## ASIST – PL2

## Criar 6 utilizadores na máquina Linux (luser1 a luser6) com as seguintes características:

1. *Através do comando useradd (verificar as características do comando através de man useradd ou useradd -?):*

**useradd -u 6000 luser1**

**useradd -u 6001 luser2**

**useradd -u 6002 luser3**

***useradd***: Este é o comando utilizado para adicionar um novo utilizador.

***-u 6000***: Esta opção especifica o Identificador de Utilizador Numérico (UID) para o utilizador. Neste caso, define o UID como 6000 para "luser1."

***luser1***: Este é o nome para o novo utilizador.

**passwd luser1**

**passwd luser2**

**passwd luser3**

Posteriormente, o comando sudo passwd luserX é usado para definir a senha do um utilizador específico.

É importante ter em consideração que, recorrendo ao comando sudo passwd, serão necessárias as permissões apropriadas (sudo) para realizar essa ação

1. *Editando os ficheiros apropriados e com as seguintes características.*

**useradd -u 7000 -d /home/luser4 luser4**

**useradd -u 7001 -d /home/luser5 luser5**

**useradd -u 7002 -d /home/luser6home luser6**

Mais uma vez recorremos ao comando useradd com o acréscimo do parâmetro -d /home/luser4, responsável por definir o diretório inicial (ou diretório home) do utilizador.

Tal como no ponto anterior, o comando sudo passwd luserX é usado para definir a senha do um utilizador específico.

1. *Quais são os ficheiros apropriados?*
2. *Quais são os ficheiros apropriados?*

Os principais arquivos relacionados à configuração de utilizadores num sistema Linux Debian são:

**/etc/passwd**: Este arquivo contém informações sobre os utilizadores do sistema, incluindo os nomes de utilizador, IDs de utilizador (UIDs), IDs de grupo principal (GIDs), nomes completos, diretórios home e shells padrão. Cada linha deste arquivo representa um utilizador e segue o seguinte formato:

**username:password:UID:GID:comment:home\_directory:shell**

**/etc/shadow**: Este arquivo contém as senhas criptografadas dos utilizadores, bem como informações de configuração relacionadas à segurança de senha.

**/etc/group**: Este arquivo contém informações sobre grupos do sistema, incluindo nomes de grupo, GIDs e listas de membros.

1. *Verificar a existência ou não das pastas (homedir) de cada utilizador criado.*
2. *Caso não existam, criá-las da forma correta.*

Crie diretórios home personalizados para os utilizadores com os IDs especificados. Para isso, recorremos ao comando mkdir:

**mkdir /home/luser1**

**mkdir /home/luser2**

**mkdir /home/luser3**

**mkdir -p /home/luser4**

**mkdir -p /home/luser5**

**mkdir -p /home/luser6home**

Depois, de forma a certificarmo-nos que os utilizadores devem ser os proprietários dos seus próprios diretórios home recorremos ao comando chown, para, consequentemente, definirmos as permissões corretas.

**chown luser1:luser1 /home/luser1**

**chown luser2:luser2 /home/luser2**

**chown luser3:luser3 /home/luser3**

**chown luser4:luser1 /home/luser4**

**chown luser5:luser2 /home/luser5**

**chown luser6:luser3 /home/luser6home**

1. *Verificar/modificar o proprietário da homedir dos utilizadores criados através do comando* chown (verificar as características do comando através de man chown ou chown -?)
2. *Este comando é suficiente ou é preciso utilizar algum adicional? Qual?*
3. *De que forma este comando é suficiente e de que forma é preciso utilizar um adicional?*

Para verificar o proprietário atual dos diretórios home, podemos recorrer ao seguinte comando:

**ls -l /home**

O comando chown é suficiente para configurar o proprietário e o grupo dos diretórios home, desmente que sejam introduzidos os nomes de utilizador corretos.

