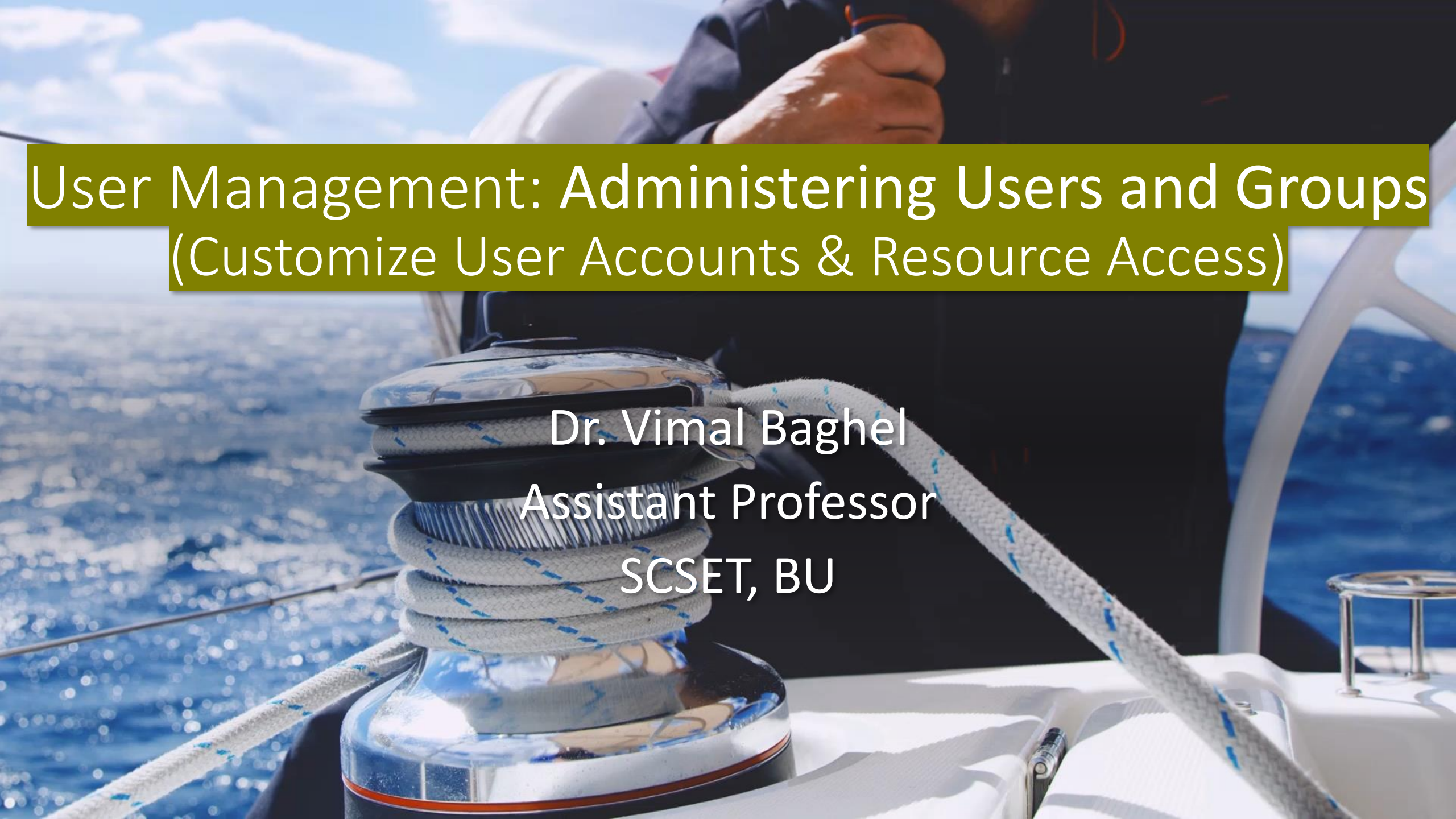


User Management: Administering Users and Groups
(Customize User Accounts & Resource Access)

Dr. Vimal Baghel
Assistant Professor
SCSET, BU

BENNETT UNIVERSITY
THE TIMES GROUP

Outline

- Types of Users on Linux
- User Configuration Files
- Contents of /etc/passwd & /etc/shadow
- User Management Commands
- User Configuration Commands
- User Account Modification Utilities
- Q & A

Objectives

- Manage user accounts.
- Manage group accounts.
- Configure privilege escalation.
- Troubleshoot user and group issues.

