



## SECURITY+ LAB SERIES

### Lab 14: Authentication, Authorization and Access Control

Document Version: **2015-09-24**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

## Contents

Introduction .....	3
Lab Topology .....	4
Lab Settings .....	5
Pre-Lab Setup .....	6
1 Adding Groups, Users and Passwords .....	7
1.1 Adding Groups, Users and Passwords on a Linux System .....	7
2 Symbolic Permissions .....	11
2.1 Using Symbolic Permissions .....	11
3 Absolute Permission .....	16
3.1 Using Absolute Permissions .....	16



## Introduction

The material in this lab aligns to the following learning objectives:

- **Objective 5.2:** Given a scenario, select the appropriate authentication, authorization or access control
- **Objective 5.3:** Install and configure security controls when performing account management, based on best practices

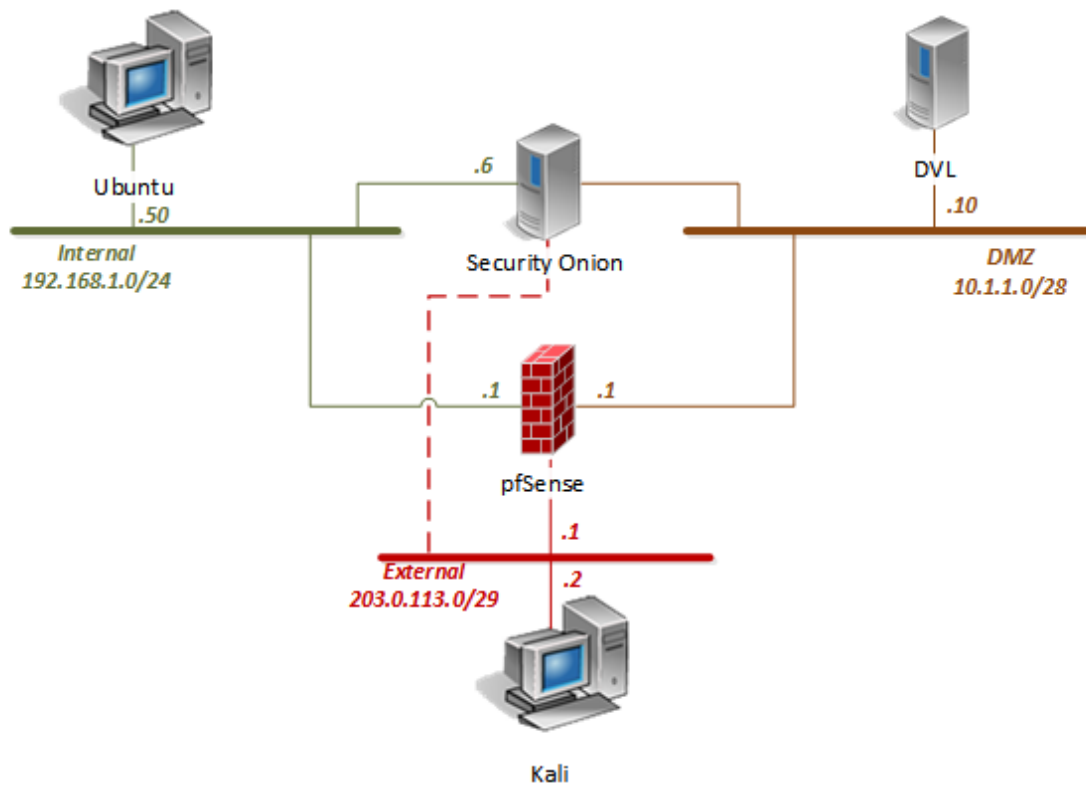
More information about individual objectives and their sections can be found in CompTIA document SY0-401, which is available from the CompTIA website.

In this lab, you will be conducting host security practices using the Linux command line. You will be performing the following tasks:

1. Adding Groups, Users and Passwords
2. Symbolic Permissions
3. Absolute Permissions



## Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Ubuntu	192.168.1.50	student	securepassword
DVL Server	10.1.1.10	root	toor
Security Onion	192.168.1.6	soadmin	mypassword
pfSense	192.168.1.1 10.1.1.1 203.0.113.1	admin	pfsense
Kali	203.0.113.2	root	toor



## Pre-Lab Setup

Before continuing to Task 1, log into the following systems below as instructed.

