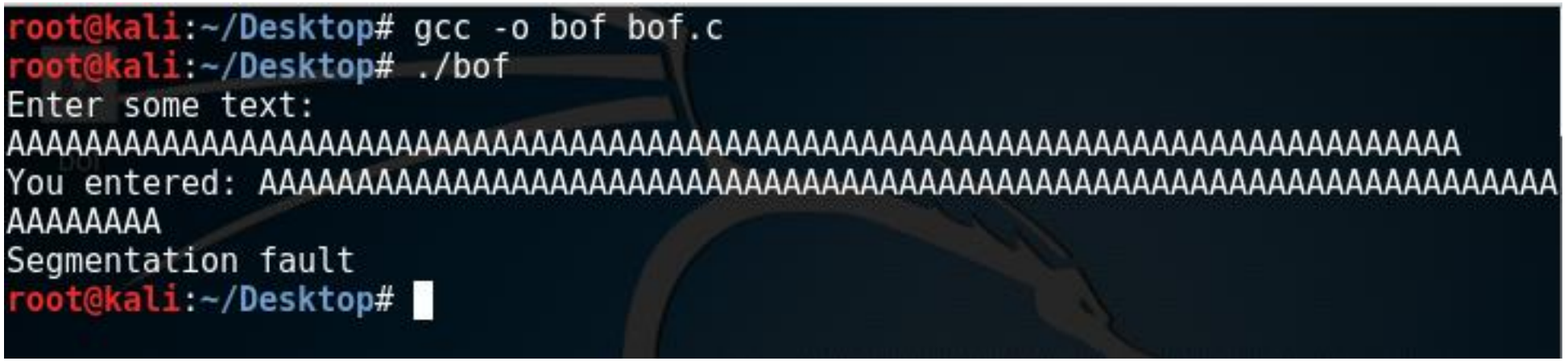
ROTATION CIPHER

- The password for the challenge page is: crypto

PWN CHALLENGES

- Smash the Stack, Heap Overflow, Format String Vulnerability, etc…

SMASH THE STACK DEMO



CALCULATING OFFSET SIZE

```
08048494 <echo>:
 8048494:       55                      push   %ebp
 8048495:       89 e5                   mov    %esp,%ebp
 8048497:       83 ec 28                sub    $0x28,%esp
 804849a:       83 ec 0c                sub    $0xc,%esp
 804849d:       68 bd 85 04 08          push   $0x80485bd
 80484a2:       e8 89 fe ff ff          call   8048330 <puts@plt>
 80484a7:       83 c4 10                add    $0x10,%esp
 80484aa:       83 ec 08                sub    $0x8,%esp
 80484ad:       8d 45 e4                lea    -0x1c(%ebp),%eax
 80484b0:       50                      push   %eax
 80484b1:       68 ce 85 04 08          push   $0x80485ce
 80484b6:       e8 95 fe ff ff          call   8048350 <__isoc99_scanf@plt>
 80484bb:       83 c4 10                add    $0x10,%esp
 80484be:       83 ec 08                sub    $0x8,%esp
 80484c1:       8d 45 e4                lea    -0x1c(%ebp),%eax
 80484c4:       50                      push   %eax
 80484c5:       68 d1 85 04 08          push   $0x80485d1
 80484ca:       e8 51 fe ff ff          call   8048320 <printf@plt>
 80484cf:       83 c4 10                add    $0x10,%esp
 80484d2:       90                      nop
 80484d3:       c9                      leave
 80484d4:       c3                      ret
```

