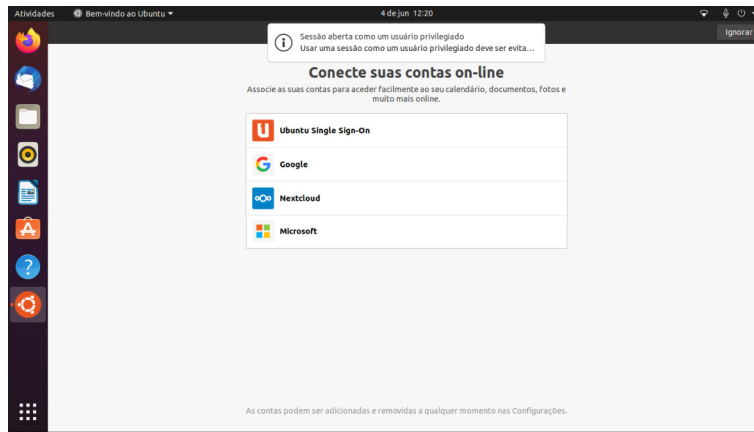


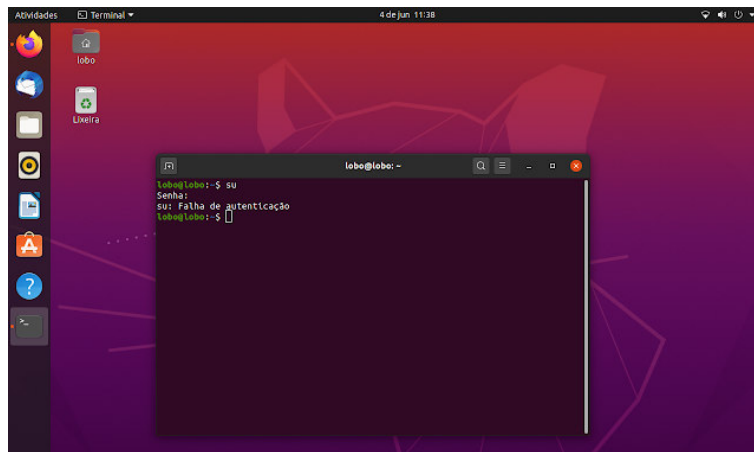
HABILITAR A CONTA DE ROOT NO UBUNTU E DERIVADOS



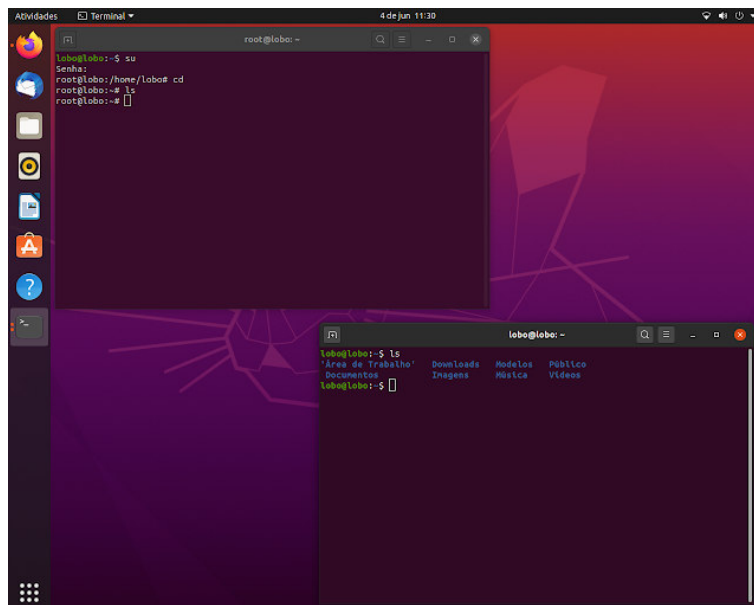
A conta de Root ou administrador, tem poder total em seu sistema operacional GNU/Linux. Não é aconselhável para usuários iniciantes.

