INFO6003 Lab-09 Linux-Security-01

Preparation

If you haven't already, download a Ubuntu for the course or use the Ubuntu from the beginning of semester.

Create a VM

- Use the **New Virtual Machine Wizard** to create the VM
  - Choose the **Typical** option
  - Make sure you have a working network connection for the install
  - Use the ISO you downloaded as the installer disc (this is not a 7Zip file)

VM Details Needed During Install:

- Full Name: **First Name, Last Name**
- Username: **FOLusername-01**
- Password: **Ubuntu1**
- VM Name: **INFO6003_Ubuntu**

Note: This is the username and password you will use to login to the Ubuntu-Server.

- Hard Disk: leave the size at the 20 GB default and **store it as a single file**.

The install is completely automated from this point on. If you are asked for any more information you have done something wrong.

- Once the VM has rebooted, shut it down via VMware and move it to the host-only network. If you didn't re-enable DHCP last week, you aren't going to get an address.
- **Errors:** You can say no to both the prompts VMware generates when you power the VM back on.
- Use **ifconfig** to confirm you have a network address

The Real Super User - Root

- Login using your username and password then record which directory you are in by using the following command:

FOLusername-01@ubuntu:~$ **pwd**

Many newer Linux distributions by default do not allow direct access to the root user. To gain access to the account, a user who has sudo privileges must assign a password to the root account. During the default install you were given sudo privileges.

FOLusername-01@ubuntu:~$ **sudo passwd root**

- Make the password **Ubuntu1** for simplicity. Once the root account has a password, we can switch to using that account by issuing the following command.

FOLusername-01@ubuntu:~$ **su -**

The dash option after the **su** command will cause the system to run all the root logon scripts to give you true root privileges. Which directory are you in now? Notice also that the command prompt changes to let us know we have become root. What changes to the prompt can you see?

- Change the hostname of your machine to **FOLusername** using **vi**

root@ubuntu:~# **vi /etc/hostname (VI commands below)**

VI Commands:
dd to delete the line you are on (lower case d twice)
i to get into insert mode (lower case i)
ESC to get into command mode (escape key)
:wq to write your changes to the file system and quit (colon, lower case w, lower case q)

- **Restart you VM** with the **init 6** command, then **login with the root account**. Make sure the hostname has changed.

root@FOLusername:~#

Creating Users

- Create the users below with the adduser command.
- Give them the **password Ubuntu1**. (accept all the empty defaults and type Y for yes)

root@FOLusername:~#**adduser student-01**
root@FOLusername:~#**adduser student-02**
root@FOLusername:~#**adduser FOLusername-02**

SUID/GUID bits

- Logout with the logout command.
- Login as **student-01** and print the working directory to show you where you are in the file system.
- Make a new directory named test.

student-01@FOLusername:~$ **mkdir test**

- Change your location to the test directory and create a file named **file-01** using the touch command. (cd test to change directory)

student-01@FOLusername:~/test$ **touch file-01**

- View the permissions on file-01 with the **ls -ail** command and record them in your notes.
- Use the **umask** command to see what student-01's umask is.
- Assign SUID privileges to file-01 with the following command.

