
Part III - Questions
Slides: http://10kstudents.eu/m/files/material/pptx/syssec_10K_Countermeasures.pptx

---

3.1 Explain how to exploit the example on slide 65 (assuming random stack canaries)

3.2 Exploit the same code, but now assume random canaries protect
the stack, and assume DEP prevents execution of the stack

3.3 Now assume that (i) random canaries protect the stack, (ii) DEP
prevents execution of the stack, and (iii) the stack and the start
address of the code is randomized by ASLR. However, let all
functions are still at the same relative offset from start address
of code (in other words: need only a single code pointer). Can you
still exploit the code?