### I. Ubuntu

1. On the login screen, select the **student** account.
2. When prompted for the password, type **securepassword**. Press **Enter**.
3. Minimize the *PC viewer* window.



## 1 Adding Groups, Users and Passwords

### 1.1 Adding Groups, Users and Passwords on a Linux System

1. Open the **Ubuntu PC Viewer**. If closed, click on the **Ubuntu** icon on the *Topology* page.



2. Open a new **Terminal** window by clicking on the **Terminal** icon located on the left menu pane.



3. Escalate privileges to the *root* level by typing the command below followed by pressing **Enter**.

```
sudo su
```

```
student@Ubuntu:~$ sudo su  
[sudo] password for student:  
root@Ubuntu: /home/student#
```

4. When prompted for a password, enter **securepassword**.
5. Add a new group named **HR**.

```
groupadd HR
```

```
root@Ubuntu: /home/student# groupadd HR  
root@Ubuntu: /home/student#
```

6. Verify the new group has been added to the group file list.

```
cat /etc/group
```

```
root@Ubuntu:/home/student# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:student
arpwatch:x:126:
telnetd:x:125:
ntp:x:127:
postfix:x:128:
postdrop:x:129:
HR:x:1002:
```

The new group *HR* will be added to the bottom of the */etc/group* file with a group ID of 1002.

7. Add a new user named **jenny**.

```
adduser jenny
```

- a. When prompted for a new password, type **lasocial**. Press **Enter**.
- b. When prompted again, type **lasocial**. Press **Enter**.
- c. When prompted for a full name, type **Jenny**. Press **Enter**.
- d. For the rest of the configurations, press **Enter** until when asked is the information correct.
- e. Type **Y** for yes and press **Enter**.

```
root@Ubuntu:/home/student# adduser jenny
Adding user `jenny' ...
Adding new group `jenny' (1003) ...
Adding new user `jenny' (1003) with group `jenny' ...
Creating home directory `/home/jenny' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for jenny
Enter the new value, or press ENTER for the default
  Full Name []: Jenny
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
```



8. Place the user **jenny** in the newly created **HR** group.

```
usermod -G HR jenny
```

```
root@Ubuntu:/home/student# usermod -G HR jenny
root@Ubuntu:/home/student#
```

9. Add another new user named **joe**.

```
adduser joe
```

- When prompted for a new password, type **tooth**. Press **Enter**.
- When prompted again, type **tooth**. Press **Enter**.
- When prompted for a full name, type **Joe**. Press **Enter**.
- For the rest of the configurations, press **Enter** until when asked is the information correct.
- Type **Y** for yes and press **Enter**.

```
root@Ubuntu:/home/student# adduser joe
Adding user `joe' ...
Adding new group `joe' (1004) ...
Adding new user `joe' (1004) with group `joe' ...
Creating home directory `/home/joe' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for joe
Enter the new value, or press ENTER for the default
  Full Name []: Joe
   Room Number []:
   Work Phone []:
   Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
```

10. Place the user **joe** in the **HR** group.

```
usermod -G HR joe
```

```
root@Ubuntu:/home/student# usermod -G HR joe
root@Ubuntu:/home/student#
```

11. Verify the newly created users in the **passwd** file.

```
cat /etc/passwd
```

```
root@Ubuntu:/home/student# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
telnetd:x:118:125::/nonexistent:/bin/false
ntp:x:120:127::/home/ntp:/bin/false
postfix:x:121:128::/var/spool/postfix:/bin/false
jenny:x:1003:1003:jenny:/home/jenny:/bin/bash
joe:x:1004:1004:Joe,,,:/home/joe:/bin/bash
```

12. View the created users in the **shadow** file.

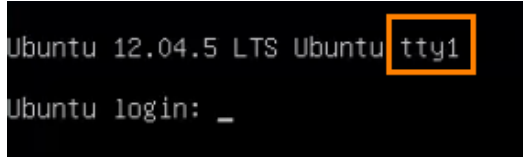
```
cat /etc/shadow
```

```
root@$6$qc1v2oIS$wwFIAZ7dGZRQpCFr8w8Lma/JtB8UPyi
:16507:0:99999:7:::
daemon:*:16289:0:99999:7:::
bin:*:16289:0:99999:7:::
sys:*:16289:0:99999:7:::
ntp:*:16289:0:99999:7:::
postfix:*:16486:0:99999:7:::
jenny:$6$KTvxwWAD$b7JG8986wW4FKDNjSwLfVY/Kihfs
/:16545:0:99999:7:::
joe:$6$l6GeU9wU$CworWf8UJIphVFUCsH4D9qsBWmNdoA
16545:0:99999:7:::
```