BENNETT UNIVERSITY
THE TIMES GROUP

Manage User Accounts

Types of Accounts on Linux

- There are three types of accounts on Linux systems:
  - root,
  - standard user, and
  - service.

USER CONFIGURATION FILES

- **USER ACCOUNT STORAGE**
  - /etc/passwd file stores the actual user account and maintains various settings related to accounts.
  - /etc/shadow file stores password information for the accounts.
  - /etc/profile to set system-wide environment **variables** and startup programs for new user shells.
  - /etc/bashrc to establish system-wide functions and aliases for new user shells.

Contents of /etc/passwd & /etc/shadow

BENNETT UNIVERSITY
TIMES OF INDIA GROUP

/etc/passwd

Field	Content
User Name	The name the user logs into the system with
Password	User password represented as an x; the actual password is stored elsewhere
User ID	Unique number representing the user to the system
Group ID	Unique number representing the user's primary group
Comment	Typically displays the user's full name
Home directory	Absolute path to the user's home directory
Login shell	Absolute path to the user's default shell (usually /bin/bash)

/etc/shadow

Field	Content
User name	The name the user logs into the system with
Password	Hash value of the user's password
Days since last password change	Number of days since the last password change; counted from January 1, 1970
Days before password may be changed	Minimum changeable period, typically set at 1 day
Days before password must be changed	Maximum number of days since the last password change before the password must be changed again; a value of 99999 means the password never needs to be changed, but often set at 90 days
Days until the user is warned to change password	Days before the date the password must be changed that the warning is issued, often set to 7 days
Days after password expires that the account is disabled	Number of days after the password expires until the account is disabled; should be immediate
Days until account expires	Number of days until the account expires and cannot be used
Unused field	Reserved for potential future use

User Configuration Files

BENNETT UNIVERSITY
THE TIMES GROUP

/ect/password file

```
student@ubuntu20:~$ tail /etc/passwd | grep student
student:x:1000:1000:student,,,:/home/student:/bin/bash
student@ubuntu20:~$
```

User Configuration Files

BENNETT UNIVERSITY
THE TIMES GROUP

/etc/shadow file

```
student@ubuntu20:~$ sudo tail /etc/shadow | grep student
student:$6$XYM8.t73X57Xq/NH$IN5RCtXNyaf4RE4yn5.4Tf464W0AR
IQWRGt/UW.U92/qAK2TqjVj5V9WdmUSQSWoMqfFXljRGyflfUxDxeeCf0
:18942:0:99999:7:::
student@ubuntu20:~$
```

Account Management Commands

- `useradd` – create user accounts in the /etc/passwd and /etc/shadow files
- `usermod` – modify existing user accounts
- `userdel` – delete existing user accounts

```
student@ubuntu20:~$ sudo adduser student12
Adding user `student12' ...
Adding new group `student12' (1004) ...
Adding new user `student12' (1004) with group `student12' ...
Creating home directory `/home/student12' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for student12
Enter the new value, or press ENTER for the default
        Full Name []: Student Twelve
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
student@ubuntu20:~$
```

- $useradd –options username
- $usermod –options username
- $userdel username

Options	Purpose
-c	Set the comment value, usually the user's full name
-e	Set an expiration date for the user account, format YYYY-MM-DD
-m	Create a user home directory in /home
-s	Set a default shell for the user
-u	Set a specific user ID value
-D	Display the default settings

The useradd Command

- Options:
  - -c comment (often used for full name)
  - -e expire
  - -D display default settings

```
student@ubuntu20:~$ sudo useradd student10
student@ubuntu20:~$ sudo usermod -c "Student Ten" student10
student@ubuntu20:~$ tail /etc/passwd | grep student10
student10:x:1002:1002:Student Ten:/home/student10:/bin/sh
student@ubuntu20:~$ sudo userdel student10
student@ubuntu20:~$
```

The *passwd* Command

BENNETT UNIVERSITY
THE TIMES GROUP

$ passwd username

Options	Purpose
-d	Delete a password and disable the account
-e	Immediately expire a password, forcing a password change by the user
-l	Lock the account (for example, during a leave of absence)
-u	Unlock a locked account

Key Demonstration: Create User and Set Password

Sign in to at least one system (either RH or Debian-based) and then walk through the process of creating a user and setting a password. Create a few more users with different options.