Por padrão no Ubuntu ela vem desativada, o usuário tem apenas o sudo para obter poderes de Root.

Note que ao tentar logar como Root com o comando su temos falha de autenticação usando a senha do sudo, essa é definida na instalação do sistema para que o seu usuário tenha poderes limitados de Root, o suficiente para executar as tarefas administrativas mais comuns no sistema.



Ao habilitar a conta de Root você deve tomar o máximo de cuidado, principalmente se além de habilitar o Root você logar em sua sessão, note abaixo o Root liberado, mas sem acesso a sua sessão, ele não tem os diretórios de um user, eles só são criados se você logar na sua sessão.

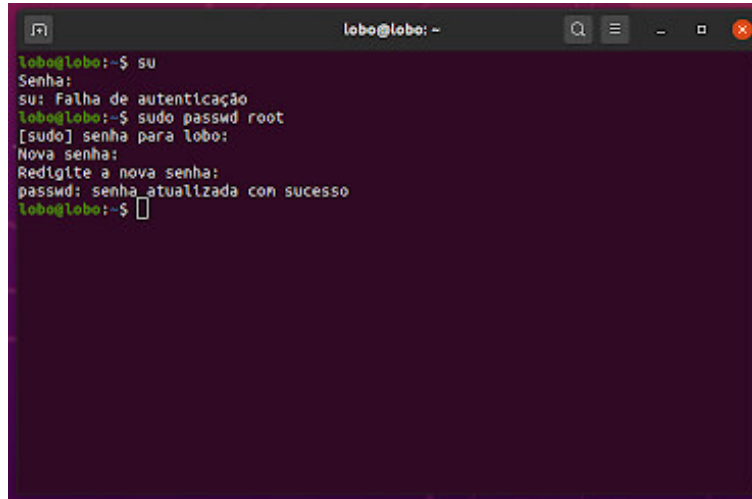


HABILITANDO O ROOT

Para habilitar o Root você precisa apenas definir uma senha para ele e usar o **su** para logar no terminal como Root.

Para definir a senha do Root execute o comando abaixo no terminal, digite a sua senha de **sudo** e em seguida a senha para o Root (digite e redigite).

sudo passwd root

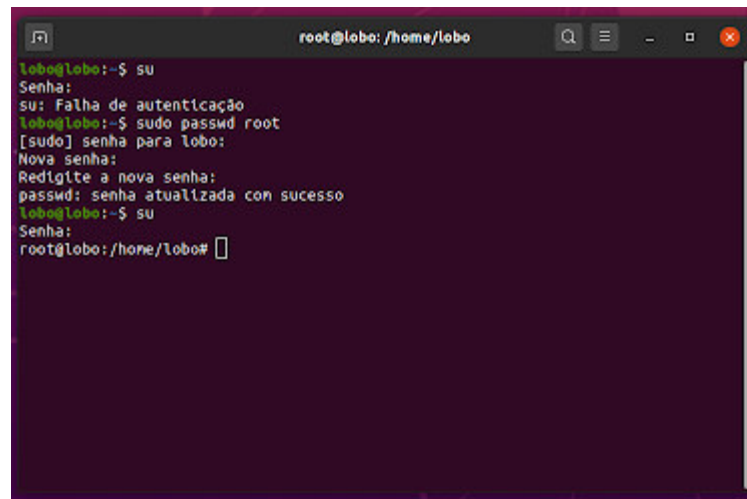


```
lobo@lobo: ~  
lobo@lobo:~$ su  
Senha:  
su: Falha de autenticação  
lobo@lobo:~$ sudo passwd root  
[sudo] senha para lobo:  
Nova senha:  
Redigite a nova senha:  
passwd: senha atualizada com sucesso  
lobo@lobo:~$
```

Para logar como Root utilize “su” como abaixo e a senha que acabou de definir.