## 2 Symbolic Permissions

### 2.1 Using Symbolic Permissions

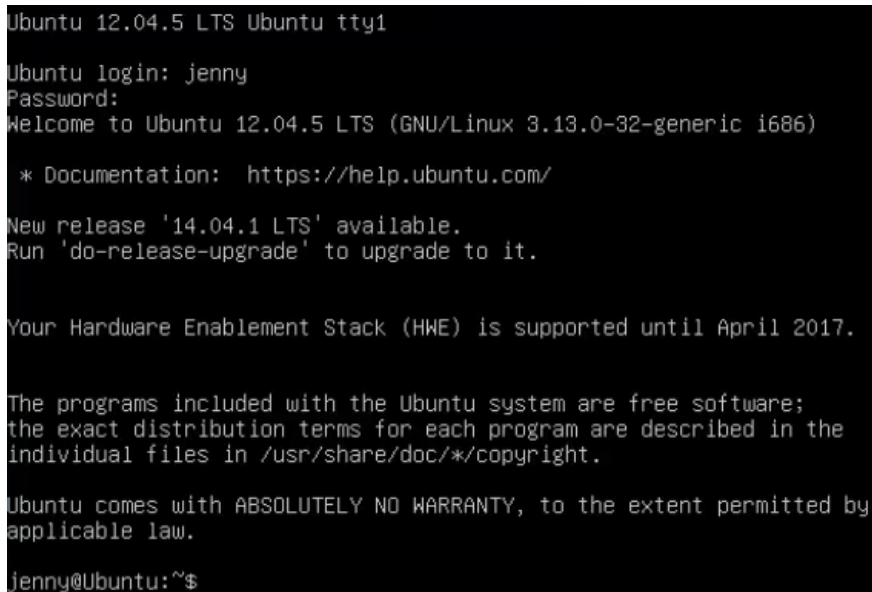
1. While on the *Ubuntu* system, press and hold the keys **CTRL+ALT+F1** until the screen changes to the *tty1 Terminal*.



```
Ubuntu 12.04.5 LTS Ubuntu tty1
Ubuntu login: _
```

When attempting to switch to the *tty1* Terminal, make sure to engage within the *PC Viewer*, otherwise it may not switch the console properly.

2. Once on the *Terminal* login screen, type **jenny** and press **Enter**.
3. When prompted for the password, type **lasocial** and press **Enter**.
4. After a successful login, you will see the *jenny@Ubuntu:~\$* prompt.



```
Ubuntu 12.04.5 LTS Ubuntu tty1
Ubuntu login: jenny
Password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

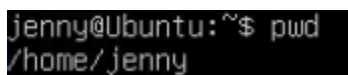
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jenny@Ubuntu:~$
```

Since we are not logged in as the *root* (*superuser*), we are presented with the dollar sign instead of the *#* if we were to be logged in as the user *root*.

5. View your present directory.

```
pwd
```



```
jenny@Ubuntu:~$ pwd
/home/jenny
```

6. Go back one directory level to the **/home** directory.

```
cd ..
```

```
jenny@Ubuntu:~$ cd ..
jenny@Ubuntu:/home$ _
```



7. List all directories and their permissions.

```
ls -l
```

```
jenny@Ubuntu:/home$ ls -l
total 16
drwxr-xr-x 3 jenny jenny 4096 Apr 20 14:32 Jenny
drwxr-xr-x 2 joe joe 4096 Apr 20 14:30 Joe
drwxr-xr-x 2 root root 4096 Apr 6 17:09 scripts
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
jenny@Ubuntu:/home$
```

The Linux operating system has a total of 10 letters or dashes in the permissions fields:

- The first field is a dash for a file and a d for a directory
- The 2<sup>nd</sup> through 4<sup>th</sup> fields are for the user
- The 5<sup>th</sup> through 7<sup>th</sup> fields are for the group
- The 8<sup>th</sup> through 10<sup>th</sup> fields are for others (accounts other than those in the group)

```
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
```

1st field

2nd - 4th fields (user)

5th - 7th fields (group)

8th - 10th fields (other)

8. Enter *Joe's folder* as Jenny by typing the command below.

```
cd joe
```

```
jenny@Ubuntu:/home$ cd joe
jenny@Ubuntu:/home/joe$ _
```

Notice that we are able to go into *Joe's home folder*.