1. Display the contents of `/etc/login.defs`. [Configuration control definition for login package]
2. Create a user with `useradd`.
3. Create a user with `useradd` and define a non-default home directory.
4. Create a user with `useradd` and define a non-Bash shell.

(continued on next slide)

Key Demonstration: Create User and Set Password

(continued from previous slide)

5. Set a password for each new user by using the `passwd` command.
6. Create a user with `adduser`, pointing out the options available during the process and showing how a password is set.
7. Display the contents of the `/etc/passwd` file to show the new users.
8. Display the contents of the `/etc/shadow` file to show the hashed passwords.

Modify and Delete User Accounts

BENNETT UNIVERSITY
THE TIMES GROUP

- usermod
- userdel

```
student@ubuntu20:~$ sudo useradd student10
student@ubuntu20:~$ sudo usermod -c "Student Ten" student10
student@ubuntu20:~$ tail /etc/passwd | grep student10
student10:x:1002:1002:Student Ten:/home/student10:/bin/sh
student@ubuntu20:~$ sudo userdel student10
student@ubuntu20:~$
```

USER ACCOUNT MODIFICATION UTILITIES

- usermod provides options for changing most of the fields in the /etc/passwd file.

Command	Description
usermod	Edits user account fields, as well as specifying primary and secondary group membership
passwd	Changes the password for an existing user
chpasswd	Reads a file of login name and password pairs, and updates the passwords
chage	Changes the password's expiration date
chfn	Changes the user account's comment information
chsh	Changes the user account's default shell

The chage Command

BENNETT UNIVERSITY
THE TIMES GROUP

$chage -l

Option	Purpose
-l	Display the current values
-M	Specify the maximum number of days between password changes
-m	Specify the minimum number of days between password changes
-W	Specify the number of warning days before a password expires
-E	Lock an account after a specified date

Key Demonstration: Account Configuration Commands

Sign in to at least one system (either RH or Debian-based), then display output of any of the following:

1. `whoami`
2. `w`
3. `who`
4. `id`
5. `/etc/login.defs` file
6. Password configurations with `chage`

$w & $who display all current logins on the system, including those that might have remote terminal connections.

Review Activity: User Account Management

1. Why are user passwords stored in the /etc/shadow file and not the /etc/passwd file?
2. What is the purpose of the /etc/skel directory?
3. Why might an administrator change a user's default shell?

BENNETT UNIVERSITY
THE TIMES GROUP

Group Management

GROUP CONFIGURATION FILES

Easier to grant permissions to a resource to a single group with five members than it is to individually grant access to each user account.

Groups are a standard administrative tool for controlling access to resources.

/etc/group stores the group configuration files

Group Configuration Files

/etc/group

```
student@ubuntu20:~$ tail /etc/group
pulse-access:x:129:
gdm:x:130:
lxd:x:131:student
student:x:1000:
sambashare:x:132:student
systemd-coredump:x:999:
student999:x:1001:
student10:x:1002:
abc:x:1003:
student12:x:1004:
student@ubuntu20:~$
```

Group Management Commands

Group Management Command	Purpose
groupadd	create a group in the /etc/group files
groupmod	Modify an existing group
groupdel	Remove an existing group

Key Demonstration: Group Management

Sign in to at least one system (either RH or Debian-based), then create several groups and display the `/etc/group` file contents. The focus of this demo is group management. Adding users to the group is in a later demonstration.

