KDMHS-CTF Write up

Written by Safflower (st4rburst@naver.com)

Warm UP 5) sanity code

c로 작성된 소스가 주어진다.

문자열을 xor해서 HackabilityCheck라는 글자랑 비교하는 기능을 한다.

따라서 간단히 역연산 해주면 된다.

```
int main(){
    int i ;
    char input[17] = "HackabilityCheck";
    char test[17] = {15,19,6,14,21,11,7,11,33,21,26,40,1,11,4,74,0};

    for(i = 0; i < 16; ++i)
        printf("%c",test[i]^input[i]);
}
```

Flag : GreetingHacking!

Warm UP 5) Toddler's Stair - (66)

웹에 대한 기초적인 지식이 있는지 테스트하는 문제이다.

Hehe

==========

```php
<?php include('./include.php'); ?>

<!DOCTYPE html>
<html>
    <head>
        <title> Prob1 </title>
    </head>
    <body>
        <?php
            if(empty($_GET['hehe'])) {
                echo "Hehe<br>========================<br>";
                show_source('./prob1.php');
            } else {
                if($_GET['hehe'] === 'givemeflag') {
                    prob1_clear();
                }
            }
        ?>
    </body>
</html>
```

GET 파라미터를 체크하는 페이지다.

http://eb8bd87adb3e3cd59f70583382e292a0.kdmhs-ctf.com/prob1.php?hehe=givemeflag

로 이동한다.

```
Hehe
==========================================
<?php include('./include.php'); ?>

<!DOCTYPE html>
<html>
    <head>
        <title> Prob2 </title>
    </head>
    <body>
        <?php
            if(empty($_POST['please'])) {
                echo "Hehe<br>==========================<br>";
                show_source('./prob2_yoyo_0123.php');
            } else {
                if($_POST['please'] === 'givemeflag') {
                    prob2_clear();
                }
            }
        ?>
    </body>
</html>
```

POST 파라미터를 체크하는 페이지다.

이건 코딩이 필요하다.

```
Private Sub Command1_Click()
    Dim w As New WinHttp.WinHttpRequest
    w.Open "POST", "http://eb8bd87adb3e3cd59f70583382e292a0.kdmhs-ctf.com/prob2_yoyo_0123.php", True
    w.SetRequestHeader "Content-Type", "application/x-www-form-urlencoded"
    w.Send "please=givemeflag"
    w.WaitForResponse
    MsgBox w.ResponseText
End Sub
```

이렇게 전송하면 다음 문제의 URL이 나온다.

http://eb8bd87adb3e3cd59f70583382e292a0.kdmhs-ctf.com/hOihOi_prob3_.php

Hehe

==========

```php
<?php include('./include.php'); ?>

<!DOCTYPE html>
<html>
    <head>
        <title> Prob3 </title>
    </head>
    <body>
        <?php
            if(empty($_POST['please']) || empty($_GET['hehe'])) {
                echo "Hehe<br>========================<br>";
                show_source('./hOihOi_prob3_.php');
            } else {
                if($_POST['please'] === 'givemeflag' && $_GET['hehe'] === 'givemeflag') {
                    prob3_clear();
                }
            }
        ?>
    </body>
</html>
```

이건 GET과 POST 파라미터 둘다 보내줘야하므로 코딩을 한다.

```
Private Sub Command2_Click()
    Dim w As New WinHttp.WinHttpRequest
    w.Open "POST", "http://eb8bd87adb3e3cd59f70583382e292a0.kdmhs-ctf.com/hOihOi_prob3_.php?hehe=givemeflag", True
    w.SetRequestHeader "Content-Type", "application/x-www-form-urlencoded"
    w.Send "please=givemeflag"
    w.WaitForResponse
    MsgBox w.ResponseText
End Sub
```

전송하면 다음 문제의 URL이 나온다.