9. Change back up one directory level.

```
cd ..
```

```
jenny@Ubuntu:/home/joe$ cd ..  
jenny@Ubuntu:/home$
```

10. Press and hold **CTRL+ALT+F2** to switch to another *Terminal* session (**tty2**).

```
Ubuntu 12.04.5 LTS Ubuntu tty2  
Ubuntu login:
```

11. Login as the user **root** with the password **securepassword**.

```
Ubuntu 12.04.5 LTS Ubuntu tty2  
  
Ubuntu login: root  
Password:  
Last login: Fri Mar 13 15:13:53 EDT 2015 from 203.0.113.2 on pts/3  
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)  
  
 * Documentation:  https://help.ubuntu.com/  
  
New release '14.04.1 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Your Hardware Enablement Stack (HWE) is supported until April 2017.
```

12. Change to the **/home** directory.

```
cd /home
```

```
root@Ubuntu:~# cd /home  
root@Ubuntu:/home# _
```

13. List all current directories with their permissions.

```
ls -l
```

```
root@Ubuntu:/home# ls -l
total 16
drwxr-xr-x  3 jenny  jenny  4096 Apr 20 14:32 jenny
drwxr-xr-x  2 joe    joe    4096 Apr 20 14:30 joe
drwxr-xr-x  2 root   root   4096 Apr  6 17:09 scripts
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
root@Ubuntu:/home# _
```

Take note of the “*other*” field for Joe’s folder, notice that it is currently set with an x, which makes it available to execute for “*other*” users.

14. Change the “*other*” permission on joe’s folder by making it *non-executable*.

```
chmod o-x joe
```

```
root@Ubuntu:/home# chmod o-x joe
root@Ubuntu:/home#
```



15. List the directories once more with their respective permissions.

```
ls -l
```

```
root@Ubuntu:/home# ls -l
total 16
drwxr-xr-x  3 jenny  jenny  4096 Apr 20 14:32 jenny
drwxr-xr--  2 joe    joe    4096 Apr 20 14:30 joe
drwxr-xr-x  2 root   root   4096 Apr  6 17:09 scripts
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
root@Ubuntu:/home#
```

Notice now that there are two dashes in the “*others*” field for joe’s folder.

16. Press and hold **CTRL+ALT+F1** to switch back to the other *Terminal* session (tty1).  
Make sure you are viewing the following command prompt:  
**jenny@Ubuntu:/home\$**.

17. Now that we switched to jenny's *Terminal* session, attempt to go into joe's folder once more.

```
cd joe
```

```
jenny@Ubuntu:/home$ cd joe
-bash: cd: joe: Permission denied
jenny@Ubuntu:/home$ _
```

Notice that we do not have the permissions to do so.

The chart below shows examples of other ways the *chmod* command can be used:

chmod command	Results
chmod u+rwx	Adds read, write and execute permissions for the user
chmod u+rw	Adds read and write permission for the user
chmod o+r	Adds read permission for others
chmod g-rwx	Removes read, write and execute permissions for the group

18. Type **exit** followed by pressing **Enter** to logout of the *Terminal* session.

```
jenny@Ubuntu:/home$ exit
logout
_
```

### 3 Absolute Permission

#### 3.1 Using Absolute Permissions

1. Login as the user **joe** with the password as **tooth** while on *tty1*.

```
Ubuntu 12.04.5 LTS Ubuntu tty1
Ubuntu login: joe
Password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

The programs included with the Ubuntu system are free software;  I
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

2. Print your current working directory.

```
pwd
```

```
joe@Ubuntu:~$ pwd
/home/joe
joe@Ubuntu:~$ _
```

3. Go back one directory level to the */home* directory.

```
cd ..
```

```
joe@Ubuntu:~$ cd ..
joe@Ubuntu:/home$ _
```



## 4. List all directories and their permissions in the current working directory.