1. *Verificar se os utilizadores criados podem aceder ao sistema.*
2. *Se podem, porquê?*

Os utilizadores devem poder aceder ao sistema se as seguintes condições forem atendidas:

* Diretórios home corretamente configurados: Os diretórios home dos utilizadores devem existir e ter as permissões corretas. Estes diretórios devem ser criados com as permissões apropriadas (geralmente chmod 700) e definido o proprietário e o grupo corretos usando chown.
* Senha definida: Os utilizadores devem ter senhas definidas. O comando passwd é responsável por configurar senhas para os utilizadores. Sem uma senha válida, eles não poderão fazer login.
* Shell padrão configurado: Cada utilizador deve ter um shell padrão configurado. Podemos usar o comando chsh para definir o shell padrão. Sem um shell válido, o login pode não ser possível.

1. *Se não podem, porquê? E como pode corrigir?*

Se os utilizadores não conseguirem aceder ao sistema, isso pode ser devido a vários motivos:

* Permissões de diretório home incorretas: Se os diretórios home não tiverem permissões adequadas, os utilizadores não poderão aceder aos seus diretórios home. Podemos corrigir isso definindo as permissões corretas com o comando chmod, por exemplo, chmod 700 /home/nome\_do\_utilizador.
* Senha ausente ou inválida: Se a senha do utilizador não estiver configurada ou estiver configurada incorretamente, o acesso será negado. Podemos definir ou alterar a senha do utilizador usando o comando passwd.
* Shell inválido ou ausente: Se o shell padrão do utilizador não estiver definido ou estiver configurado para um shell inexistente, o login não será possível. O comando chsh é responsável por definir um shell válido.
* Bloqueio da conta: Às vezes, uma conta pode ser bloqueada por motivos de segurança, como tentativas de login repetidas com falha. Podemos verificar se uma conta está bloqueada recorrendo ao comando passwd -S nome\_do\_utilizador. Se a conta estiver bloqueada, podemos desbloqueá-la com o comando passwd -u nome\_do\_utilizador.
* Problemas de autenticação: Se o sistema de autenticação estiver configurado incorretamente, os utilizadores podem ter problemas de login. Os arquivos /etc/nsswitch.conf e /etc/pam.d/\* são responsáveis por garantir estas configurações.
* Problemas de espaço em disco: Se o sistema estiver sem espaço em disco, os utilizadores podem enfrentar problemas para fazer login.
* Problemas de configuração de grupos: Se os grupos não estiverem configurados corretamente, isso também pode afetar o acesso dos utilizadores. Podemos verificar os arquivos /etc/group e /etc/gshadow para garantir que as configurações estejam corretas.
* Adicionalmente, podemos verificar permissões, senhas, shells e outras configurações relevantes. Em caso de dúvida, é ainda importante consultar os logs de autenticação do sistema (geralmente em /var/log/auth.log ou /var/log/secure) para obter informações mais detalhadas sobre falhas de login.

1. *Criar 3 utilizadores na máquina Windows (wuser1 a wuser3).*
2. *Estes utilizadores podem aceder ao sistema? Porquê?*
3. *Na máquina Windows, criar os grupos wgrupo1, wgrupo2 e wasistgrupo.*
4. *Alterar os utilizadores wuser1 a wuser3 para pertencerem ao grupo wasistgrupo.*
5. *Que grupos existem por omissão num Windows Server?*
6. *Quais os seus objetivos?*
7. *Criar 6 utilizadores na máquina Linux (luser1 a luser6) com as seguintes características:*
8. *Os grupos lasistgrupo e o lgrupo1 através do comando groupadd (verificar as características do comando através de man groupadd ou groupadd -?).*

**groupadd lgrupo1**

**groupadd lasistgrupo**

1. *O grupo lgrupo2 editando os ficheiros apropriados.*

**nano /etc/group**

**lgrupo2:x:GID**

**lgrupo2**: Este é o nome do grupo. Neste caso, o grupo é chamado "lgrupo2".

**x**: O segundo campo geralmente é reservado para a senha do grupo, mas quando aparece como "x" ou algum outro caractere, indica que a senha do grupo é armazenada no arquivo /etc/gshadow em vez de estar visível neste arquivo. Isso é uma medida de segurança para proteger as senhas dos grupos.

