COSC 3364 – Principles of Cybersecurity

Lab 06

Discretionary Access Control

Groups

**What Are Groups Used For?**

* Being a member of a group allows special access to system resources
* Group membership can also be used to prevent access to system resources

**Primary and Secondary Groups**

* *Primary group*: Main group user belongs to
* *Secondary groups*: Other groups that user belongs to

**Getting a User’s Group Information**

* Use the id command to see what groups a user belongs to
  + Interpreting the results:
    - uid=1002(student): User ID and user name
    - gid=1002(student): Primary user group ID and group name
    - groups=1002(student,60(games),1001(ocs): Secondary group IDs and group names
* Use the group command to list all the groups the user is a member of
  + The primary group is always listed first

**Making Changes to Groups**

* Change group ownership of a file to another group: chgrp
  + Example: chgrp games sample.txt

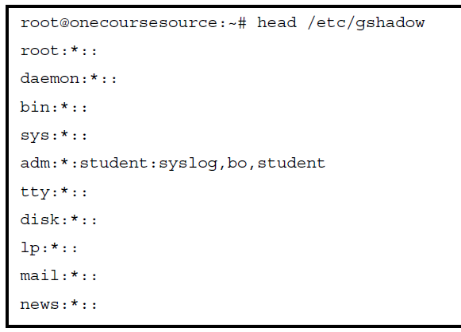
**Modifying Group Information**

* /etc/passwd
  + Defines the user’s primary group membership
  + Uses the GID of the group
* /etc/group
  + Stores information about each group, including group name, GID, and secondary user membership
* /etc/gshadow
  + Stores additional information about the group, including group administrators and the group password

**Special Groups**

* Have GID values under 1000
* root: system administrator only
* adm: users who can access files related to system monitoring such as log files
* lp, tty, mail, cdrom: used by the OS for background processes to access files
* sudo (super user do): used with the sudo command

**User Private Groups**

* Each user has his or her own private group
* ****This group is usually their primary group

**The /etc/gshadow File**

* Contains group information
* Viewable only by the root user
* Each line describes one group
* Each line is separated into fields of data using **:** as the field separator

**Creating and Modifying Groups**

* Creating groups
  + groupadd command
  + Example: groupadd -g 5000 payroll
  + The -g option assigns the GID to the group (in this case 5000)
* Modifying groups
  + groupmod command
  + Example: groupmod -n payables payroll to change the name of the group from payables to payroll

**Deleting Groups**

* Use the groupdel command
* First, search the filesystem for all files owned by the group and change their ownerships to another group
* If this step isn’t taken, the files owned by the deleted group end up just being owned by the GID of the group, which makes the group permission worthless

**Adding Users to Groups**

* Use the usermod command with the -G option
  + Example: usermod -G adm student
  + Warning: this option will override existing group membership
* To add a user to a group while keeping the current group membership, add the -a option
  + Example: usermod -G adm -a student

**Group Administrators**

* To allow a user to manage a group, add them as a group administrator with the -A option of the gpasswd command
  + Example: gpasswd -A student games
* Then the user can add users to the group with the -a option
  + Example: gpasswd -a bo games
* To remove a user, use the -d option
  + Example: gpasswd -d bo games

Users

**Importance of User Accounts**

* Granting system access
* Securing files and directories
* Security processes
* Additional privileges
* Additional authentication

**User Account Information Storage**

* Local user account information
  + /etc/passwd: primary account data
  + /etc/shadow: passwords and related data
  + /etc/group: group account data
  + /etc/gshadow: group account data
* User accounts can also be provided by network servers

**The /etc/passwd File**

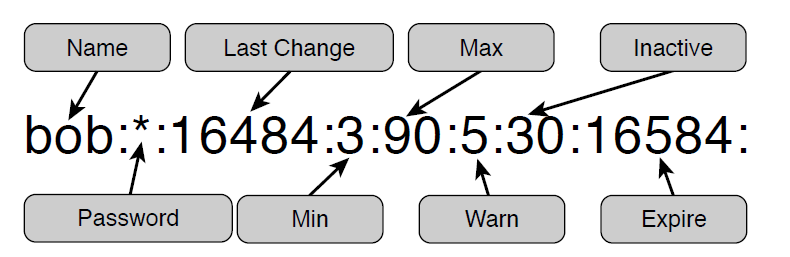
* Despite its name, doesn’t contain password information
* This file is not usually manually modified; commands such as useradd, userdel, and usermod change its contents
* Each line describes one group
* Each line contains fields of data with a **:** as a field separator
* Example line: root:x:0:0:root:/root:/bin/bash
* Example line: root:x:0:0:root:/root:/bin/bash
  + root is the user name
  + x is the password placeholder
  + 0 represents the UID
  + 0 represents the user’s primary group
  + root is a comment field
  + /root is the user’s home directory
  + /bin/bash is the user’s login shell