student-01@FOLusername:~/test$ **chmod 4664 file-01**

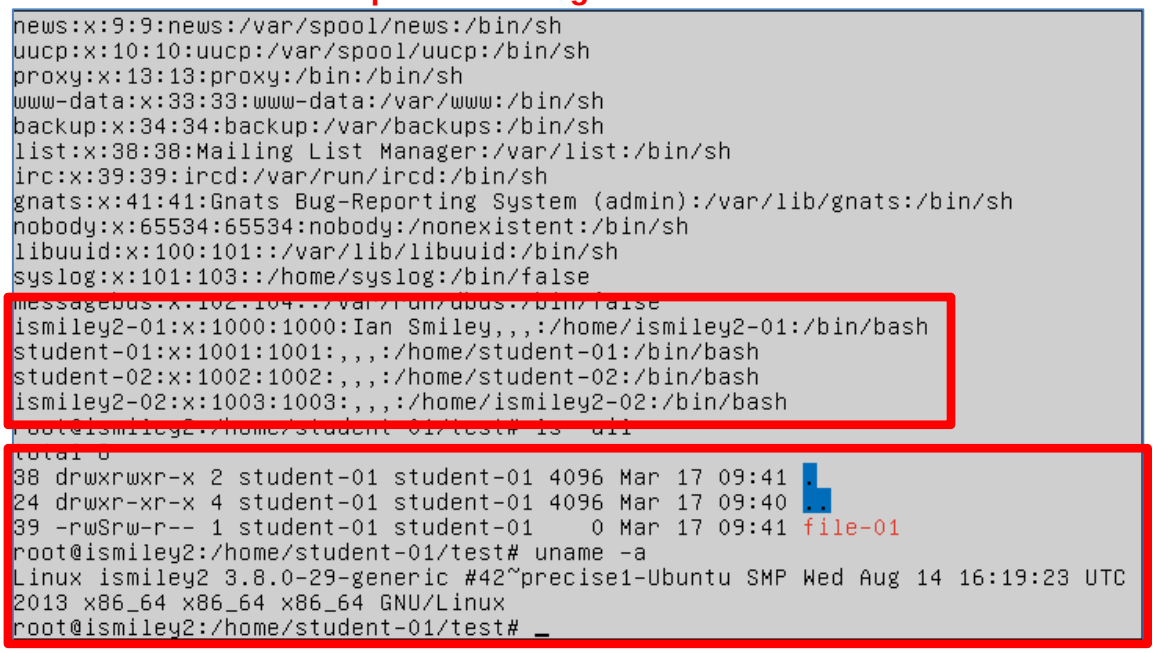
- Note: you could also use the chmod u+s file-01 command to accomplish this task

- **Switch to the root user and navigate back to the test directory for student-01**.
  - **/home/student-01/test**

- Type the following commands to get the first screenshot.

cat /etc/passwd
ls -ail
uname -a

Slide 1: take a screen capture showing the information below



Note the **S** where execute (x) permission is normally shown.
Why is this a capital S instead of a small s?

- To remove the permissions we can use chmod again.

root@FOLusername:/home/student-01/test# **chmod 664 file-01**

- Note: you could also use the chmod u-s file-01 command
- To set both suid & guid in one command we can use the octal form of the permissions.

root@FOLusername:/home/student-01/test# **chmod 6664 file-01**

The first **6** gives both suid & guid permissions to file-01 and 644 gives user rw, group rw, and other r.

Note: In this version of Linux the files that are highlighted in red indicate if the suid special permission is set.

Sticky Bit

- As root, create a directory named **ShareAll** in the **/** directory (not **/root**, but **/**).
- Add all permissions to the directory, so that all users can use the directory and change other user's files.

chmod 777 ShareAll

- View the permissions on the directory, then **cd into the ShareAll** directory and create a file named root-01

touch root-01 **(**View the permissions on the file)

- Use the **umask** command to see what root's umask is.
- **As student-01** create a file named **student-01** in the **ShareAll** directory.

touch student-01

- **Logon as FOLusername-01** then create a file named **yourlastname** in the **ShareAll** directory.

touch yourlastname

- View the permissions of the three files.

ls -ail

- Try to remove the root-01 file with the following commands. **(Leave the output onscreen for the next screenshot)**

rm root-01
y

- Even though there is a warning because you only have read access to the file, you can still remove the file because you have rwx to the directory.

ls -ail

Slide 2: take a screen capture showing the information below

```
ismiley2-01@ismiley2:/ShareAll$ ls -ail
total 8
262145 drwxrwxrwx  2 root        root        4096 Mar 17 10:05 .
     2 drwxr-xr-x 24 root        root        4096 Mar 17 10:05 ..
262240 -rw-r--r--  1 root        root           0 Mar 17 10:05 root-01
262239 -rw-rw-r--  1 ismiley2-01 ismiley2-01    0 Mar 17 10:03 smiley
262224 -rw-rw-r--  1 student-01  student-01     0 Mar 17 10:02 student-01
ismiley2-01@ismiley2:/ShareAll$ rm root-01
rm: remove write-protected regular empty file `root-01'? y
ismiley2-01@ismiley2:/ShareAll$ ls -ail
total 8
262145 drwxrwxrwx  2 root        root        4096 Mar 17 10:06 .
     2 drwxr-xr-x 24 root        root        4096 Mar 17 10:05 ..
262239 -rw-rw-r--  1 ismiley2-01 ismiley2-01    0 Mar 17 10:03 smiley
262224 -rw-rw-r--  1 student-01  student-01     0 Mar 17 10:02 student-01
ismiley2-01@ismiley2:/ShareAll$ _
```

- **Switch to the root** user, go to the **/** directory and add the sticky bit to the **ShareAll** directory.

chmod 1777 /ShareAll

- View the permissions on the directory. The **t** has now been added to denote the sticky bit. Also note the permissions on the tmp directory. Why does that make sense?