1. Sign in
2. Create a new group named sales - `groupadd sales`
3. Create a new group named marketing - `groupadd marketing`
4. Display the contents of `/etc/group` to show the two new groups - `tail /etc/group`

(continued on next slide)

Key Demonstration: Group Management

(continued from previous slide)

5. Modify the marketing group by changing its name to publicity - `groupmod -n publicity marketing`
6. Display the contents of `/etc/group` to show the renamed group - `tail /etc/group`
7. Delete the sales group - `groupdel sales`
8. Display the contents of `/etc/group` to show the sales group no longer exists

Add Users to a Group

BENNETT UNIVERSITY
THE TIMES GROUP

- Use the usermod command covered earlier to add a user to an existing group.
  - usermod –aG sales USERNAME

Option	Purpose
-a	Append the user to the group, and maintain any existing group memberships
-G	Specify a group to which the user will be added

```
student@ubuntu20:~$ sudo useradd student9
student@ubuntu20:~$ sudo groupadd sales
student@ubuntu20:~$ sudo usermod -aG sales student9
student@ubuntu20:~$ sudo tail /etc/group | grep sales
sales:x:1006:student9
student@ubuntu20:~$
```


$ groupmod -n publicity marketing

Key Demonstration: Add Members to Groups

Sign in to at least one system (either RH or Debian-based), then create a group and add members to it. The focus of this demo is adding users to groups; creating a group was covered in a previous demonstration.

1. Sign in
2. Create a group named Labs - `groupadd Labs`
3. Display the contents of `/etc/group` to show there are no members listed for the Labs group

(continued on next slide)

Key Demonstration: Add Members to Groups

(continued from previous slide)

4. Add USER to the Labs group - `usermod -aG Labs USER`
5. Display the contents of `/etc/group` to show that USER is a member of Labs
6. Display information about the USER account to show group membership - `id USER`

Review Activity: Group Account Management

1. Suggest at least two ways to display group membership information.
2. What command adds a user to a group?
3. What is the result if an administrator forgets to add the -a option when adding a user to a group?
4. Why might a user be a member of multiple groups?

BENNETT UNIVERSITY
THE TIMES GROUP

Configure Privilege Escalation

Root Users

BENNETT UNIVERSITY
THE TIMES GROUP

- Do not log on as the root user
- Many distributions disable the root account
- Use suor sudoto elevate privileges, or “get root”
- Delegate tasks by configuring the /etc/sudoers file

Elevate Privileges with su Command

- `su root` – switches to the root user in the original user's context.
- `su - root` – switches to the root user in the root user's context.
- You must know the password for the account you're switching to (unless you are root).

Elevate Privileges with sudo Command

BENNETT UNIVERSITY
THE TIMES GROUP

To create a user account usingn`sudo`:

- `sudo useradd {user- name}`

```
student@ubuntu20:~$ sudo tail /etc/sudoers

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
student@ubuntu20:~$
```

Configuration Examples for /etc/sudoers

BENNETT UNIVERSITY
THE TIMES GROUP

Example1

To grant full administrative privileges to a user, type `username ALL=(ALL:ALL) ALL`

- The user will be prompted for their password. Be very careful with this level of delegation!

Example 2

To delegate the ability to execute these shutdown commands without entering a password, type `SOMEUSER ALL=(ALL) NOPASSWD: SHUTDOWN_CMDS`

- Assumes that `SHUTDOWN_CMDS` is aliased to all related options for the shutdown command

Key Demonstration: Elevate Privileges with sudo

Instructor - sign in to at least one system (either RH or Debian-based), then demonstrate the process of adding a user to the `sudoers` file and delegating the ability to issue the shutdown command to the system.

1. Log in
2. Get root privileges `su - root`
3. Select a user to delegate authority to, or create a new user with `useradd`

(continued on next slide)

Key Demonstration: Elevate Privileges with sudo

(continued from previous slide)

4. Open the `/etc/sudoers` file for editing with `vi sudo`
5. At the bottom of the file, add the following line:

   ```
   SOMEUSER ALL=(ALL) NOPASSWD: SHUTDOWN_CMDS
   ```

6. Save changes and exit
7. (*Optional*) Switch to the delegated user and issue the shutdown `-h now` command

PolicyKit Configuration

BENNETT UNIVERSITY
THE TIMES GROUP

Alternative delegation method to sudo

- More granular control via defined rules and actions

Examples of delegated tasks:

