
Part II - Questions
Slides: http://10kstudents.eu/m/files/material/pptx/syssec_10K_Real_BO.pptx

---

2.1 A NOP sled in the injection vector is really useful for an attack,
    as it no longer need to be very precise in where it jumps to. Why
    can the attacker *not* (always) simply make an enormous NOP sled
    of, say megabytes or gigabytes long, so you can be extremely
    sloppy in picking the target address as you have a good chance of
    hitting the sled?

2.2 Say the reply buffer starts at address 0xbfffee00. Explain exactly
    what you need to do to exploit the code example on slides 6-18.
