Lab Report Requirements

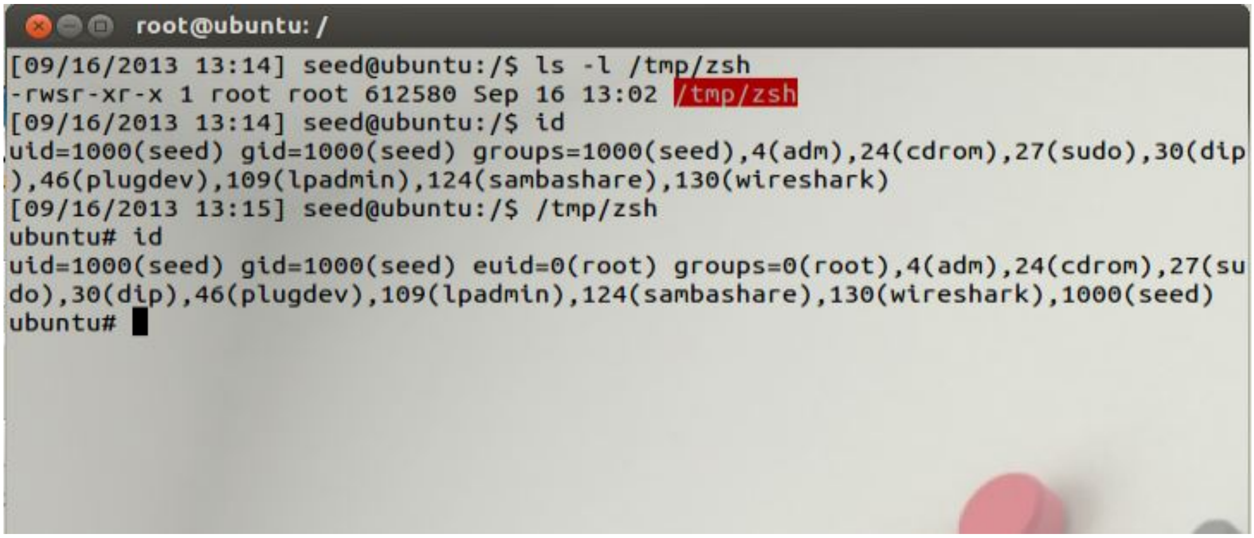
For each lab, there are **tasks** and **questions**. Your report should cover them all, or else you should expect deductions. Please see the syllabus for the lab schedule and grading information.

Here we will talk about how to work on a task: for most of the labs, the lab report is the only way to prove that you have done the lab correctly. So the lab report should be carefully done and include the following:

1. **Including a screen shot** is the best proof. Usually, each task requires two screen shots: before the attack and after the attack to honor your answer. Also, the **time stamp** and **background** on the terminal should be included just in case the screen shot is copied from the previous student.
2. Only including the screen shot doesn't mean you understand what you are doing. So **observations** and **explanations** are required. The observation section will describe the screen shot, and the explanation section will link back to the lab description or the concept to complete the story. Sometimes, the two sections can be mixed together but the idea is the same.
3. If there is anything wrong or suspicious about your report, we will deduct extra points. The only way to get the points back should be a **demo** in the lab section or during office hours. Extra questions are expected as well.

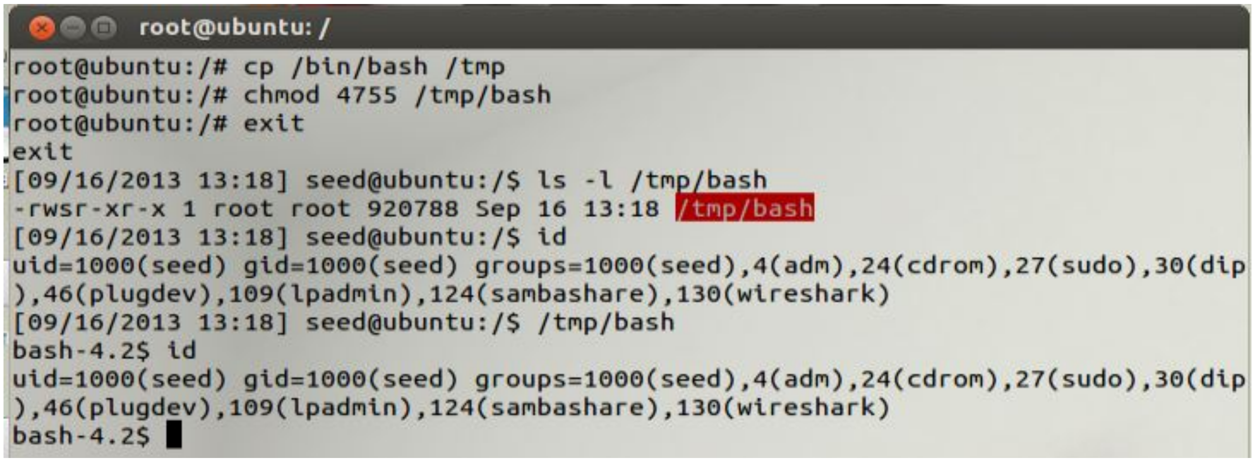
Here is an example to show you what the report task should look like.