CALCULATING OFFSET SIZE

- 1C (Hexadecimal) => 28 (Decimal)
- 1c =28 bytes
- ebp=4 bytes
- eip=4 bytes

- python print –c ‘print”A”*32+”<controlled_eip>”‘

CONTROLLING EIP

```
0804846b <secretFunction>:
 804846b:       55                      push   %ebp
 804846c:       89 e5                   mov    %esp,%ebp
 804846e:       83 ec 08                sub    $0x8,%esp
 8048471:       83 ec 0c                sub    $0xc,%esp
 8048474:       68 80 85 04 08          push   $0x8048580
 8048479:       e8 b2 fe ff ff          call   8048330 <puts@plt>
 804847e:       83 c4 10                add    $0x10,%esp
 8048481:       83 ec 0c                sub    $0xc,%esp
 8048484:       68 94 85 04 08          push   $0x8048594
 8048489:       e8 a2 fe ff ff          call   8048330 <puts@plt>
 804848e:       83 c4 10                add    $0x10,%esp
 8048491:       90                      nop
 8048492:       c9                      leave
 8048493:       c3                      ret
```

CONTROLLING EIP

STEGANOGRAPHY CHALLENGES

- Hidden File in Images, Hidden File in Audio/Video, Hidden Text , etc…

- File Signatures
- http://www.garykessler.net/library/file_sigs.html

STEGANO DEMO

```
root@kali:~/Desktop# binwalk -e ctfexample.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
40804         0x9F64          Zip archive data, at least v2.0 to extract, compressed si
ze: 32993, uncompressed size: 33783, name: got2.jpg
73941         0x120D5         End of Zip archive
```

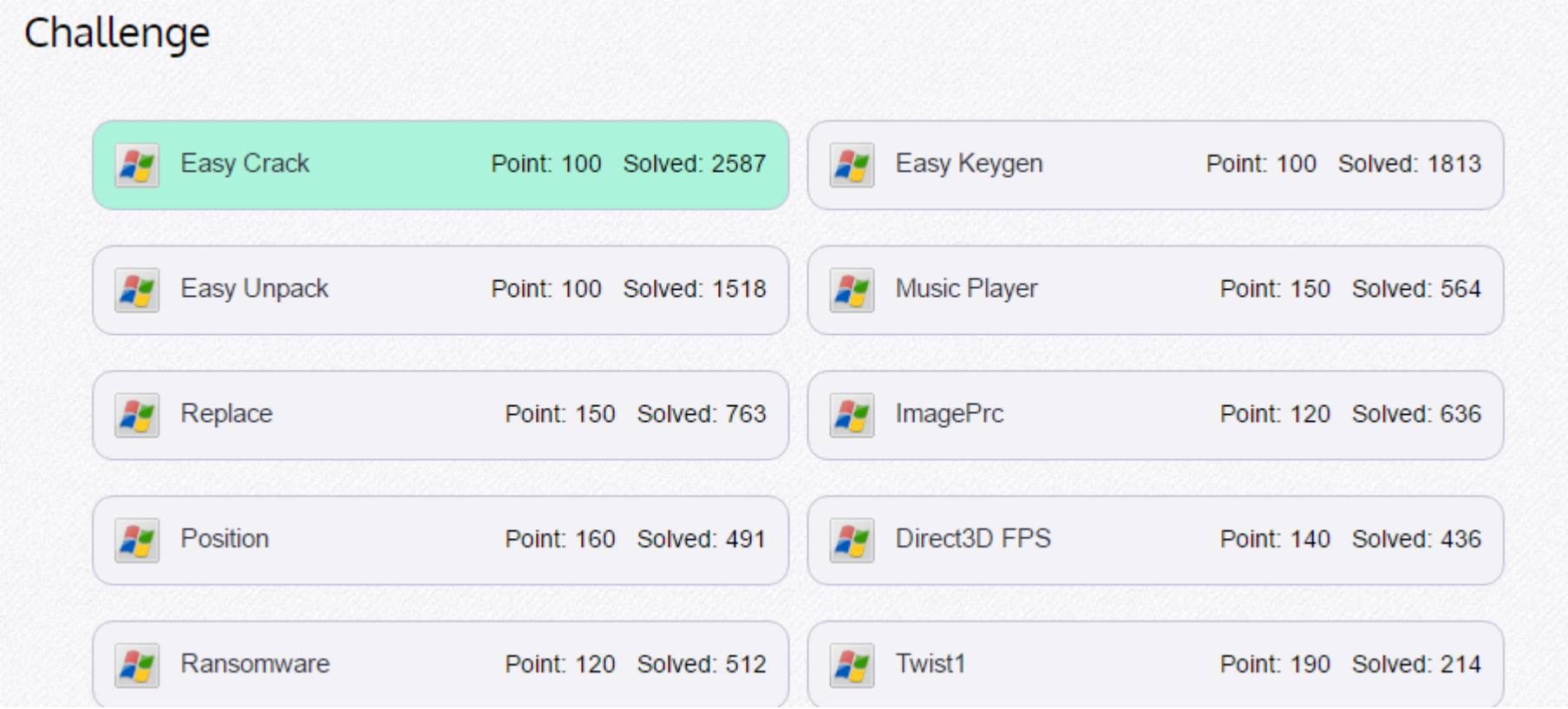
STEGANO DEMO

```
root@kali:~/Desktop# dd if=./ctfexample.jpg of=./ctfexample.zip skip=40804 bs=1
33159+0 records in
33159+0 records out
33159 bytes (33 kB, 32 KiB) copied, 0.114752 s, 289 kB/s
root@kali:~/Desktop#
```