**Special User Accounts**

* Default accounts, typically with UID values under 1000
* Some default accounts are daemon accounts, used by daemon-based software
* Other accounts provide features to the OS, such as the nobody account
* Some accounts are created when you add new software
* Administrators should be aware of default accounts and their security features or threats

**Default User Account Examples**

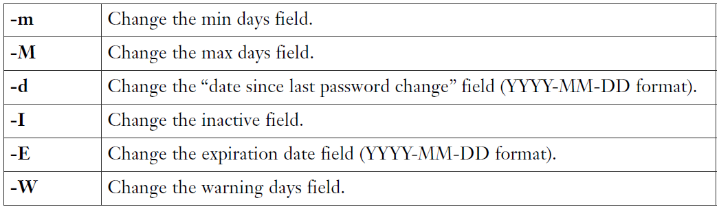
* root: The system administrator account
* syslog: used by the system logging daemon to access files
* lp: one of many users (including mysql, mail, postfix, and dovecot) used by the OS to provide access to specific files by daemons
* bind: used by the software that provides DNS functions

**The /etc/shadow File**

* Contains password data
* Viewable only by the root user
* Each line describes one user’s account’s password information
* Each line is separated into fields with a **:** as a field separator

**Managing User**

* Creating users
  + Use the useradd command
  + Example: useradd timmy
  + -u option can assign a UID to the user
  + New user’s account is locked by default
* **Setting the account password**
  + Use the passwd command
  + Example: passwd timmy
  + You are prompted to enter the new password

**Modifying Users**

* Use the usermod command
* Use options to specify the change to make

**Restricted Shell Accounts**

* Add the -s option to the useradd command and provide an argument of /bin/rbash

Example: useradd -m -s /bin/rbash limited

* Properties of restricted accounts
  + Cannot change directories with the cd command
  + Cannot change the values of these variables: SHELL, PATH, ENV, and BASH\_ENV
  + Cannot run any command that have a pathname that starts with the **/** character
  + Cannot redirect output to a file

**Using su**

* Switches to another user account
  + Example: su - student
* Opens a new shell in which the identity has been switched
* The - option enables you to switch as if you were logging in directly, so that the user’s initialization files are executed
* To use su you must be the root user or you must have the password for the account being switched to
* Use the exit command to close the shell

**Using sudo**

* Executes specific tasks as another user without actually switching to that account
  + Example: sudo apt-get install joe
* Access is configured in /etc/sudoers
* /etc/sudoers should not be modified directly; use the visudo command

**Pluggable Authentication Modules (PAM)**

* Set of libraries that is called by authentication-based software
* Features
  + Can limit access by time or date
  + Can limit system resource utilization after the user logs in
  + Can be applied to specific login commands
  + Can create additional log entries for specific login events
* Primary configuration file, /etc/pam.conf, is rarely used
* Each authentication-based program has a separate configuration file under the /etc/pam.d directory

A screenshot of a computer

Description automatically generated

A diagram of a server

Description automatically generated

A screenshot of a computer screen

Description automatically generated

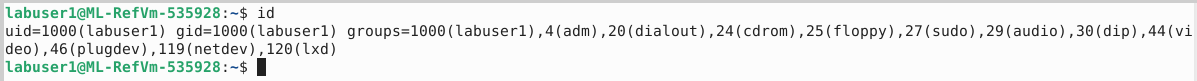
A screenshot of a computer

Description automatically generated

Tasks

Provide screenshots where \* is indicated.