http://eb8bd87adb3e3cd59f70583382e292a0.kdmhs-ctf.com/yeah_f1nal_stag3.php

```
Hehe
==========================================
<?php include('./include.php'); ?>

<!DOCTYPE html>
<html>
    <head>
        <title> Prob3 </title>
    </head>
    <body>
        <?php
            if(empty($_COOKIE['kokoro'])) {
                echo "Hehe<br>========================<br>";
                show_source('./yeah_f1nal_stag3.php');
            } else {
                if($_COOKIE['kokoro'] === "PYON_PYON_SURUN_JAA") {
                    flag();
                }
            }
        ?>
    </body>
</html>
```

쿠키를 보내주면 된다. 따라서 코딩.

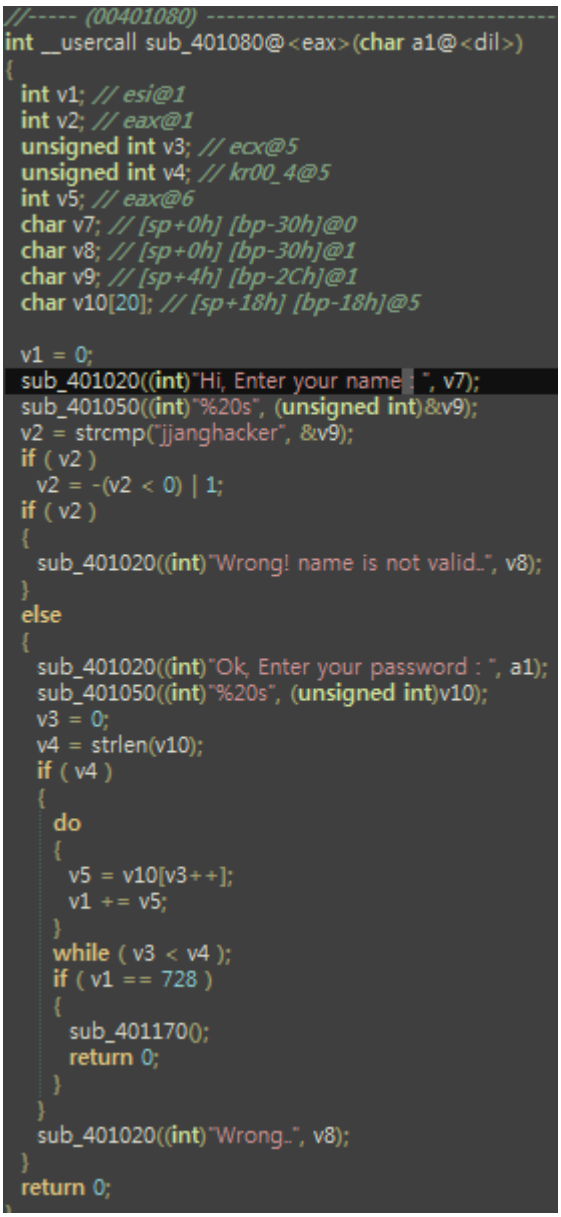
```
Private Sub Command3_Click()
    Dim w As New WinHttp.WinHttpRequest
    w.Open "POST", "http://eb8bd87adb3e3cd59f70583382e292a0.kdmhs-ctf.com/yeah_f1nal_stag3.php", True
    w.SetRequestHeader "Cookie", "kokoro=PYON_PYON_SURUN_JAA"
    w.SetRequestHeader "Content-Type", "application/x-www-form-urlencoded"
    w.Send
    w.WaitForResponse
    MsgBox w.ResponseText
End Sub
```

이렇게 하면 Flag가 나온다.