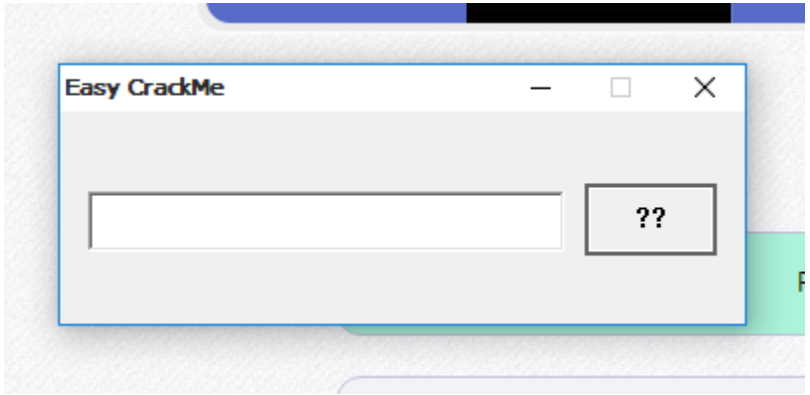
```
root@kali:~/Desktop# unzip ctfexample.zip
Archive:  ctfexample.zip
  inflating: got2.jpg
root@kali:~/Desktop#
```

STEGANO DEMO

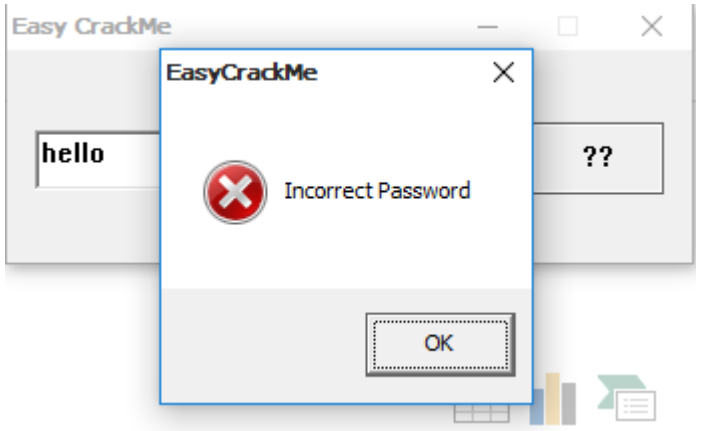
REVERSING DEMO



RUNNING APPLICATION



ERROR



DISASSEMBLING WITH IDA PRO

```
.text:00401000
.text:00401000
.text:00401000 ; int __stdcall WinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance,LPSTR lpCmdLine,int nShowCmd)
.text:00401000 _WinMain@16     proc near               ; CODE XREF: start+C9↓p
.text:00401000
.text:00401000 hInstance       = dword ptr  4
.text:00401000 hPrevInstance   = dword ptr  8
.text:00401000 lpCmdLine       = dword ptr  0Ch
.text:00401000 nShowCmd        = dword ptr  10h
.text:00401000
.text:00401000                 mov     eax, [esp+hInstance]
.text:00401004                 push    0               ; dwInitParam
.text:00401006                 push    offset DialogFunc ; lpDialogFunc
.text:0040100B                 push    0               ; hWndParent
.text:0040100D                 push    65h             ; lpTemplateName
.text:0040100F                 push    eax             ; hInstance
.text:00401010                 call    ds:DialogBoxParamA ; Create a modal dialog box from a
.text:00401010                                         ; dialog box template resource
.text:00401016                 xor     eax, eax
.text:00401018                 retn    10h
.text:00401018 _WinMain@16     endp
.text:00401018