su

Pronto, agora você tem poderes de Root no terminal, use com moderação.



```
root@lobo: /home/lobo  
lobo@lobo:~$ su  
Senha:  
su: Falha de autenticação  
lobo@lobo:~$ sudo passwd root  
[sudo] senha para lobo:  
Nova senha:  
Redigite a nova senha:  
passwd: senha atualizada com sucesso  
lobo@lobo:~$ su  
Senha:  
root@lobo: /home/lobo#
```

HABILITANDO A SESSÃO DO ROOT

Ao habilitar a sessão de Root, poderá logar no ambiente gráfico com poderes de Root. Nenhuma senha será pedida ao fazer alterações na / Raiz, ao instalar programas, todos na rede poderão assumir o controle total do seu computador, pragas virtuais podem ser instaladas sem que você perceba, muito cuidado ao usar a sessão Root.

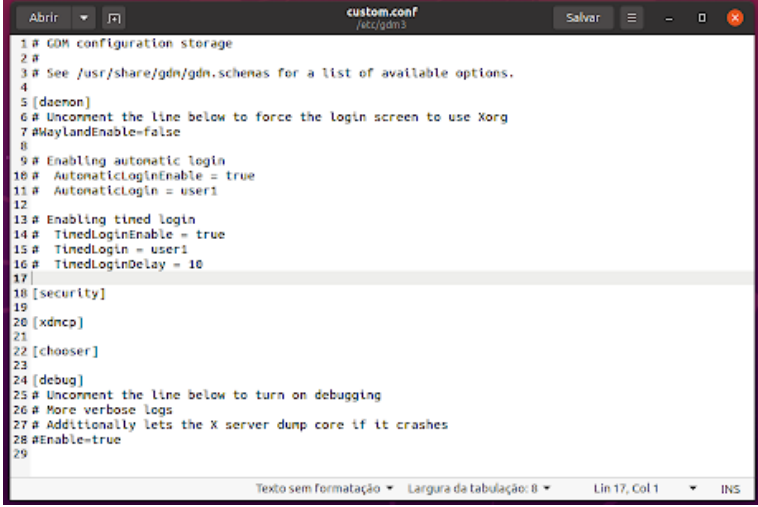
Para logar na sessão como Root vá em configurações do gerenciador de sessão gdm. Logue como Root no terminal.

su

Abra as configurações.

