COLLABORATOR(S):\_\_\_\_\_

5/3/1/0 1. What configuration file stores information about the user id's (or uid's)? What configuration file stores information about the group id's (or gid's)?

5/3/1/0 2. Using the id command, what is your user id and what groups are you a part of?

5/3/1/0 3. Using the id command, what is the user id for the user's aviv, pepin, and m179998.

5/3/1/0 4. Explain why there must be a descalation of priviledge when **login** executes the **shell** for an authenticated user?

5/3/1/0 5. Consider a program with the following permissions:

-rwxr-x--x 1 aviv scs 8622 Mar 30 10:40 /home/scs/aviv/lec-23-demo/get uidgid

When you run that program, as your user information, what capabilities does thatprogram have? Is it the owner of the program or the user who runs the program? 10/8/4/2/0 Match the system call to their descriptions:

getuid()	 (a) get the effective group id
getgid()	 (b) set the effective user id
getegid()	 (c) set the real and effective user id
geteuid()	 (d) get the real user id
setuid(uid)	 (e) get the effective user id
setgid(gid)	 (f) set the effective group id
setreuid(uid,euid)	 (g) set the real and effective group id
<pre>setregid(gid,egid)</pre>	 (h) get the real group id

 $^{5/3/1/0}$  7. What is the difference between the effective and the real user or group id?

5/3/1/0 8. What are the three additional set-bits and their octal values?

9. Match the chmod command to its permission string:

chmod 6750 \_\_\_\_ (a) rwxr-s---

chmod 4750 \_\_\_\_ (b) rwsr-s---

chmod 2750 (c) rwsr-x---

5/3/1/0 10. When you run an set-bit program what system call do you use to downgrade to the **real group id** of the user who executed the program?

5/3/1/0 11. What is the user and group id for the root user?

5/3/1/0 12. Explain how a set-bit programs can be dangerous for security?

5/3/1/0 13. What does the library function system() do?

5/3/1/0 14. Explain how the enviroment variable **PATH** is used to select which program to execute.

5/3/1/0

 $\frac{3}{10}$  15. Match the attack to it discription:

NAME :

5/3/1/0 16. The following program has a security flaw, describe how to exploit it:

int main() {

system("cat sample.db | cut -d ',' -f 3 | sort | uniq")

}

5/3/1/0 17. For the above program, how would you protect this program?

 $8/5/3/1/0\,18\,.$  The following program has two security flaws, describe them and how to exploit them: 

```
int main() {
    char cmd[1024];
    char fname[40];
    printf("Enter file name:\n");
     scanf("%s",fname);
```

```
snprtinf(cmd,1024,"/bin/cat %s",fname);
system(cmd);
                                         b)
```

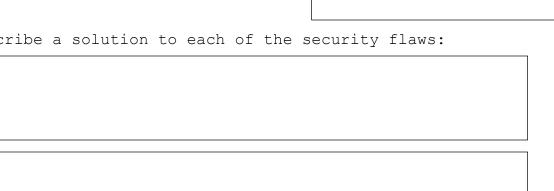
}

7/5/3/1/0

a)

b)

19. Describe a solution to each of the security flaws:



a)			