Concrete Sample Answer:



```
[09/16/2013 13:14] seed@ubuntu:/$ ls -l /tmp/zsh
-rwsr-xr-x 1 root root 612580 Sep 16 13:02 /tmp/zsh
[09/16/2013 13:14] seed@ubuntu:/$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[09/16/2013 13:15] seed@ubuntu:/$ /tmp/zsh
ubuntu# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=0(root),4(adm),24(cdrom),27(su
do),30(dip),46(plugdev),109(lpadmin),124(sambashare),130(wireshark),1000(seed)
ubuntu# █
```

Observation: We copied zsh to /tmp folder, and changed mode to 4755, to made it a set-uid program. The indicator # shows that we have gained root privilege, so the attack succeeded. We can further demonstrate that by running "id" command; we can see the effective user id is 0(root). Before we run zsh, we can see the effective user id is seed.



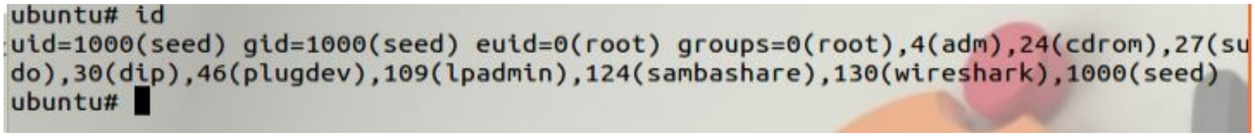
```
root@ubuntu:/# cp /bin/bash /tmp
root@ubuntu:/# chmod 4755 /tmp/bash
root@ubuntu:/# exit
exit
[09/16/2013 13:18] seed@ubuntu:/$ ls -l /tmp/bash
-rwsr-xr-x 1 root root 920788 Sep 16 13:18 /tmp/bash
[09/16/2013 13:18] seed@ubuntu:/$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[09/16/2013 13:18] seed@ubuntu:/$ /tmp/bash
bash-4.2$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
bash-4.2$ █
```

Observation: We do the same test for “bash” as above. The indicator $ shows that we don’t gain root privilege. We also demonstrate that by running “id” command. Before we run bash, the effective user is seed; after we run bash, the effective user remains the same. Attack failed.

Explanation: For bash shell, it has some built-in protection mechanism; if the effective uid is root but the real uid is not root, then it will set the effective uid to the real uid in the new shell to prevent the abuse of root privilege. But in zsh shell, the effective user id will remain the same with whoever invokes this new shell. So the attack works in zsh case but does not work in bash case.

Unacceptable Answers:

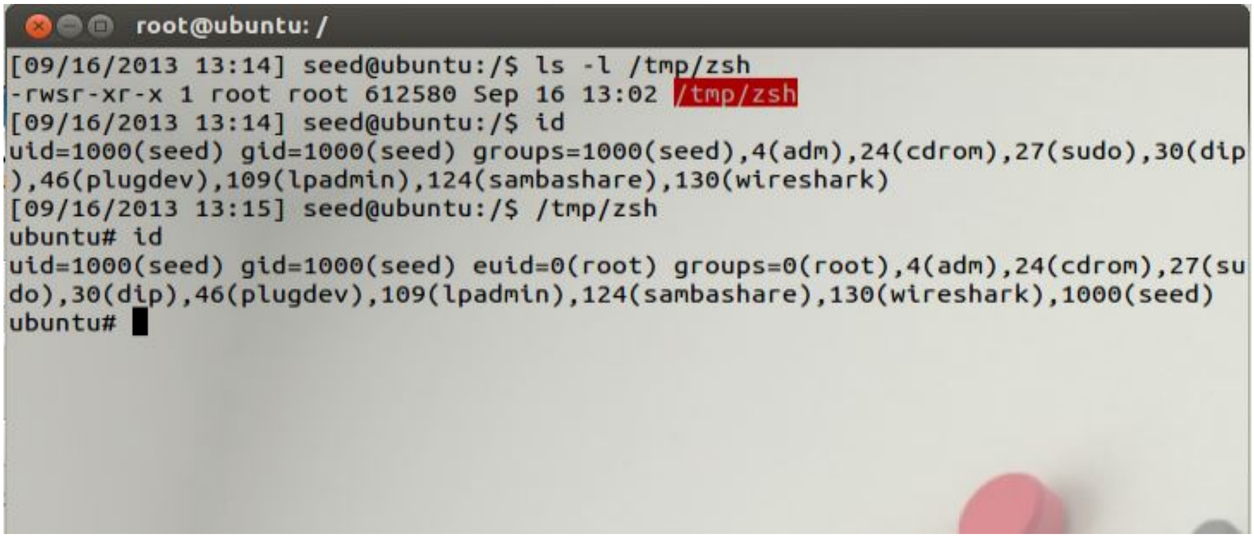
1.



