CEG 429/629:Internet Security

Spring 2010 • Midterm • 100 points • 75min

Prabhaker Mateti

Login and use a Linux or Windows PC and use any editor in the OSIS Lab while answering. However, this is a closed book, closed notes exam. Surfing is disabled. Do not use pre-existing files. Do not give or take help during the exam. Man-pages, KDE/Gnome, konsole, re-booting into Windows or Linux, etc. are available. 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 *the underlined technical term* occurring in each statement. Explain/ discuss/ dispute the statement. It is *possible* 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 `suid` program.
   b. Backdoors are used to install rootkits.
   c. In a TCP segment with SYN=1, the SEQ number must be non-zero.
   d. On a host that has two NICs, a fully capable *routing table* need be no more than two rows.
   e. It is possible to determine the local gateway of an unknown network via passive sniffing.
2. (3*15 points)
   a. Suppose that an attacker has acquired privileges to read/write/execute any file on a Linux/Unix system. Suppose his/her goal is to obtain one hundred userid-password combinations, and replace what ever changes he/she may have made with their originals so that this activity has a greater chance of going unnoticed. Describe what files are changed where and how.
   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. (5 points) Order these events chronologically. (10 points) Explain steps E3, and E8 further, and describe how security may have been breeched in these two steps.
3. (3*10 points) The context of this question is the paper by Aleph One.

```
bottom of  DDDDDDDDEEEEEEEEEEEE  EEEE  FFFF  FFFF  FFFF  FFFF      top of
memory     89ABCDEF0123456789AB  CDEF  0123  4567  89AB  CDEF      memory
           buffer                sfp   ret   a     b     c
<------   [JJSSSSSSSSSSSSSSCCss][ssss][0xD8][0x01][0x02][0x03]
           ^|^             ^|            |
           |||_____________||____________|  (1)
       (2)  ||_____________||
             |______________| (3)
top of                                                          bottom of
stack                                                               stack
```

   a. Explain *fully* the arrow labeled (3).
   b. How does `exploit3.c` from the paper by Aleph One differ from `exploit4.c`?
   c. Describe an alternate but equivalent version of `get_sp()` without using any assembly code.