1. **Explore Group and User Information:**
   1. Display default user’s information\*



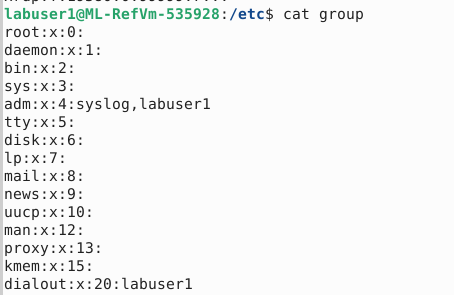
* 1. Display contents of passwd\*



* 1. Display contents of shadow\*

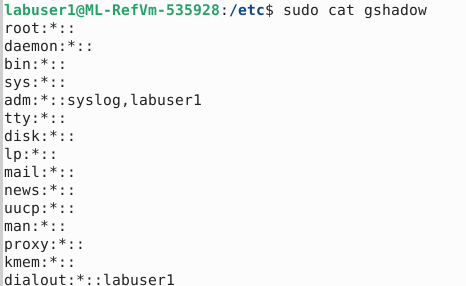


* 1. Display contents of group\*



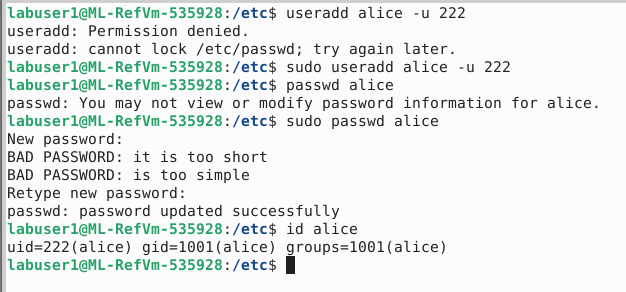
I couldn’t fit all of it in the screenshot.

* 1. Display contents of gshadow\*



I couldn’t fit all of it in the screenshot.

1. **Alice:**
   1. Create user named **alice** with an ID of 222
   2. Set the password of the user account to ‘alice’
   3. Determine the primary group of **alice**\*

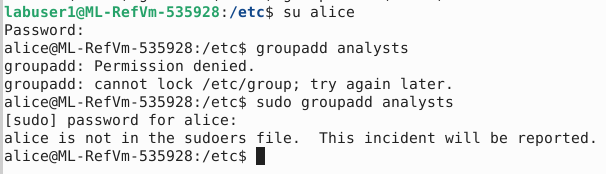


The primary group is alice.

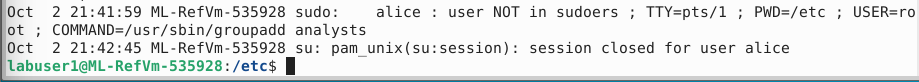
* 1. What is the primary group ID of **alice’s** primary group? How was this generated?

The primary group ID is 1001. This is generated when the user is created and is incremented from the highest group id.

* 1. Switch to user account **alice**
  2. Attempt to create group **analysts**
  3. Attempt to create group **analysts** as super user\*



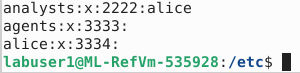
* 1. Return to default user
  2. Display the end of /var/log/auth.log
  3. Locate incident report\*



1. **Analysts and Agents:**
   1. Create group **analysts** with an ID of 2222
   2. Create group **agents** with an ID of 3333
   3. Add **alice** to group **analysts**
   4. Display group information for **alice**\*

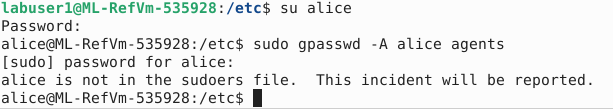


* 1. Delete user account **alice**
  2. Create user account **alice** with an ID of 222 while adding account to **analysts**
  3. Display group information for **alice**\*



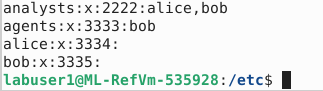
* 1. What is the primary group of ID of **alice’s** primary group? How was this generated?

1. The primary group ID is 3334. This is generated when the user is created and is incremented from the highest group id.
   1. Switch to user account **alice**
   2. Attempt to set **alice** as group administrator of **agents**\*

