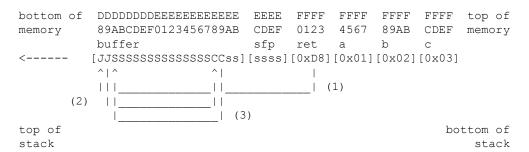


CEG 429/629:Internet Security

Spring 2011 • Midterm • 100 points • 75min

Remote login to gandalf and turnin your answers as in ~pmateti/CEG429/turnin MT answers.txt

- 1. (5*5 points each) The following statements may or may not be (fully or partially) valid. Explain <u>the underlined technical term</u> occurring in each statement. Explain/discuss/ dispute the statement. It is <u>possible</u> to write no more than, say, ten, sentences each, and yet receive full score.
 - a. It is possible to setup a Linux/ Unix system without a single <u>suid</u> program.
 - b. Backdoors are used to install <u>rootkits</u>.
 - c. In a TCP segment with SYN=1, the <u>SEQ number</u> must be non-zero.
 - d. Masquerading, <u>spoofing</u>, and smurfing are all describing changes made to IP packets.
 - e. It is possible to determine the local gateway of an unknown network via passive sniffing.
- 2. (3*15 points)
 - a. Explain how public-key encryption scheme can be useful in the communication between two people.
 - b. Describe, in detail, the techniques used in hijack.
 - c. Consider the following ten significant events that occur in the rebooting of a Unix machine from power on to login prompt. The events may or may not occur in the order given. E1: Root volume is mounted by the kernel; E2: Process init is created; E3: inetd daemon is started; E4. OS Boot loader invokes the kernel; E5: getty processes are started. E6: The run level changes from 3 to 5. E7: BIOS finds the boot device. E8: run level changes to 0, E9: All file volumes are unmounted. E10: Networking is shutdown. (3*5 points) Explain steps E3, E4 and E8 further, and describe how security could be breeched in these steps.
- 3. (3*10 points) The context of this question is the paper by Aleph One.



- a. Explain *fully* the purpose and functionality of the arrow labeled (3).
- b. How does exploit3.c differ from exploit4.c?
- c. Describe an alternate but equivalent version of get_sp() without using any assembly code.