```
ls -l
```

```
joe@Ubuntu:/home$ ls -l
total 16
drwxr-xr-x  3 jenny  jenny  4096 Apr 20 14:34 jenny
drwxr-xr--  3 joe    joe    4096 Apr 20 14:34 joe
drwxr-xr-x  2 root   root   4096 Apr  6 17:09 scripts
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
joe@Ubuntu:/home$
```

Notice that Joe's folder is set so that "others" are not able to access the folder.

The other way of assigning permissions besides using symbolic permissions is the use of absolute permissions. Absolute permissions use a three digit octal number to represent the permissions for owner, group and other.

The table below outlines each absolute value and its corresponding permissions:

Number	Permissions
7	Read, Write and Execute
6	Read and Write
5	Read and Execute
4	Read
3	Write and Execute
2	Write
1	Execute
0	None

By typing the command, *chmod 764 <examplefile>*, the examplefile will be assigned the follow permissions:

- The user will get Read, Write and Execute permissions
- The group will get Read and Write permissions
- Others will get Read Access

Breakdown of how 764 represents these permissions:

Digit	Binary Equivalent	Permission
7 (user)	111	1-Read 1-Write 1-Execute
6 (group)	110	1-Read 1-Write 0-No Execute
4 (others)	100	1-Read 0-No Write 0-No Execute

5. Modify the “others” field for Joe’s folder so that others will be able read and execute but not write while still maintaining the “user” field to read, write, and execute.

```
chmod 705 joe
```

```
joe@Ubuntu:/home$ chmod 705 joe
joe@Ubuntu:/home$
```



6. List the file permissions of the current directory to see that the absolute changes were made.

```
ls -l
```

```
joe@Ubuntu:/home$ ls -l
total 16
drwxr-xr-x 3 jenny jenny 4096 Apr 20 14:34 jenny
drwx--r-x 3 joe joe 4096 Apr 20 14:36 joe
drwxr-xr-x 2 root root 4096 Apr 6 17:09 scripts
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
joe@Ubuntu:/home$ _
```

7. Change to the */home/joe* directory.

```
cd joe
```

```
joe@Ubuntu:/home$ cd joe
joe@Ubuntu:~$ _
```

8. Create a simple text file named **test.txt** using *nano*.

```
touch test.txt
```

```
joe@Ubuntu:~$ touch test.txt
joe@Ubuntu:~$
```

9. Type **exit** followed by pressing **Enter** to log out of Joe's session.  
 10. While on the *tty1 Terminal*, log back in as **jenny** and enter the password **lasocial**. Press **Enter**.

```
Ubuntu 12.04.5 LTS Ubuntu tty1
Ubuntu login: jenny
Password:
```

11. Change to the **/home** directory.

```
cd /home
```

```
jenny@Ubuntu:~$ cd /home
jenny@Ubuntu:/home$ _
```

12. List all directories with their respective permissions.

```
ls -l
```

```
jenny@Ubuntu:/home$ ls -l
total 16
drwxr-xr-x  3 jenny  jenny  4096 Apr 20 14:34 jenny
drwx---r-x  3 joe    joe    4096 Apr 20 14:36 joe
drwxr-xr-x  2 root   root   4096 Apr  6 17:09 scripts
drwxr-xr-x 31 student student 4096 Apr 20 14:28 student
jenny@Ubuntu:/home$
```

13. Change to the **/home/joe** directory.

```
cd /home/joe
```

```
jenny@Ubuntu:/home$ cd joe
jenny@Ubuntu:/home/joe$
```

## 14. List all files in the current directory.

```
ls -l
```

```
jenny@Ubuntu:/home/joe$ ls -l
total 12
-rw-r--r-- 1 joe joe 8445 Apr 20 14:30 examples.desktop
-rw-rw-r-- 1 joe joe   0 Apr 20 14:36 test.txt
jenny@Ubuntu:/home/joe$ _
```

Notice that we are able to enter Joe's folder and read the files within the directory. We are able to see the *test.txt* file.

## 15. Attempt to create a file.

```
touch jenny.txt
```

```
jenny@Ubuntu:/home/joe$ touch jenny.txt
touch: cannot touch `jenny.txt': Permission denied
jenny@Ubuntu:/home/joe$
```

Notice we do not have permission to create the file.

16. **Close** all remaining windows.