Race Condition Lab

Computer Security

Outline

- Some basic methods
- File format of /etc/shadow and /etc/passwd

Functions

- fstat()
- seteuid()

File format of passwd and shadow

- http://tinyurl.com/etcpasswd-cis643
- http://tinyurl.com/etcshadow-cis643

Note

- To add a new user to the PC, add a new entry to /etc/passwd and /etc/shadow.
- Add a new user attacker. Pay close attention to the user id and group id fields.
- Remember to save a copy of /etc/passwd and /etc/shadow to other directory.
- Before you reboot, make sure that /etc/passwd and /etc/shadow are correct.
- Use `sudo sysctl –w kernel.yama.protected_sticky_symlinks=0` (Remember to use '-w')

Task 1

- First look at /etc/passwd and /etc/shadow. Understand the format.
- Use check.sh from the lab description website: http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Race_Condition/
- Modify /etc/passwd file and /etc/shadow file using vulp.c (Use input redirection. Create a file with the new attacker user details. Run the input redirection command to vulp in a loop. Use a shell script for that).
- NOTE: in the /etc/shadow file, for the encrypted password, use `U6aMy0wojraho` as the encrypted password. (This is the encrypted format for a blank password)

Task 1

- Write a program (Use a shell script/Write a program in any language i.e shell script, C, C++, Java, Python, etc) to change the link between passwd, shadow, and a valid file
- Depending on the speed of your computer, the attack can happen in either the first shot, or after 1000 tries. Use a program that **loops over all the steps**

Task 2

- Add new access() and open() checks to program. Also add i-node checks.
- Report if you are successful with the new changes.

Task 3

- Use seteuid() to change the user’s effective user id from root to a lower privilege level
- Report if attack was successful

Task 4

- Reactivate protection scheme.
- Answer the questions asked in the report.