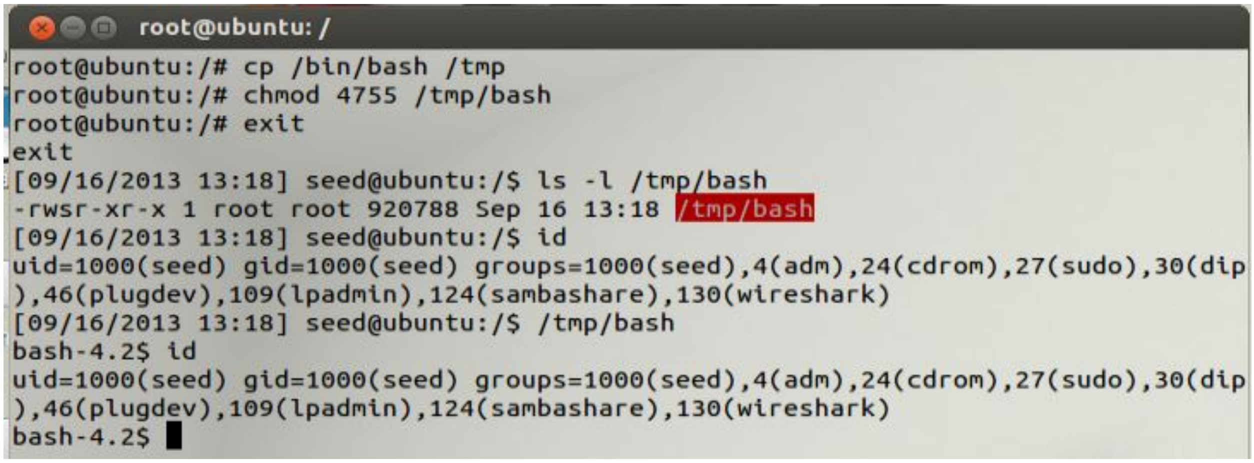
```
ubuntu# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=0(root),4(adm),24(cdrom),27(su
do),30(dip),46(plugdev),109(lpadmin),124(sambashare),130(wireshark),1000(seed)
ubuntu# █
```

No time stamp; need at least one entry in the screen shot to contain time stamp

2.



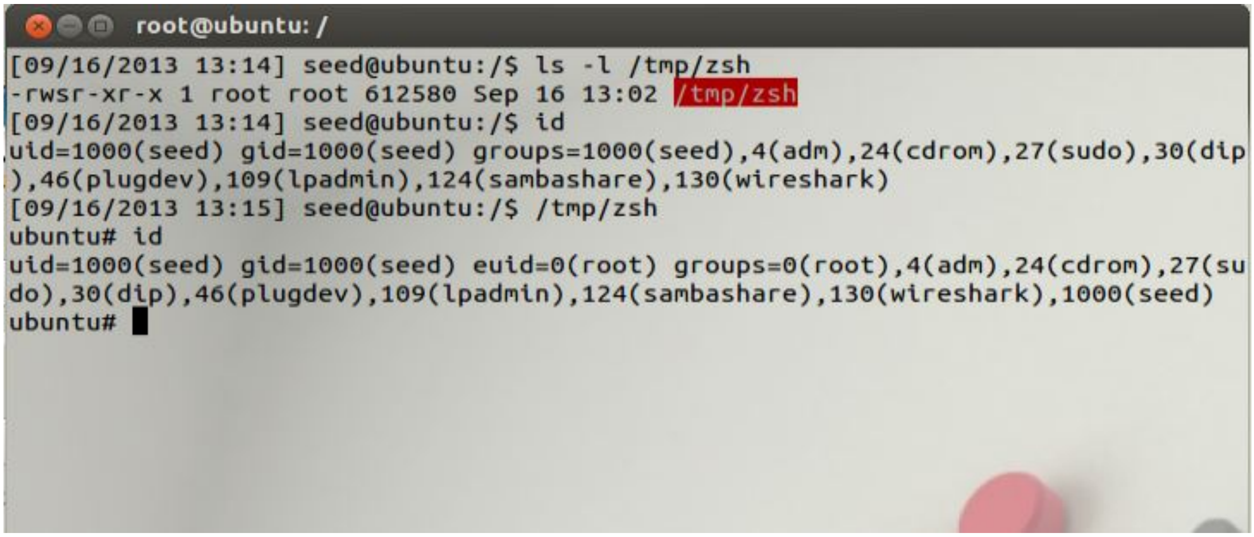
```
[09/16/2013 13:14] seed@ubuntu:/$ ls -l /tmp/zsh
-rwsr-xr-x 1 root root 612580 Sep 16 13:02 /tmp/zsh
[09/16/2013 13:14] seed@ubuntu:/$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[09/16/2013 13:15] seed@ubuntu:/$ /tmp/zsh
ubuntu# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=0(root),4(adm),24(cdrom),27(su
do),30(dip),46(plugdev),109(lpadmin),124(sambashare),130(wireshark),1000(seed)
ubuntu# 
```



```
root@ubuntu:/# cp /bin/bash /tmp
root@ubuntu:/# chmod 4755 /tmp/bash
root@ubuntu:/# exit
exit
[09/16/2013 13:18] seed@ubuntu:/$ ls -l /tmp/bash
-rwsr-xr-x 1 root root 920788 Sep 16 13:18 /tmp/bash
[09/16/2013 13:18] seed@ubuntu:/$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[09/16/2013 13:18] seed@ubuntu:/$ /tmp/bash
bash-4.2$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
bash-4.2$ 
```