Flag : BASIC_WEB_PROB_WWWwwwWWW

Warm UP 5) sanity binary

exe 바이너리가 주어지는 간단한 리버싱 문제이다.



```
//----- (00401080) --------------------------------------------------------
int __usercall sub_401080@<eax>(char a1@<dil>)
{
  int v1; // esi@1
  int v2; // eax@1
  unsigned int v3; // ecx@5
  unsigned int v4; // kr00_4@5
  int v5; // eax@6
  char v7; // [sp+0h] [bp-30h]@0
  char v8; // [sp+0h] [bp-30h]@1
  char v9; // [sp+4h] [bp-2Ch]@1
  char v10[20]; // [sp+18h] [bp-18h]@5

  v1 = 0;
  sub_401020((int)"Hi, Enter your name : ", v7);
  sub_401050((int)"%20s", (unsigned int)&v9);
  v2 = strcmp("jjanghacker", &v9);
  if ( v2 )
    v2 = -(v2 < 0) | 1;
  if ( v2 )
  {
    sub_401020((int)"Wrong! name is not valid..", v8);
  }
  else
  {
    sub_401020((int)"Ok, Enter your password : ", a1);
    sub_401050((int)"%20s", (unsigned int)v10);
    v3 = 0;
    v4 = strlen(v10);
    if ( v4 )
    {
      do
      {
        v5 = v10[v3++];
        v1 += v5;
      }
      while ( v3 < v4 );
      if ( v1 == 728 )
      {
        sub_401170();
        return 0;
      }
    }
    sub_401020((int)"Wrong..", v8);
  }
  return 0;
}
```

처음으로 입력받은 문자열인 name을 jjanghacker와 비교한다.

그리고 몇몇 연산을 통해 비교하는데 무시하고

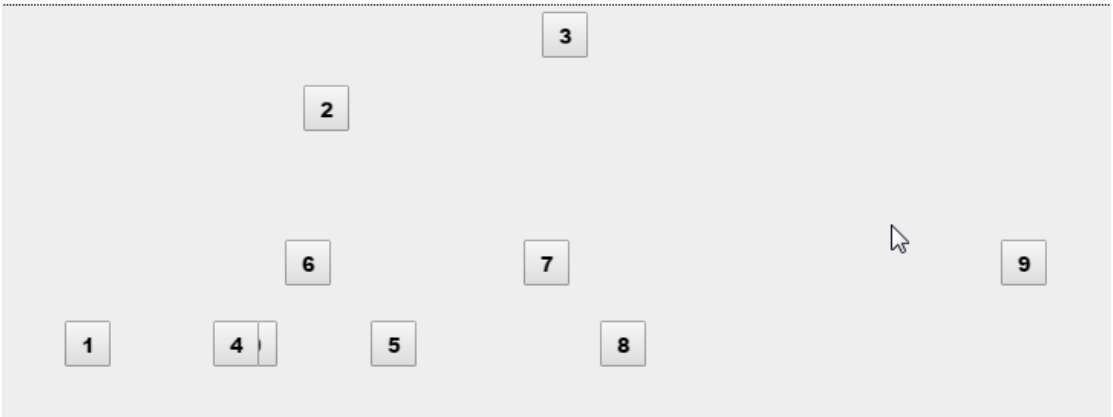
401170 함수를 실행하면 Flag가 나온다.

Flag : Good_You_are_little_jjanghacker

WEB 150) PhoneBook

그대의 이름도 성도 나 필요없소. 하지만 정말 나 원하는게 하나있소. 네 전화번호

초기화 알려주기



문제에서 주어진 URL에 들어가면 저런 페이지가 나온다.