.text:00401018 ; ---------------------------------------------------------------------------
.text:0040101B                 align 10h
```

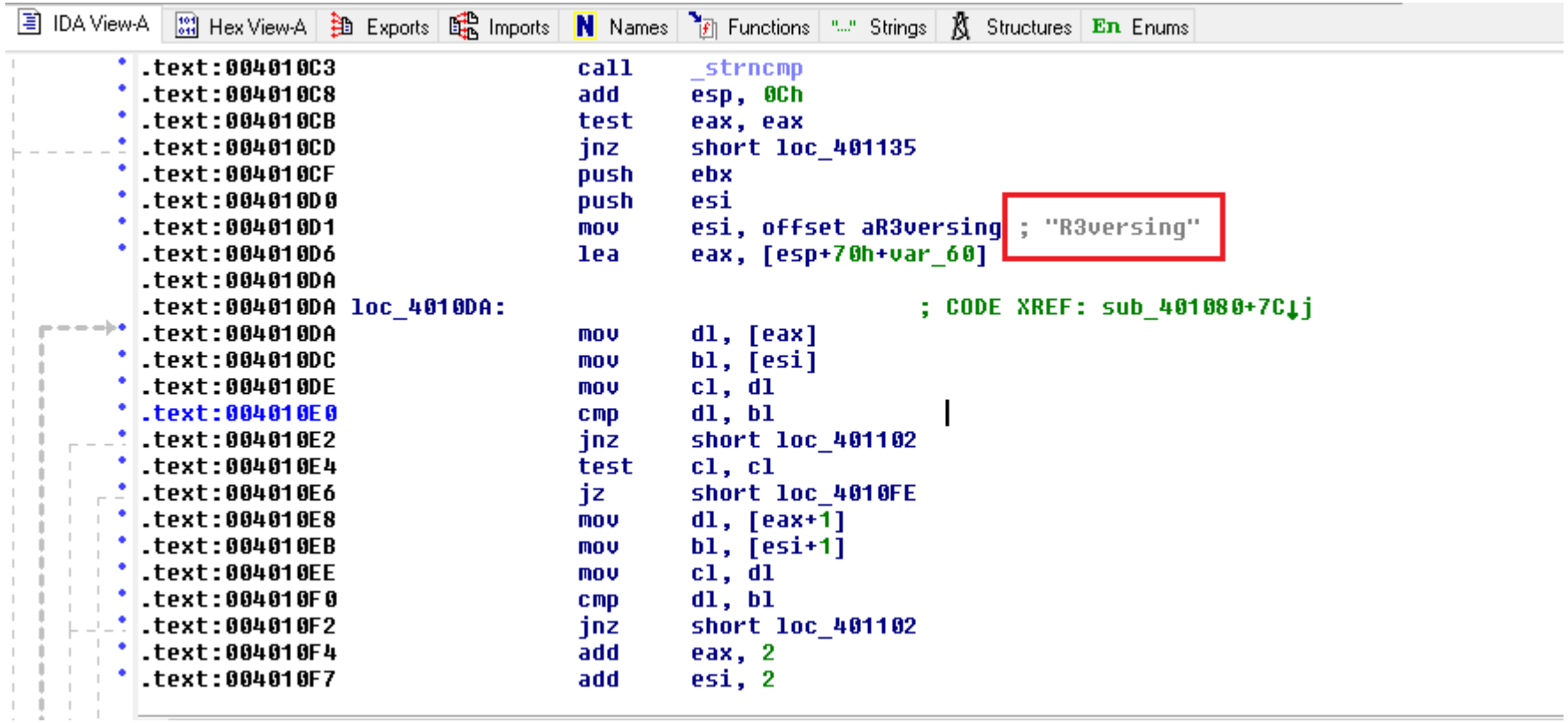
DIALOG BOX

```
.text:0040102F loc_40102F:                             ; CODE XREF: DialogFunc+8↑j
.text:0040102F                 mov     eax, [esp+arg_8]
.text:00401033                 and     eax, 0FFFFh
.text:00401038                 sub     eax, 2
.text:0040103B                 jz      short loc_40105E
.text:0040103D                 sub     eax, 3E7h
.text:00401042                 jz      short loc_401049
.text:00401044                 xor     eax, eax
.text:00401046                 retn    10h
.text:00401049 ; ---------------------------------------------------------------------------
.text:00401049
.text:00401049 loc_401049:                             ; CODE XREF: DialogFunc+22↑j
.text:00401049                 mov     eax, [esp+hDlg]
.text:0040104D                 push    eax             ; hDlg
.text:0040104E                 call    sub_401080
.text:00401053                 add     esp, 4
.text:00401056                 mov     eax, 1
.text:0040105B                 retn    10h
.text:0040105E ; ---------------------------------------------------------------------------
.text:0040105E
.text:0040105E loc_40105E:                             ; CODE XREF: DialogFunc+1B↑j
.text:0040105E                 mov     ecx, [esp+hDlg]
.text:00401062                 push    2               ; nResult
.text:00401064                 push    ecx             ; hDlg
```

