Elijah Andrushenko

10/26/2018

Computer Security

CPTS 427

Project 3

1.

Setting kernel.randomize\_va\_space to 0 disables address space layout randomization. The purpose of this is to allow us the track where things are in memory as it will now follow a more logical structure, rather than being place randomly in memory.

2.

“-z execstack” override binaries and libraries from being required on the executable stack.

“-fno-stack-protector” just in case stack protection is on, we turn it off

It is important to disable these features otherwise it may not compile anything that’s not linked in the standard user space libraries

3.

The error is at strcpy(buf, passwd);

Destination size is 512 bytes

Source size is 1024 bytes

4.

letmein

5.

Stack pointer = 0xbfffe8c0

Base pointer = 0xbfffed48

Buf Array = 0xb7f1cef0

Auth = 0xbfffd8c0

6.

Location = 0xb7e51df9 //0xbfffe8cc

Value = “=” //”\371\035\345\267H\355\377\277\003”

7.

“/0x90” \* 521

8.

521 bytes

9.

Output value = length 7, letmein

10.

No it does not work, since the address of the registers changes every time it compiles so we don’t have the correct information any longer.