___/40 IC221 System Programming
Spring 2015
HW13

NAME:_____

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?

____/25

NAME: _____

10/8/4/2/0 6. 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
setregid(gid,egid)	____	(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---

____/20

NAME: _____

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 15. Match the attack to it discription:

Priviledge escalation _____	(a) Where an attacker inserts a program of the same name as the one the shell is searching to execute
Injection Attack _____	(b) Where an attacker can execute a shell (or arbitrary programs) as another user
Buffer Overflow _____	(c) Where an attacker provides excessive input to alter some program state to launch an attack
Path Attack ____	(d) Where an attacker crafts input to contain aribitrary programs to be executed

___/30

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);

}
```

a)

b)

7/5/3/1/0 19. Describe a solution to each of the security flaws:

a)

b)

___/25