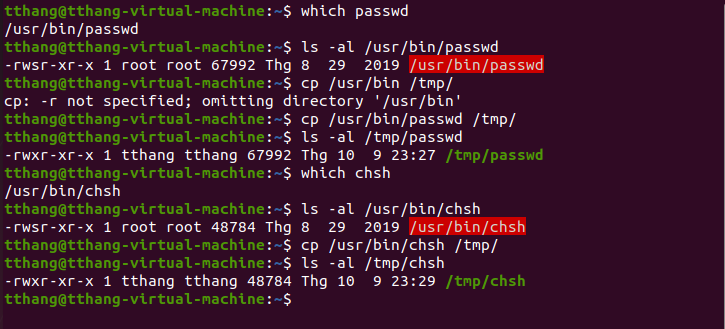
Lab 4: Set-UID Program Vulnerability Lab

1. Figure out why "passwd", "chsh", "su", and "sudo" commands need to be Set-UID programs. What will happen if they are not? If you are not familiar with these programs, you should first learn what they can do by reading their manuals. Please copy these commands to your own directory; the copies will not be Set-UID programs. Run the copied programs, and observe what happens.

* ở đây chúng ta có thể thấy khi sao chép “passwd” hay “chsh” vào tmp thì đều mất quyền root tương tự thị “su” và “sudo” cũng vậy.



1. Run Set-UID shell programs in Linux, and describe and explain your observations.
2. Login as root, copy /bin/zsh to /tmp, and make it a set-root-uid program with permission 4755. Then login as a normal user, and run /tmp/zsh. Will you get root privilege? Please describe your observation.

