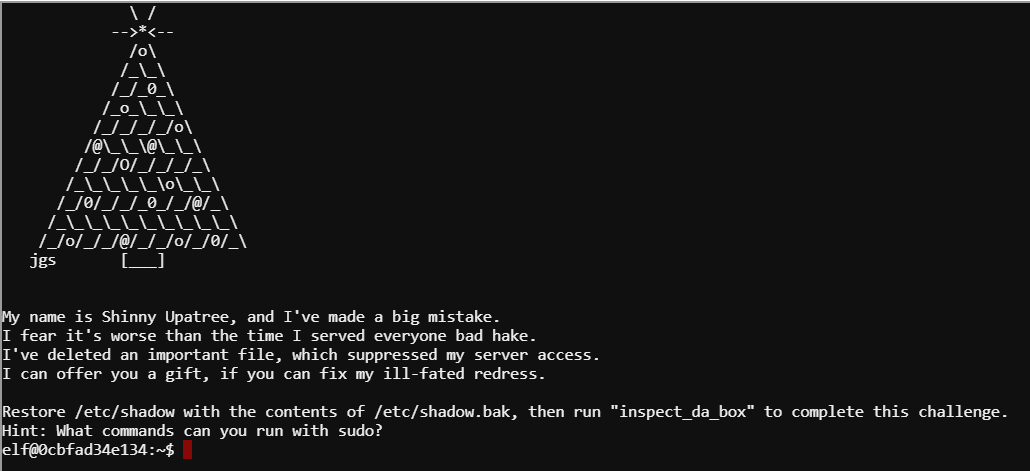
# Oh Wait! Maybe We Are… Linux Challenge, or Shadow File Restoration terminal challenge

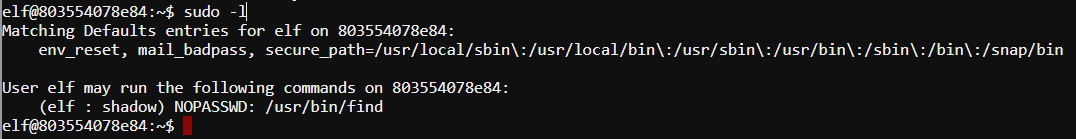
This challenge teaches you more about the sudo and file commands. You often use sudo when it is configured to let you run any command as root, so that you only use root privileges when you need them. The sudo command can be configured to be much more granular than that, allowing a user to run only specific programs as root or some other user.

The find command also can execute commands based on what it finds, using the -exec option. For example, consider the case where you would like to find all files that contain “sql” in the file name, and then grep those files to see if they contain “username”.  
find ~ -name \*sql\* -exec grep username {} \;  
The first part of the command is a standard find, which looks for files in my home directory that have sql in the name. The second part causes find to execute a grep search for username, and it inserts the name of the file it found in place of the braces. The command needs to end with a semicolon, hence the “\;”.

The terminal is in the “Oh Wait! Maybe We Are…” game, in the bottom right corner. If you use the SVGS account, the terminal is in the stocking as Shadow File Restoration terminal challenge.

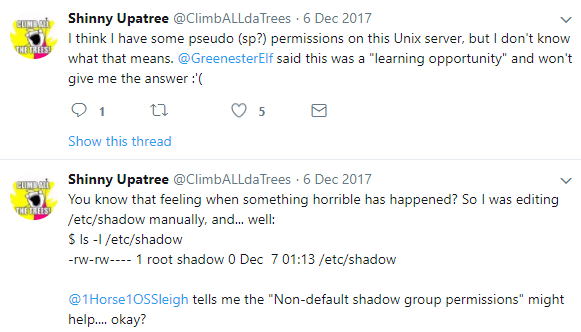


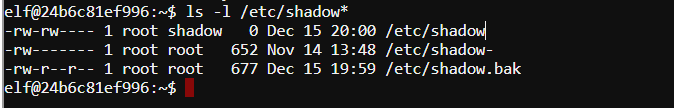
Our goal is to help Shinny repair his /etc/shadow file, without access to the root password.

Note that the terminal shows a hint, “what commands can you run with sudo?” The sudo command has an option that will list your user’s privileges. Find the option and run it. 1) What commands can the elf user run with sudo? 

The user elf can run /usr/bin/find, without a password.

## Other Hints



By looking at Shinny’s posts, or using ls -l, you should be able to see what the problem is with /etc/shadow. 2) What is wrong, and what impact could it have on the server? 

The /etc/shadow file is 0 bytes long…empty. No one can log in to this server as it stands.

## Method

Once you’ve execute sudo with the correct option, you should know elf can run find. Whoever configured that must have forgotten that find can execute other commands. If we use sudo to run find as root, the commands we execute from find will also execute as root. As a test, run  
sudo find --help  
just to confirm it will work.

You should find that sudo asks for a password, even though the original sudo output told us that elf did not need a password to run find. 

Note that the user portion is “(elf : shadow)”. This says that to run /usr/bin/find, the user should be elf and the group should be shadow. Run the command, groups elf, to determine the primary group for the user elf. You should find that the primary group for the user elf is the group elf. We need to run sudo as user elf, but with group shadow. 3) Is there a way to change the group that sudo uses, instead of the user’s primary group? What is it? From sudo -h

sudo -g shadow find… should work for us.

Once you can run find as root, you should be able to execute a command from find that copies the file shadow.bak to shadow. Then run ./inspect\_da\_box to see if it worked.

4) What is the command that will copy shadow.bak to shadow, and solve Shinny’s problem? Note: You don’t need to use the {} syntax unless you want to--you should know exactly the command you need to run. You don’t want find to locate 1,000 files and execute your command 1,000 times, so it is probably best to search for shadow.bak, so you only find one. You can save time by starting the search from the directory that shadow.bak lives in, instead of searching from the file system root.

sudo -g shadow find /etc -name shadow.bak -exec cp {} /etc/shadow \;  
or  
sudo -g shadow find /etc -name shadow.bak -exec cp /etc/shadow.bak /etc/shadow \;