CHECK FUNCTION CALL FROM DIALOGBOX

```
.text:00401089                 xor     eax, eax
.text:0040108B                 lea     edi, [esp+5]
.text:0040108F                 mov     [esp+68h+String], 0
.text:00401094                 push    64h             ; nMaxCount
.text:00401096                 rep stosd
.text:00401098                 stosw
.text:0040109A                 stosb
.text:0040109B                 mov     edi, [esp+6Ch+hDlg]
.text:0040109F                 lea     eax, [esp+6Ch+String]
.text:004010A3                 push    eax             ; lpString
.text:004010A4                 push    3E8h            ; nIDDlgItem
.text:004010A9                 push    edi             ; hDlg
.text:004010AA                 call    ds:GetDlgItemTextA
.text:004010B0                 cmp     byte ptr [esp+5], 61h
.text:004010B5                 jnz     short loc_401135
.text:004010B7                 push    2               ; size_t
.text:004010B9                 lea     ecx, [esp+0Ah]
.text:004010BD                 push    offset a5y      ; "5y"
.text:004010C2                 push    ecx             ; char *
.text:004010C3                 call    _strncmp
.text:004010C8                 add     esp, 0Ch
.text:004010CB                 test    eax, eax
.text:004010CD                 jnz     short loc_401135
.text:004010CF                 push    ebx
```