- Go into the ShareAll directory **as root** and try to remove the student-01 file.

rm student-01

Even though the sticky bit has been added, the root user still has control over *all* the files in the directory!

- **Recreate the root-01** file then log out of the system completely. (touch root-01)
- Log back in as **student-01** and try to remove the **yourlastname** file located in **/ShareAll**.

What happened?
Was permission granted?

File Attributes – The Immutable Attribute

- Switch to the root user. Then in the ShareAll directory, add the immutable attribute to the file root-01.

root@FOLusername:/ShareAll# **chattr +i root-01**

- Use the **lsattr** command to view the attributes assigned to the file.
- As root**, try to remove the root-01** file.

What happened? Was permission granted?

- As root in the ShareAll directory, perform the following commands in order:

clear
ls -ail
rm root-01
uname -a

Slide 3: take a screen capture showing the information below

```
root@ismiley2:/ShareAll# ls -ail
total 8
262145 drwxrwxrwt  2 root        root        4096 Mar 17 10:12 .
     2 drwxr-xr-x 24 root        root        4096 Mar 17 10:05 ..
262224 -rw-r--r--  1 root        root           0 Mar 17 10:12 root-01
262239 -rw-rw-r--  1 ismiley2-01 ismiley2-01    0 Mar 17 10:03 smiley
root@ismiley2:/ShareAll# rm root-01
rm: cannot remove `root-01': Operation not permitted
root@ismiley2:/ShareAll# uname -a
Linux ismiley2 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC
2013 x86_64 x86_64 x86_64 GNU/Linux
root@ismiley2:/ShareAll# _
```

User Password Encryption

The PAM daemon can be used to change the cryptographic method used to store the password in the /etc/shadow directory.

- **As root, change into the /etc/pam.d** directory and look at the contents of the common-password file with the command below.

nano common-password

Note that most of the lines will start with a # which means this line is a comment and is not executed by the PAM daemon.

- Find the following line:

password [success=1 default=ignore] pam_unix.so obscure sha512

The entry **sha512** can be changed to a different hash or encryption method.

- Using the nano editor, change the entry in the above line from **sha512** to **md5** and save the file.
  - **Ctrl-X, Yes, Enter to save the file**.

Any new password entered will now use the MD5 hash algorithm to store the password.

- Create a new user named **student-03** with a password of **Ubuntu1**

adduser student-03 **(**Accept the defaults when creating the user)

- View the password hash in the /etc/shadow file with the following command: **cat /etc/shadow**

Note the entry following student-03 starts with **1** these symbols indicate MD5 was the hash algorithm. Also note that although FOLusername-02, student-01 and student-02 have the same password, their password hashes are all different. This is because a salt is added when creating the password.

- Edit the common-password file again and change the hash method to **sha256**
  - **Ctrl-x, Yes, Enter to save the file.**

- Create a new user named **student-04** with a password of **Ubuntu1**
- View the shadow file.

Note the entry following student-04 starts with **5** and the hash is now larger than the hash for user student-03

- As root in the **/etc/pam.d** directory, enter the following commands in order:

clear
cat common-password | grep success=
cd ..
cat shadow | grep student-03
cat shadow | grep student-04
uname -a

Slide 4: take a screen capture showing the information below

```
root@ismiley2:/etc/pam.d# cat common-password | grep success=
password        [success=1 default=ignore]      pam_unix.so obscure sha256
root@ismiley2:/etc/pam.d# cd ..
root@ismiley2:/etc# cat shadow | grep student-03
student-03:$1$lDh.PZEc$ZX9yjPCAq7MXE.G7DNI5m0:16511:0:99999:7:::
root@ismiley2:/etc# cat shadow | grep student-04
student-04:$5$nLHVD9Ck$1JaYTkxoGk4w6uxAoEimt4ly88J9TyS.t1jF0T.I3X.:16511:0:99999
:7:::
root@ismiley2:/etc# uname -a
Linux ismiley2 3.8.0-29-generic #42~precise1-Ubuntu SMP Wed Aug 14 16:19:23 UTC
2013 x86_64 x86_64 x86_64 GNU/Linux
root@ismiley2:/etc# _
```

Shutdown your VM and take a snapshot called After_Lab-09