**GID**: O terceiro campo representa o GID (Identificador de Grupo Numérico). O GID é um número único que identifica o grupo. No exemplo, "GID" provavelmente é apenas um marcador e deve ser substituído pelo valor numérico real do GID do grupo "lgrupo2".

1. *Mudar o grupo primário dos utilizadores luser1 a luser2 para o grupo lasistgrupo usando o comando usermod (verificar as características do comando através de man usermod ou usermod -?).*

**usermod -g 7004 luser1**

**usermod -g 7004 luser2**

Este comando é usado para modificar a configuração de um utilizador. Neste caso, o comando está a configurar o grupo principal (GID) do utilizador "luserX" para 7004 (GID referente ao *lasistgrupo)*.

1. *Mudar o grupo primário dos utilizadores luser3 a luser6 para o grupo lasistgrupo manualmente editando os ficheiros apropriados.*

**nano /etc/passwd**

Encontramos as linhas correspondentes aos utilizadores em questão:

**luser3:x:6002:1000::/home/luser3home:/bin/bash**

**luser6:x:7002:1000::/home/luser6home:/bin/bash**

Após editar o arquivo /etc/passwd, os utilizadores "luser3" a "luser6" terão o grupo "lasistgrupo" como grupo principal, correspondente ao GID 1000.

1. *Alterar os utilizadores luser1 a luser4 para pertencerem como grupo secundário ao grupo lgrupo2 com o comando usermod.*

**usermod -aG lgrupo2 luser1**

**usermod -aG lgrupo2 luser2**

**usermod -aG lgrupo2 luser3**

**usermod -aG lgrupo2 luser4**

Recorremos ao comando usermod para adicionar os utilizadores ao grupo secundário "lgrupo2". A opção relevante é -aG, que permite adicionar utilizadores a grupos secundários.

1. *Alterar os utilizadores luser5 a luser6 para pertencerem como grupo secundário ao grupo lgrupo2 manualmente, editando os ficheiros necessários.*

Semelhantemente ao ponto d):

**nano /etc/passwd**

Encontramos a linha correspondente ao grupo "lgrupo2" e adicionamos "luser5" e "luser6" separados por vírgulas (sem espaços) após os dois pontos. O formato da linha terá este aspeto:

**lgrupo2:x:GID:luser5,luser6**

1. *Corrigir os grupos das homedir dos utilizadores criados.*

**chown :lasistgrupo /home/luser1**

**chown :lasistgrupo /home/luser2**

**chown :lasistgrupo /home/luser3**

**chown :lasistgrupo /home/luser4**

**chown :lasistgrupo /home/luser5**

**chown :lasistgrupo /home/luser6home**

Seguidamente, podemos verificar as alterações recorrendo ao comando ls -l para um dos diretórios home, por exemplo:

**ls -l /home/luser1**

Concluiremo que o grupo do diretório home foi alterado para "lasistgrupo".

1. *Na máquina Linux alterar as permissões das homedir dos utilizadores para o mínimo possível através do comando chmod*
2. *De que forma pode ser dado este comando?*
3. *Como interpreta mínimo possível?*

Para alterar as permissões das diretórios home dos utilizadores para o mínimo possível recorremos ao comando chmod. No contexto de segurança, "mínimo possível" geralmente significa restringir o acesso ao máximo, permitindo que apenas o proprietário do diretório tenha permissões para aceder ao mesmo.

Para dar permissões mínimas aos diretórios home, foi executada a seguinte linha de comando:

**chmod 700 /home/nome\_do\_utilizador**

O chmod 700 define as seguintes permissões:

* + **7 (rwx)** para o proprietário do diretório, o que significa que o proprietário tem permissão total para ler, escrever e executar o diretório.
  + **0** para o grupo e outros, o que significa que nenhum acesso é permitido.

Isso garante que apenas o proprietário do diretório tenha acesso total ao mesmo, enquanto todos os outros não têm permissão de leitura, escrita ou execução.

1. *Na máquina Linux alterar as permissões das homedir dos utilizadores para o mínimo possível através do comando chmod*