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>전화번호</title>
<link rel="stylesheet" href="/assets/css/style.css">
</head>
<body>
<div id="input">
<p>그대의 이름도 성도 나 필요없소. 하지만 정말 나 원하는게 하나있소. 네 전화번호</p>
<div class="number"></div>
<div class="submit">
<button class="startOver">초기화</button>
<button class="enter" type="submit">알려주기</button>
</div>
<iframe style="margin-top:200px;" width="1" height="1" src="https://www.youtube.com/e
</div>
<div id="form">
<button id="button0" class="button">0</button>
<button id="button1" class="button">1</button>
<button id="button2" class="button">2</button>
<button id="button3" class="button">3</button>
<button id="button4" class="button">4</button>
<button id="button5" class="button">5</button>
<button id="button6" class="button">6</button>
<button id="button7" class="button">7</button>
<button id="button8" class="button">8</button>
<button id="button9" class="button">9</button>
</div>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.2/jquery.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/react/0.14.7/react.min.js"></script>
<script src="/assets/js/script.js"></script>
</body>
</html>
```

소스를 보면 저렇게 되어있다.

여기서 다들 여러가지 삽질을 했을것으로 예상된다.

소스에 있는 http://ctf2.codpot.net/assets/css/style.css 를 접속해보고

http://ctf2.codpot.net/assets/css/ 도 한번 접속해보았다.

그러면 파일 목록이 뜨는걸 막지 않은걸 알 수 있다.

Index of /assets/

../		
css/	07-May-2016 09:53	-
image/	07-May-2016 09:46	-
js/	07-May-2016 09:53	-

http://ctf2.codpot.net/assets/ 에 접속하면 폴더가 3개 나온다.

image 폴더는 소스에서 본적 없는 경로였다.

Index of /assets/image/

../		
a/	07-May-2016 09:46	-
b/	07-May-2016 09:46	-
c/	07-May-2016 09:46	-
d/	07-May-2016 09:46	-
e/	07-May-2016 09:46	-
f/	07-May-2016 09:46	-
g/	07-May-2016 09:46	-
h/	07-May-2016 09:46	-
i/	07-May-2016 09:46	-
j/	07-May-2016 09:46	-
k/	07-May-2016 09:46	-
l/	07-May-2016 09:46	-
m/	07-May-2016 09:46	-
n/	07-May-2016 09:46	-
o/	07-May-2016 09:46	-
p/	07-May-2016 09:46	-
q/	07-May-2016 09:46	-
r/	07-May-2016 09:46	-
s/	07-May-2016 09:46	-
t/	07-May-2016 09:46	-
u/	07-May-2016 09:46	-
v/	07-May-2016 09:46	-
w/	07-May-2016 09:46	-
x/	07-May-2016 09:46	-
y/	07-May-2016 09:46	-
z/	07-May-2016 09:46	-

접속하면 a부터 z까지의 폴더가 있고

한번 더 접속하면, 또 접속하면 또 있고, 또 접속하면 또 있다. 총 4번이다.

Index of /assets/image/a/a/a/a/

../

적당히 들어가보면 아무것도 없다.

저 많은 경로들 중 Flag가 숨어있을것이라 짐작하고 코딩을 했다.

```
Private Sub Command1_Click()
    Dim w As New WinHttp.WinHttpRequest
    Dim z As Long, x As Long, c As Long, v As Long, url As String
    Const a = "abcdefghijklmnopqrstuvwxyz"

    For z = 1 To 26
    For x = 1 To 26
    For c = 1 To 26
    For v = 1 To 26
        url = Mid(a, z, 1) & "/" & Mid(a, x, 1) & "/" & Mid(a, c, 1) & "/" & Mid(a, v, 1) & "/"

        w.Open "Get", "http://ctf2.codpot.net/assets/image/" & url, True
        w.Send
        w.WaitForResponse