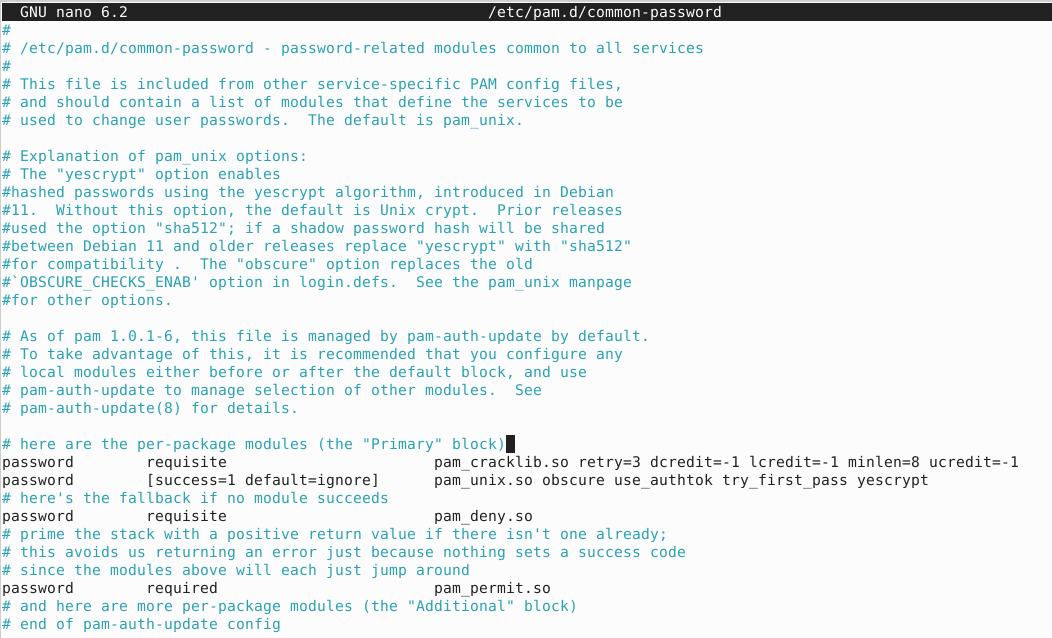


* 1. Return to default user
  2. Set **alice** as group administrator of **agents**

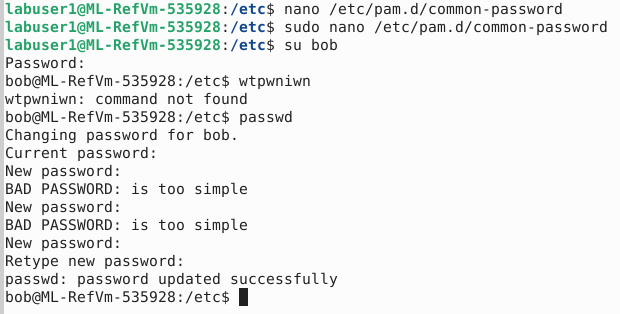
1. **Bob:**
   1. Create user named **bob** with an ID of 333
   2. Set the password of the user account to ‘bob’
   3. Add **bob** to group **analysts** and set as group administrator
   4. Add **bob** to group **agents**
   5. Display contents of group\*



* 1. Open /etc/pam.d/common-password as super user
  2. Update password policy to a minimum length of 8 and must contain an uppercase letter, lowercase letter, and a digit\* (<https://linux.die.net/man/8/pam_cracklib>)

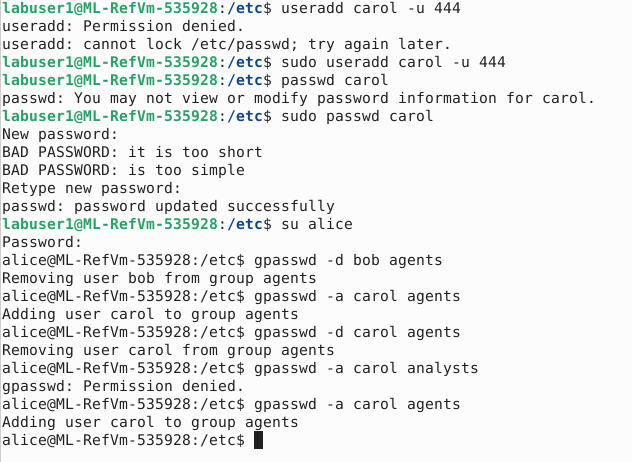


* 1. Switch to user account **bob**
  2. Attempt to set the password of the user account to ‘wtpwniwn’
  3. Set the password of the user account to ‘Wtpw0912’\*



* 1. Return to default user

1. **Carol:**
   1. Create user named **carol** with an ID of 444
   2. Set the password of the user account to ‘carol’
   3. Switch to user account **alice**
   4. Delete **bob** from group **agents**
   5. Attempt to add **carol** to group **analysts**
   6. Add **carol** to group **agents**\*



* 1. Return to default user
  2. Display contents of passwd\*



* 1. Display contents of group\*