FINDING COMPARISON



FINDING COMPARISON

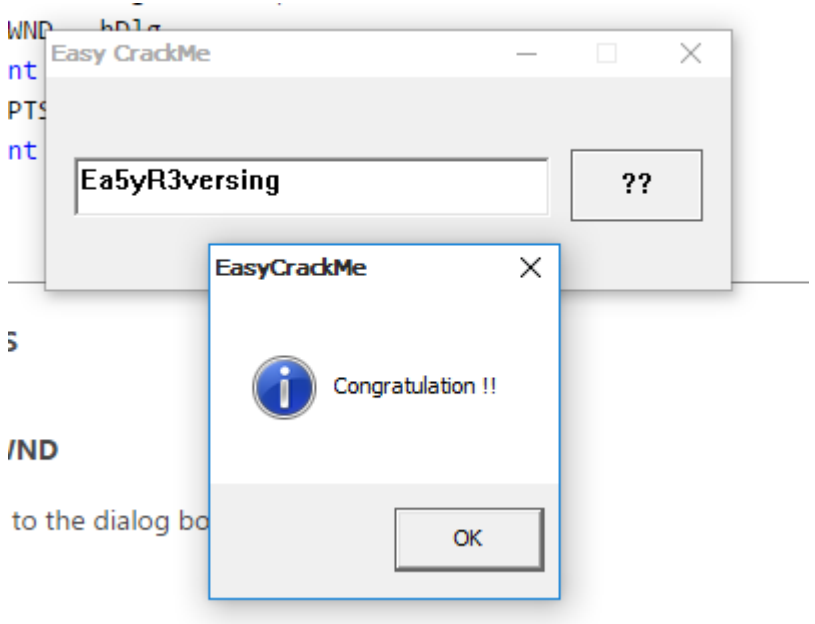
```
.text:004010FE loc_4010FE:                             ; CODE XREF: sub_401080+66↑j
.text:004010FE                 xor     eax, eax
.text:00401100                 jmp     short loc_401107
.text:00401102 ; ---------------------------------------------------------------------------
.text:00401102
.text:00401102 loc_401102:                             ; CODE XREF: sub_401080+62↑j
.text:00401102                                         ; sub_401080+72↑j
.text:00401102                 sbb     eax, eax
.text:00401104                 sbb     eax, 0FFFFFFFFh
.text:00401107
.text:00401107 loc_401107:                             ; CODE XREF: sub_401080+80↑j
.text:00401107                 pop     esi
.text:00401108                 pop     ebx
.text:00401109                 test    eax, eax
.text:0040110B                 jnz     short loc_401135
.text:0040110D                 cmp     [esp+68h+String], 45h
.text:00401112                 jnz     short loc_401135
.text:00401114                 push    40h             ; uType
.text:00401116                 push    offset Caption  ; "EasyCrackMe"
.text:0040111B                 push    offset Text     ; "Congratulation !!"
.text:00401120                 push    edi             ; hWnd
.text:00401121                 call    ds:MessageBoxA
.text:00401127                 push    0               ; nResult
.text:00401129                 push    edi             ; hDlg
```

WHAT WE GOT?

- 61h = 0x61 (hexadecimal) = a (Ascii)
- 45h = 0x45 (hexadecimal) = E (Ascii)
- R3versing (String)
- 5y (String)

- So “Ea5y R3versing” ?

