**Set-UID Program Vulnerability Lab Report**

Ankit Kumar

**Task 1:** Understanding “passwd”, “chsh”, “su” and “sudo”

**Observation:**

1.

* 1. passwd is a program or tool on UNIX operating systems that is used to change the user’s password or to change a local accounts password.

1.2. chsh is short form for change shell, it is used to change a login shell. This program modifies the /etc/passwd file and only allows users to modify their own login shells

1.3. su is short for substitute user, it is used to change the login session’s owner. Su can change the ownership of a session to any owner but is mostly use to change

the owner to root, to gain access to all commands and files of a system.

1.4. sudo is short for substitute user do, it allows the substituted user to execute commands as the owner of that session, the real and effective uid and gid are set

and made to match with that of the target user in the passwd file. Authorized users are determined by referring to /etc/sudoers file.

1. 2.1

**Explanation:**

**Task 2:**

**Observation:**

**Explanation:**

**Task 3:**

**Observation:**

**Explanation:**

**Task 4:**

**Observation:**

**Explanation:**

**Task 5:**

**Observation:**

**Explanation:**

**Task 6:**

**Observation:**

**Explanation:**

**Task 7:**

**Observation:**

**Explanation:**