        If UBound(Split(w.ResponseText, "<a href=""")) <> 1 Then
            MsgBox "빙고 : " & url, 64
        End If
    Next v
    Next c
    Next x
    Next z
End Sub
```

이렇게 돌리다보면

http://ctf2.codpot.net/assets/image/t/i/p/i/

경로에 파일이 들어있음을 감지한다.

http://ctf2.codpot.net/assets/image/t/i/p/i/<-flag/

tipi가 Flag임을 알려준다.

(이건 너무 짧은거 아닌가 싶다.)

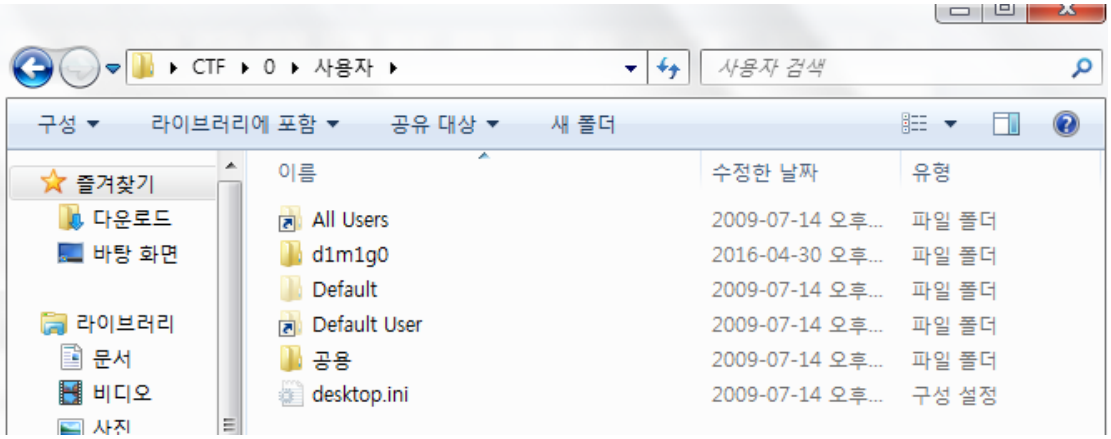
Flag : tipi

FORENSIC 250) Window Forensic 1

박군의 하드디스크의 사본(vmdk 파일)이 주어진다.

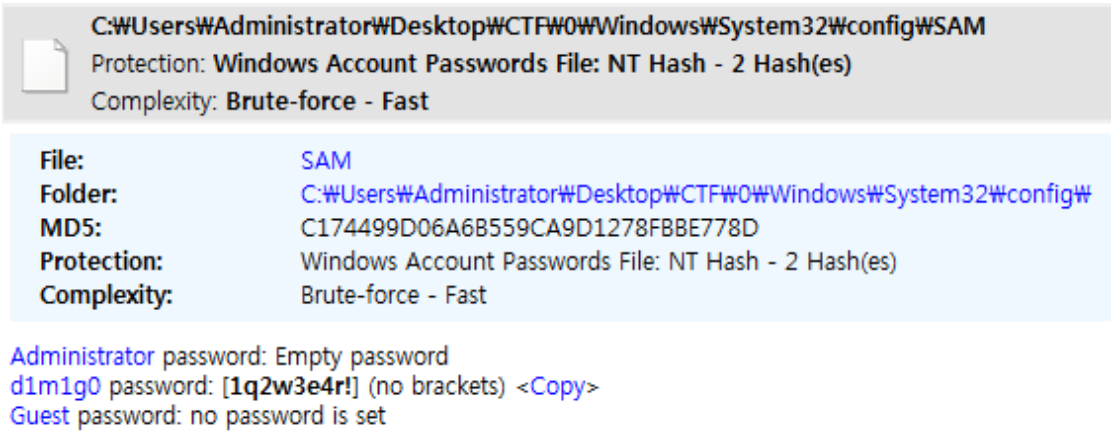
그리고 박 군이 사용하는 윈도우 계정명_박 군이 사용하는 윈도우 비밀번호가 Flag 라고 한다.

일단 vmdk 파일을 폴더와 파일로 바꾼다. 7z로 했다.



좀 돌아보면 박군의 윈도우 계정 이름은 d1m1g0 임을 알 수 있다.

윈도우 비밀번호는 ₩windows₩system32₩config 경로에 있는 SAM과 SYSTEM 파일을 통해 알아낼 수 있다.



브루트포스 프로그램을 돌리면 눈깜짝할새에 크랙된다.

윈도우 비밀번호는 1q2w3e4r! 이다.

Flag : d1m1g0_1q2w3e4r!

보너스) 1점짜리 Flag

JTJ님은 핸섬하다.

Flag : JTJISHANSOME_ARNT?zzzzzzzzzzzz
