

CVE-2017-9430分析

复现环境：

推荐使用的环境	备注	
操作系统	Ubuntu 12.04	体系结构：32 位
调试器	gdb-peda	版本号：7.4
漏洞软件	DNSTracer	版本号：1.9

安装dnstracer：

```
$ wget http://www.mavetju.org/download/dnstracer-1.9.tar.gz
$ tar zxvf dnstracer-1.9.tar.gz
$ cd dnstracer-1.9
$ ./configure
$ make && sudo make install
```

安装peda：

这个可以自己网上找教程

关闭各种栈保护：

1.改makefile至如下

```
$ cat Makefile | grep -w CC
```


```
root@ubuntu:~/dnstracer-1.9# cat Makefile | grep -w CC
CC = gcc -fno-stack-protector -z execstack -D_FORTIFY_SOURCE=0
COMPILE = $(CC) $(DEFS) $(DEFAULT_INCLUDES) $(INCLUDES) $(AM_CPPFLAGS) \
CCLD = $(CC)
```

2.卸载之前编译的dnstracer，要不然编译了没用（踩坑）：

```
make uninstall
make clean
```

3.重新编译：

```
make  
make install
```

A terminal window with a dark purple background. The prompt is 'gdb-peda\$'. The command 'checksec' has been executed, resulting in the following output: 'CANARY : disabled', 'FORTIFY : disabled', 'NX : disabled', 'PIE : disabled', and 'RELRO : Partial'.

```
gdb-peda$ checksec  
CANARY : disabled  
FORTIFY : disabled  
NX : disabled  
PIE : disabled  
RELRO : Partial
```

如图为关闭栈保护的情况

关闭ASLR

```
# echo 0 > /proc/sys/kernel/randomize_va_space
```