- Software management
- System shutdown or hibernation
- Configuration of network devices
- Device access
- Mounting and unmounting filesystems on removable media

Polkit Commands

- `pkexec` - allows an authorized user to execute an action
- `pkaction` - display details about an action
- `pkcheck` - display whether a process is authorized
- `pkttyagent` - provides a text-based authentication agent

```
student@ubuntu20:~$ sudo pkexec useradd student5
student@ubuntu20:~$ tail /etc/passwd | grep student5
student5:x:1007:1008::/home/student5:/bin/sh
student@ubuntu20:~$
```

Troubleshoot Privilege Escalation Issues

- User has switched user identities, but variables and other profile settings are not present.
- User fails to switch identities when using the `su` command.
- `Sudo` does not function as expected.
- Cannot exercise administrative privileges.
- User cannot run a command, even when the command is preceded by `sudo`.

Review Activity: Privilege Escalation

1. A developer at your organization needs the ability to reboot a test server, but their account's standard privileges do not permit this. The developer requests the system's root user password in order to use su to reboot the server. Is there a more secure option that aligns with the principle of least privilege?

2. How are the su root and su - root commands different?

3. You must delegate the shutdown -h privilege to SOMEUSER. What tool is used to modify the /etc/sudoers file, and what line must be added to that file?

4. Whose password must be entered with sudo? Whose password must be entered with su?

BENNETT UNIVERSITY
THE TIMES GROUP

Troubleshoot User and Group Issues

Troubleshooting User Management Issues

BENNETT UNIVERSITY
THE TIMES GROUP

- Only authorized users can manage groups
  - root
  - Users delegated the privileges with `sudo`
- Does the group exist?
  - Check `etc/passwd` or `etc/group` files to confirm
- Halt active user processes with `sudo killall -u {username}`

User Login Attempt Failures

1. Confirm the user has an account on the system by displaying the contents of `/etc/passwd`. If necessary, create an account for the user by using the `useradd` command.
2. If the account exists, confirm that a password is set. Display the contents of `/etc/shadow` and verify a hashed password exists. Use the `passwd` command to set a password if one did not exist.
3. If the account exists and a password is set, the user may have forgotten the correct password. Reset the password with the `passwd` command.
4. If the account exists and a password is set, the password may be expired. Reset the password by using the `passwd` command.
5. If the account exists and a password is set, the account may be locked. Unlock the account by using the `chage` command.

Reviewing the Login Process

1. The operating system boots and the kernel is loaded. Assume the system boots to the CLI. An authentication prompt is displayed.
2. The user enters a name and password combination. These are checked against the `/etc/passwd` and `/etc/shadow` files. Settings such as expired passwords and locked accounts are checked for at this point.
3. System and user profile files are processed, and the user is presented with an authenticated and customized environment.

Using User Login Commands

- `lastlog` – displays recent login information
- `last` – pulls login history information from /var/log/wtmp
- `w` – displays current logins to the system, including idle time
- `who` – displays current logins to the system

```
student@ubuntu20:/etc/polkit-1$ last
student  :1           :1                Thu Dec  9 08:34   still logged in
reboot   system boot  5.8.0-43-generic Thu Dec  9 08:27   still running
student  :1           :1                Thu Nov 11 14:45 - 14:47  (00:01)
reboot   system boot  5.8.0-43-generic Thu Nov 11 14:44 - 14:48  (00:03)

wtmp begins Thu Nov 11 14:44:38 2021
student@ubuntu20:/etc/polkit-1$
```