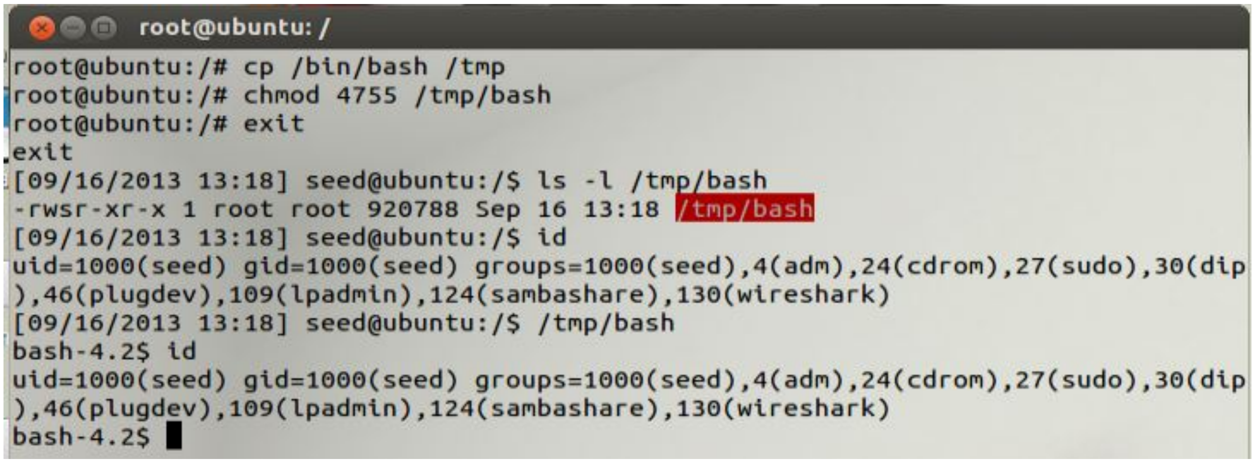
Without any description and explanation, you will lose most of the points.

3.



```
[09/16/2013 13:14] seed@ubuntu:/$ ls -l /tmp/zsh
-rwsr-xr-x 1 root root 612580 Sep 16 13:02 /tmp/zsh
[09/16/2013 13:14] seed@ubuntu:/$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[09/16/2013 13:15] seed@ubuntu:/$ /tmp/zsh
ubuntu# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=0(root),4(adm),24(cdrom),27(su
do),30(dip),46(plugdev),109(lpadmin),124(sambashare),130(wireshark),1000(seed)
ubuntu# 
```

In zsh, the attack works, and you gain the root privilege.



```
root@ubuntu:/# cp /bin/bash /tmp
root@ubuntu:/# chmod 4755 /tmp/bash
root@ubuntu:/# exit
exit
[09/16/2013 13:18] seed@ubuntu:/$ ls -l /tmp/bash
-rwsr-xr-x 1 root root 920788 Sep 16 13:18 /tmp/bash
[09/16/2013 13:18] seed@ubuntu:/$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[09/16/2013 13:18] seed@ubuntu:/$ /tmp/bash
bash-4.2$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
bash-4.2$ 
```

In bash, the attack fails, and you do not gain root privilege.

Without any explanation, you will still lose most of the points.