GOTCHA


Easy CrackMe
Ea5yR3versing
??
EasyCrackMe
Congratulation !!
OK

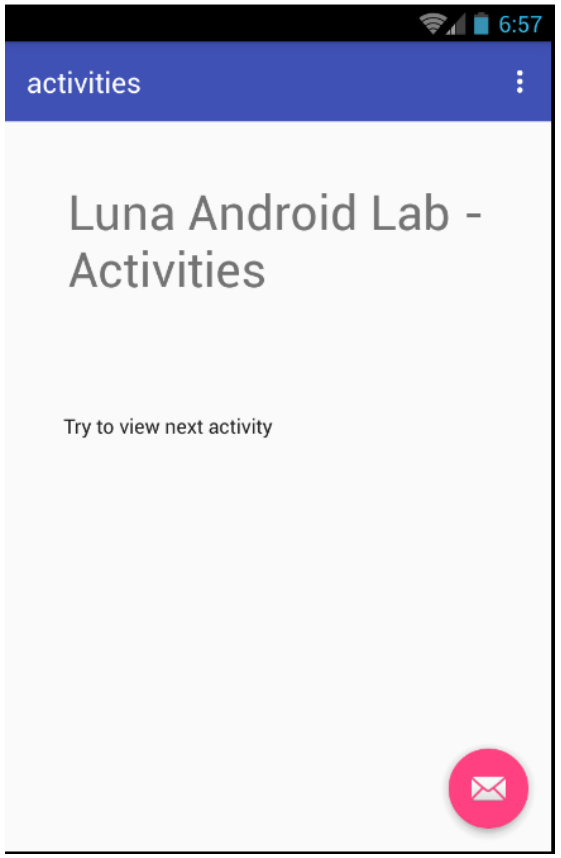
MOBILE

- Android , iOS , Tizen ,etc…

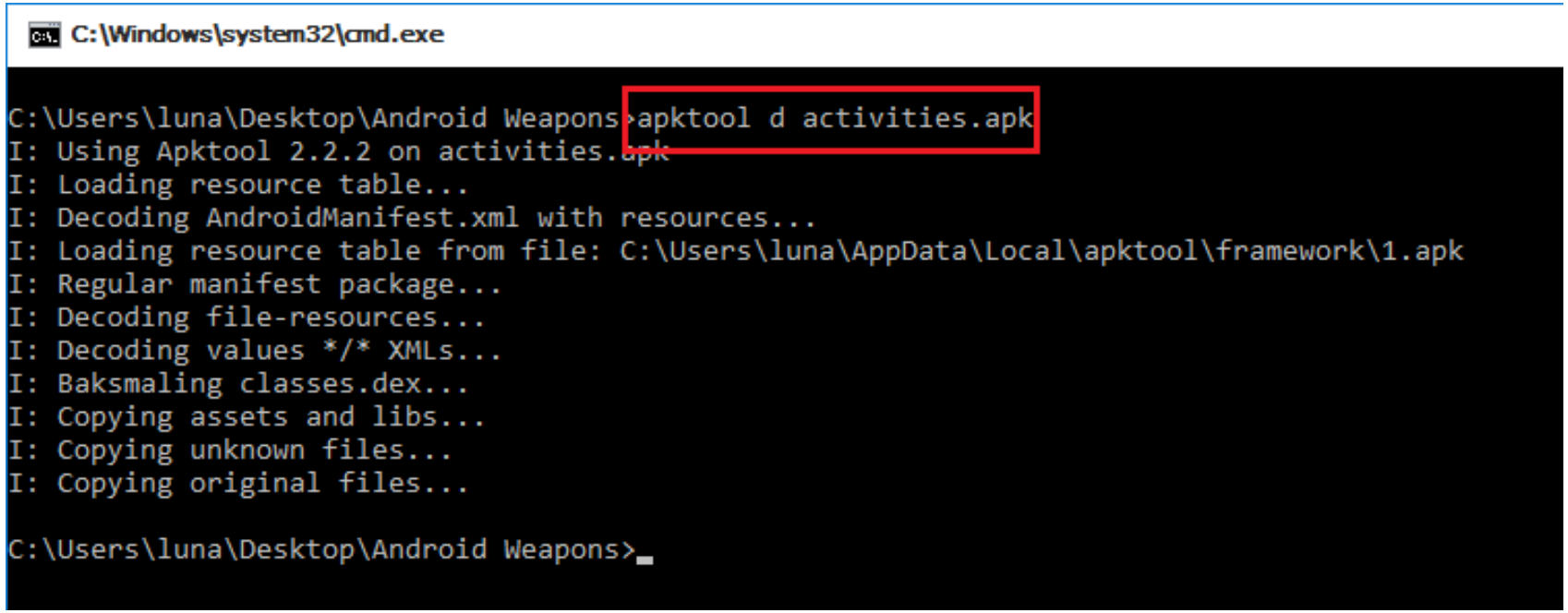
EXPLOITING ACTIVITIES

- https://developer.android.com/reference/android/app/Activity.html
- https://developer.android.com/guide/components/activities/index.html
- Activities are one of the fundamental building blocks of apps on the Android platform. They serve as the entry point for a user's interaction with an app, and are also central to how a user navigates within an app (as with the Back button) or between apps (as with the Recents button).

