Your organization has setup a security policy that requires all passwords to be unique and should not be reused once changed. What type of policy would you define this requirement as?

Password history

Password age

Password complexity

Password length

Answer: A

Explanation: A password history policy is used to prevent password reuse. For example, if I set the Password History to 3, you cannot reuse a previous password until you have used 3 new passwords first. (Password1 -> Password2 -> Password3 -> Password4, then you can reuse Password1)

You are working as a college professor and want to verify that you have the correct permissions assigned to a folder on a Linux file server which will serve as a virtual Dropbox for students to submit their homework. Since you are the owner of the folder, you would like to ensure you have read and write permissions enabled. You also have a group setup that contains your teaching assistants’ and your own user account. For this group, you want to ensure the folder is setup for read and write access. Your students are considered part of “all users”, so you want to ensure they can write to the folder but cannot read from it. Which of the commands would you use to correctly set the permissions for the folder Dropbox on a Linux system?

chmod 777 Dropbox

chmod 662 Dropbox

chmod 642 Dropbox

chmod 741 Dropbox

Answer: B

Explanation: Permissions in Linux are set using three-digit codes for the Owner, Group, and All User permission levels. Read (4), Write (2), and Execute (1) all have values associated with them. You add up the values for the permissions for each group. In this case, Read/Write (6), Read/Write (6), and Write (2) for the Owner, Group, and All Users (662).

You are working as a contractor for a high-security military organization. Which of the following models of access control is appropriate to ensure that a person has the appropriate security clearance and “need-to-know” prior to accessing a file?

Discretionary Access Control (DAC)

Attribute-Based Access Control (ABAC)

Mandatory Access Control (MAC)

Role-Based Access Control (RBAC)

Answer: C

Explanation: Mandatory Access Control (MAC) relies on labeling all subjects and objects and ensuring that a subject has a matching or higher-security label and a “need-to-know” prior to accessing a file. MAC has evolved into Rule-Based Access Control and Lattice-Based Access Control. MAC can be enabled in the BSD and SELinux operating systems.