LAB 2

1.

A screenshot of a computer program

Description automatically generated

2.

A screenshot of a computer program

Description automatically generated

3.

A screenshot of a computer

Description automatically generated

4.

A screenshot of a computer program

Description automatically generated

5.

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Part 2

1. The idea of limiting user, account, and computer process access permissions to only those resources that are necessary to carry out authorized tasks is known as least privilege. Privilege is the right to go beyond certain security measures. The principle of least privilege (POLP), as applied to individuals, refers to enforcing the lowest clearance level, or the minimum degree of user rights, that permits the user to carry out his or her role. However, processes, applications, systems, and devices (such as IoT) also fall under the definition of least privilege access because they should each have only the rights required to carry out a permitted action. Least privilege access enforcement is a crucial best practice to lower security risk and minimize business disruption brought on by mistakes or malicious intent by someone in the organization or outside who has accessed the resource illegally.
2. Privilege creep is simply when a user just started with the right access or power needed for their role and over time, they end up getting more privileges or access rights than they should. For example, new permissions are added, but those that already exist are never deleted likely to become a security risk due to the increased likelihood of illegal access, resource misuse, and security breaches, this phenomenon might result in serious security problems. Organizations must routinely examine and modify user permissions to prevent privilege creep and make sure that people only have access to resources that are necessary for their tasks. Proper access management and maintenance prevent privilege creep.
3. According to Microsoft, “The Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network.” (Source: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview>) On a local network or over the internet, files, printers, and other resources can be shared using the Server Message Block (SMB) network communication protocol. Users can access shared files and resources as if they were on their own computers because it makes it easier for data to be exchanged and for devices on a network to communicate with one another. In simple terms, it’s a way to share things like files. Imagine, I have a set of friends and I want to share with them my makeup. SMB is like the rule or a communication tool I use to share and for us to do makeup together.