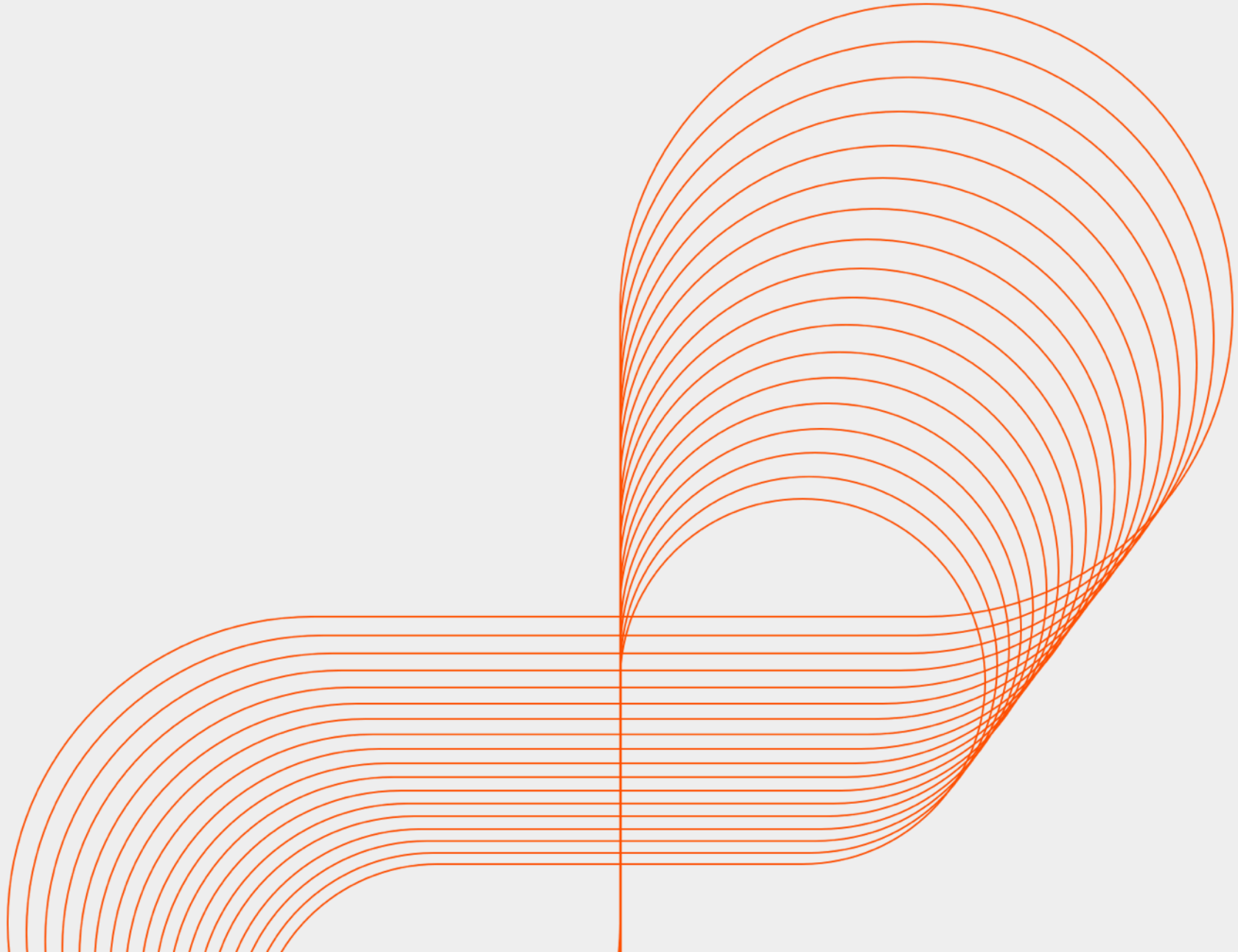
Persistent

UNIX



Accounts & Groups

Account Basics

- A user account provides you with access to the Unix system, either by a shell, an ftp account or other means
- To use the resources that the Unix system provides, you need a valid user account and resource permissions
- There are three primary types of accounts on a Unix system
  - root account
  - system account
  - user account

Confidential © 2020 Persistent Systems

Account Types

- Root Account
  - The root account’s user has complete access to the system
  - The root user(root) can do absolutely anything on the system, without any restriction
- System Accounts
  - These accounts are required for the operation of system-specific components e.g. mail account, sshd account, etc
  - These are generally provided by the OS during installation and assist in the running of services that the users require
- User Accounts
  - These accounts provide interactive access to the system for users and groups of users
  - General users are assigned to these accounts and usually have limited access to critical system files and directories

Confidential © 2020 Persistent Systems

Users

- Every user of the system is assigned a unique User ID number (the **uid**).
- Users' names and uids are stored in **/etc/passwd**.
- Users are assigned a home directory and a shell.
- Users cannot read, write or execute each other's files without permissions.
- Find out currently logged in users:
  - Users, who, w

Confidential © 2020 Persistent Systems

Groups

- Group accounts add the capability to assemble other accounts into logical arrangements for simplification of privilege (permission) management.
- Users are assigned to groups with unique group id numbers (the **gid**).
- gids are stored in **/etc/group**.
- To find out what groups you belong to:
  - Groups, id

Confidential © 2020 Persistent Systems

User Administration Config Files

- There are three main user administration files
  - /etc/passwd – identifies the authorized accounts for the system
  - /etc/shadow – holds the encrypted password of the corresponding account. Was not present on earlier Unix systems
  - /etc/group – Contains information on group accounts
- Not all user accounts have access to all files. Only root user has read/write access to all the files. Other user accounts can view the /etc/passwd and /etc/group file, but not the /etc/shadow file

Confidential © 2020 Persistent Systems

su & sudo Commands

- Sometimes, you will need to log into another account without logging out of the system
- There are two commands for this purpose – *su*, which is present on all versions of Unix, and *sudo*, that may be not available with all versions
- While using the commands, you might be asked for the password of that account, unless you are the root user
- Running *su* by itself takes you to the root account
- When using *su*, you continue to use your environment variables and profile. If you want to use the account's user environment, put a – between the su and the account name: *su – amber*
- *sudo* is used to execute commands as another user

Confidential © 2020 Persistent Systems

Links for objective multiple choice questions.

- http://www.sanfoundry.com/linux-command-mcq-1/
- http://www.sanfoundry.com/linux-command-mcq-2/
- http://www.sanfoundry.com/linux-command-mcq-3/
- http://www.indiabix.com/computer-science/unix/
- http://www.avatto.com/computer-science/test/mcqs/questions-answers/unix/153/1.html
- http://www.gkseries.com/computer-engineering/unix/multiple-choice-questions-and-answers-on-unix-and-shell-programming
- http://www.withoutbook.com/online_test.php?quiz=38&quesNo=10&subject=Top%2010%20UNIX%20Online%20Practice%20Test%20%7C%20Multiple%20Choice

Confidential © 2020 Persistent Systems