Homework #1 Race Condition Vulnerability and Dirty CoW
CIS 4626/CIS 5627, Offensive Computer Security, Fall 2023
Department of Computer Science, Florida State University

Points: 55
Due: 11:59PM on Friday, December 8th, 2023 (note that no late submissions will be accepted for this assignment.)

Submission: For this assignment, you must submit your answers online via Canvas by uploading a pdf file named "**hw1-Report-Firstname-Lastname.pdf**". Here replace "Firstname" by your first name and replace "Lastname" by your last name in the file name.

Problem 1 (15 points) Describe the general race condition problem and the special TOCTTOU race condition problem. Then describe the race condition vulnerabilities and how they can be exploited. Note that you do NOT need to conduct any experiments.

Problem 2 (10 points) Does the following privileged Set-UID program have a race condition problem? If so, where is the attack window? Then describe how you would exploit this race condition window.

```
1   filename = "/tmp/XYZ";
2   fd = open (filename, O_RDWR);
3   status = access (filename, W_OK);
    ...
    ... (code omitted) ...
    ...
10  if (status == ACCESS_ALLOWED) {
11     write_to_file(fd);
12  } else {
13     fprintf(stderr, "Permission denied\n");
14  }
```

Problem 3 (10 points) How many race conditions do attackers have to win in the following program in order to exploit the vulnerability successfully? Briefly justify your answer.

```
int main()
{
   struct stat stat1, stat2;
   int fd1, fd2;

   if (access("/tmp/XYZ", O_RDWR)) {
      fprintf(stderr, "Permission denied\n");
      return -1;
   }
   else fd1 = open("/tmp/XYZ", O_RDWR);

   if (access("/tmp/XYZ", O_RDWR)) {
      fprintf(stderr, "Permission denied\n");
      return -1;
   }
   else fd2 = open("/tmp/XYZ", O_RDWR);

   The program then checks whether fd1 and fd2 refer to
   the same file, if so, the program will write to
   fd1 (or fd2). Otherwise, the program will do nothing
   and exit.
}
```

Problem 4 (5 points) A file's content is a string "*Florida_State_University*" without the double quotes. When this file is mapped to memory (the entire file) using mmap(), and the memory address is stored in a variable *map*. Describe what the following *printf*() statement prints out.

```
char *addr = (char *)map;
printf("%s\n", map +8);
```

Problem 5 (15 points) Explain clearly the Dirty CoW race condition vulnerability in the Linux Kernel and how that is exploited to gain the root privilege by an attacker.

Extra Credit Problem

Problem 6 (5 points) The chapter on the Dirty CoW Race Condition Attack in the textbook shows that by exploiting the Dirty COW race condition, one can modify /etc/passwd file and gain the root privilege. Name two other files that can be attacked to gain the root privilege and briefly explain.