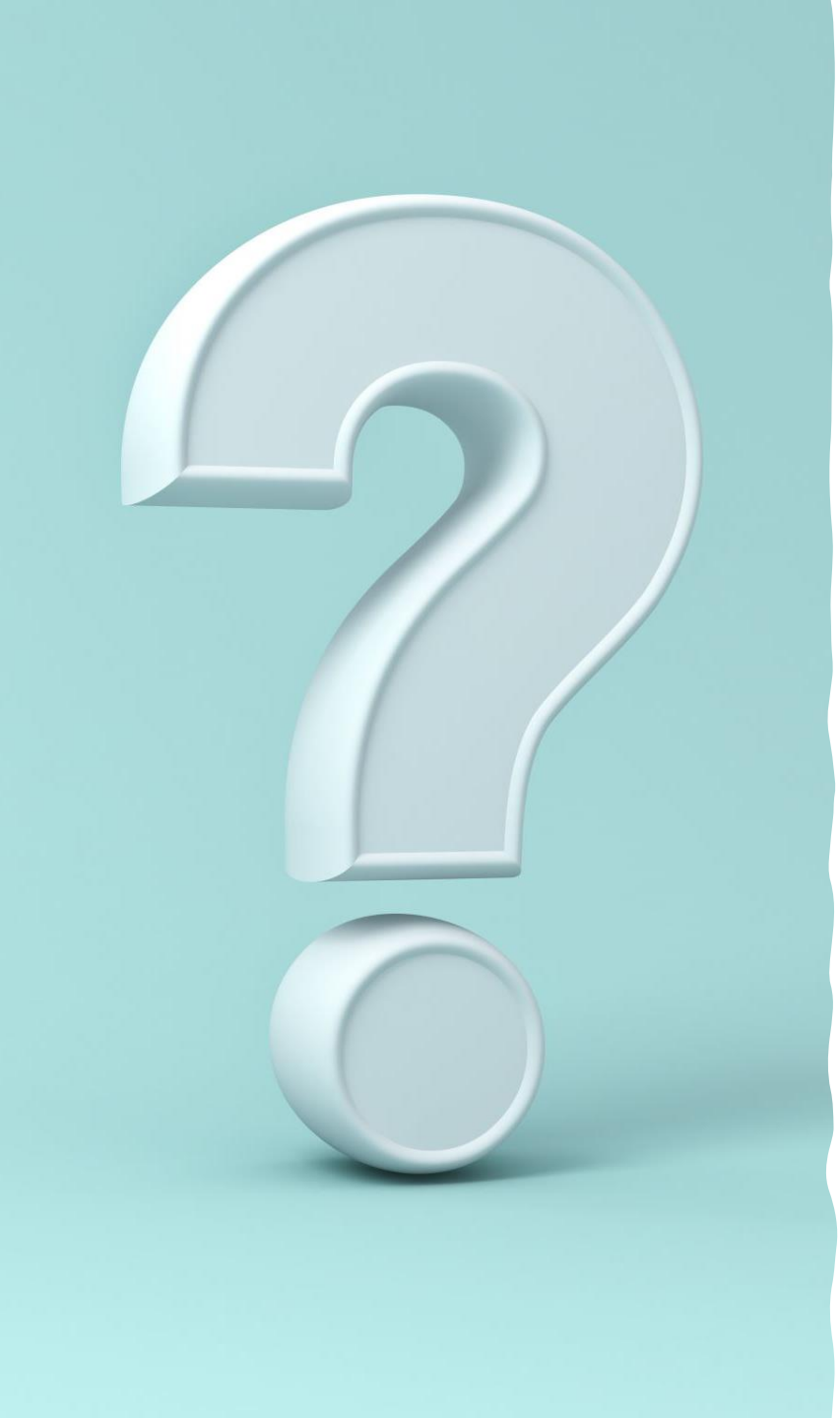
Key Demonstration: User Login Commands

Sign in to at least one system (either RH or Debian-based), then run the following commands and discuss the output. Note that the output can vary from system to system.

1. Run the `last` command.
2. Run the `lastlog` command.
3. Run the `w` command.
4. Run the `who` command and compare the results to the output from the `w` command.

Review Activity: User and Group Troubleshooting

1. List at least three scenarios where you might need records of who logged in to a Linux system.
2. Another administrator asks you to explain the value of editing the /etc/sudoer's file with visudo rather than a traditional text editor. What is your response?
3. List at least three reasons a user account might be locked.
4. During a security audit it is discovered that a user does not have a password set. When you check the /etc/passwd file, the password field is properly populated with the x character. What file would actually display whether a password has been set for the user?
5. A user places sudo before a command, but the command still fails to run. What might be the cause?
6. An administrator asks you how to delegate Linux administrative privileges to a specific user. What group is used for such delegation?



BENNETT UNIVERSITY
TIMES OF INDIA GROUP

Thanks

Q & A