DEMO APPLICATION



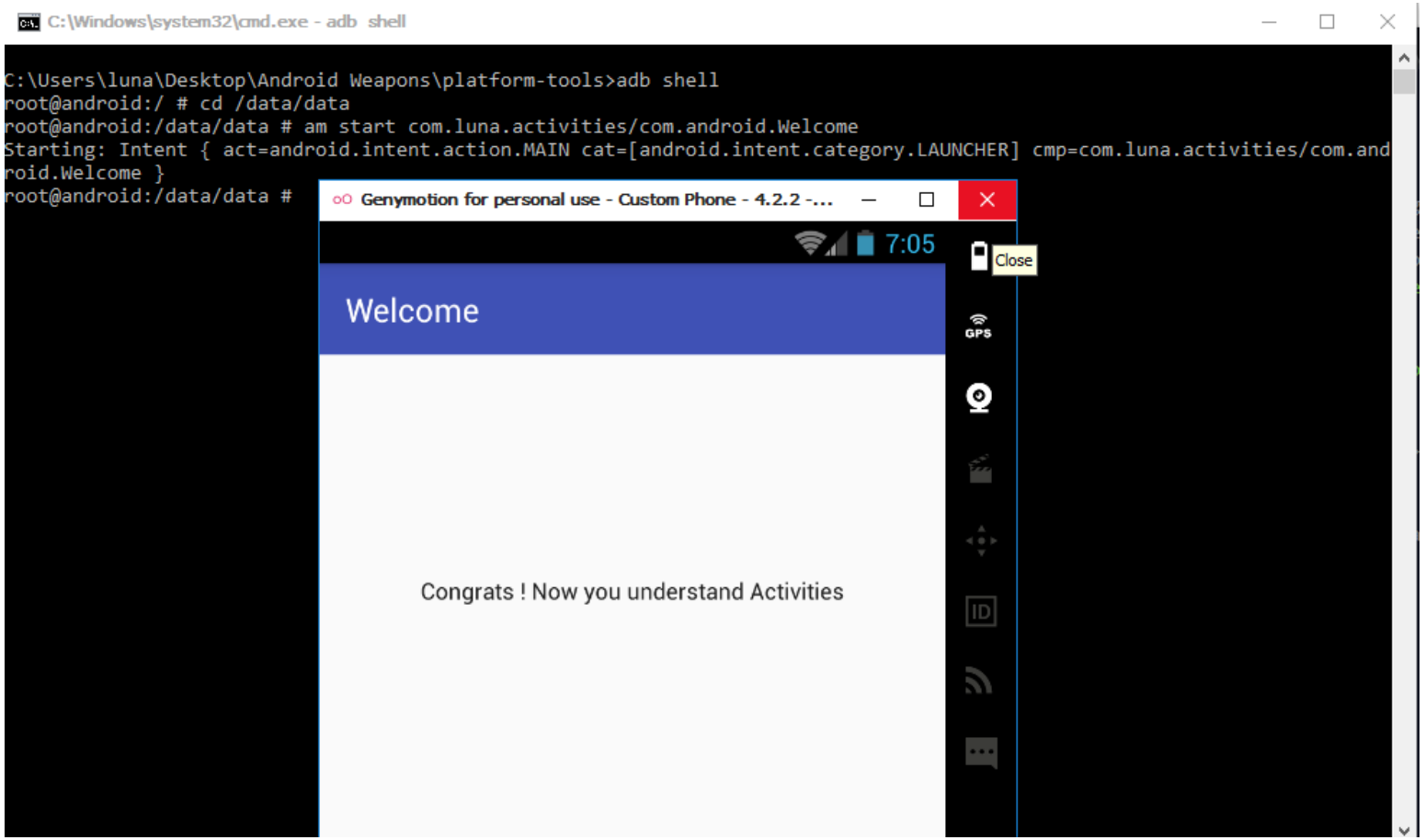
DECOMPILE APK FILE



ACTIVITIES IN ANDROIDMANIFEST.XML

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="
com.luna.activities" platformBuildVersionCode="24" platformBuildVersionName="7.0">
    <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/
    ic_launcher" android:label="@string/app_name" android:supportsRtl="true" android:theme="
    @style/AppTheme">
        <activity android:label="@string/app_name" android:name="
        com.luna.activities.MainActivity" android:theme="@style/AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_welcome" android:name="
        com.android.Welcome" android:theme="@style/AppTheme.NoActionBar"/>
    </application>
</manifest>
```

ACTIVITY MANAGER



QUESTIONS?

Feel Free to ask

THANKS

- There is so many references for my presentation.
- All of topics are googling