Admin Privileges

User & group privileges

For users to have escalated privilege on a server (root access), they need to be granted this permission.

==========

sudo

Users with sudo access have full administrator permissions, this means that they can essentially perform any task on the system.

There are 2 methods we can use to grant users sudo access:

---

1. usermod

```
sudo usermod -aG sudo username
```

You can then validate that this has worked by checking the groups that the specified user is included in:

```
groups username
```

---

2 Editing the sudoers file directly

Users with sudo access are defined within the /etc/sudoers file. This file should ONLY ever be edited using the visudo text editor - as this will check the syntax for any errors.

```
visudo
```

To add a new user to the sudoers group, we need to append a line to the /etc/sudoers file.

1. Edit the /etc/sudoers file using visudo:

```
visudo
```

2. Find the line that reads `# User privilege specification` and add the following line below it:

```
username ALL=(ALL:ALL) ALL
```

Adding user groups to sudoers

In addition to adding specific users to the sudoers group, we can also add user groups. Once again, this is best achieved by editing the sudoers file directly using visudo.

1. Edit the sudoers file

```
visudo
```

2. Find the line that reads `# User privilege specification` and add the following line below it:

```
%groupname ALL=(ALL:ALL) ALL
```

Groups are defined by placing a % symbol in front of the group name.

Giving users sudo privilege for specific tasks/commands

In addition to giving a user full sudo permission on a system, we can also implement a more limited set of sudo-enabled privileges.

For example, I want to add a user who has sudo permission to run updates on a system, but I don't want them to have all privileges. To do this, we would need to edit the sudoers file as above using the visudo command, once there you can add a line like the following:

```
username ALL=(ALL:ALL) /usr/bin/apt update,/user/bin/apt upgrade
```

Note: As best practice, you're best off specifying the full binary path of the commands you wish to grant access to. This prevents a user from renaming a binary to apt (in this example) and being able to run the command with sudo privilege.

==========

Wheel

The alternative to adding users to the sudoers file, is to add users to the Wheel group. The Wheel group is essentially an exclusion that can be added for users to allow access to certain roles.

By default, any users in the wheel group have full privileges on the server.

An example of how this could be utilised, would be to add a rule into the /etc/wheel file that specifies a group that can be used to perform a specific task. Users that need this privilege could then be added to this file.

==========

PolicyKit

PolicyKit (also known as polkit) is a toolkit for defining and handling authorizations in Linux systems. It is used to manage privileges for unprivileged processes to perform tasks that normally require higher privileges, such as those of the root user. This allows for more fine-grained control over what users and processes are allowed to do without requiring full administrative access.

Revision #6
Created 2023-08-20 15:59:18 UTC by Daniel
Updated 2024-05-26 19:46:17 UTC by Daniel