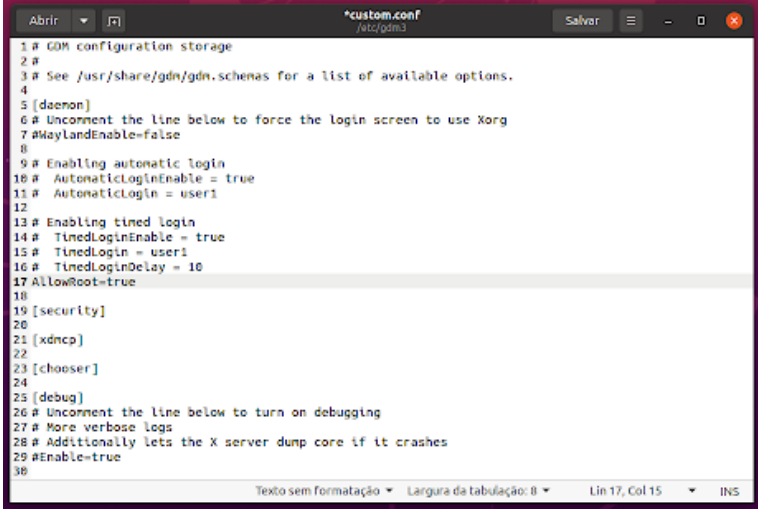
`gedit /etc/gdm3/custom.conf`

Na sessão "# Enabling timed login" é que iremos adicionar a linha para liberar a sessão do Root.



```
1 # GDM configuration storage
2 #
3 # See /usr/share/gdm/gdm.schemas for a list of available options.
4
5 [daemon]
6 # Uncomment the line below to force the login screen to use Xorg
7 #WaylandEnable=false
8
9 # Enabling automatic login
10 # AutomaticLoginEnable = true
11 # AutomaticLogin = user1
12
13 # Enabling timed login
14 # TimedLoginEnable = true
15 # TimedLogin = user1
16 # TimedLoginDelay = 10
17 |
18 [security]
19
20 [xdnccp]
21
22 [chooser]
23
24 [debug]
25 # Uncomment the line below to turn on debugging
26 # More verbose logs
27 # Additionally lets the X server dump core if it crashes
28 #Enable=true
29
```

Adicione "AllowRoot=true" como na imagem abaixo.



```
1 # GDM configuration storage
2 #
3 # See /usr/share/gdm/gdm.schemas for a list of available options.
4
5 [daemon]
6 # Uncomment the line below to force the login screen to use Xorg
7 #WaylandEnable=false
8
9 # Enabling automatic login
10 # AutomaticLoginEnable = true
11 # AutomaticLogin = user1
12
13 # Enabling timed login
14 # TimedLoginEnable = true
15 # TimedLogin = user1
16 # TimedLoginDelay = 10
17 AllowRoot=true
18
19 [security]
20
21 [xdnccp]
22
23 [chooser]
24
25 [debug]
26 # Uncomment the line below to turn on debugging
27 # More verbose logs
28 # Additionally lets the X server dump core if it crashes
29 #Enable=true
30
```

Salve o arquivo e feche.

Precisamos editar também, a autenticação PAM, abra o arquivo abaixo.

`gedit /etc/pam.d/gdm-password`

Localize "auth required pam_succeed_if.so user != root quiet_success"

```
gdm-password
/etc/pam.d

1 #PAM-1.0
2 auth requisite      pam_nologin.so
3 auth required      pam_succeed_if.so user != root quiet success
4 @include common-auth
5 auth optional      pam_gnome_keyring.so
6 @include common-account
7 # SELinux needs to be the first session rule. This ensures that any
8 # lingering context has been cleared. Without this it is possible
9 # that a module could execute code in the wrong domain.
10 session [success=ok ignore=ignore module_unknown=ignore default=bad]      pam_selinux.so close
11 session required      pam_loginuid.so
12 # SELinux needs to intervene at login time to ensure that the process
13 # starts in the proper default security context. Only sessions which are
14 # intended to run in the user's context should be run after this.
15 # pam_selinux.so changes the SELinux context of the used TTY and configures
16 # SELinux in order to transition to the user context with the next execve()
17 # call.
18 session [success=ok ignore=ignore module_unknown=ignore default=bad]      pam_selinux.so open
19 session optional      pam_keyinit.so force revoke
20 session required      pam_limits.so
21 session required      pam_env.so readenv=1
22 session required      pam_env.so readenv=1 user_readenv=1 envfile=/etc/default/locale
23 @include common-session
24 session optional      pam_gnome_keyring.so auto_start
25 @include common-password
```

Comente a linha adicionando # no início dela.

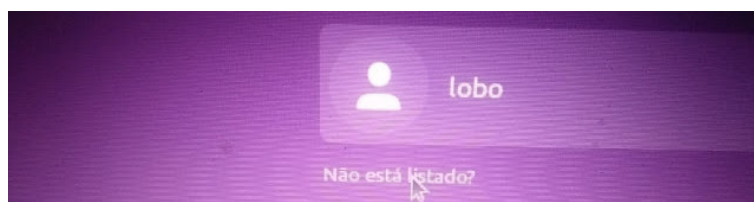
```
*gdm-password
/etc/pam.d

1 #PAM-1.0
2 auth requisite      pam_nologin.so
3 #auth required      pam_succeed_if.so user != root quiet success
4 @include common-auth
5 auth optional      pam_gnome_keyring.so
6 @include common-account
7 # SELinux needs to be the first session rule. This ensures that any
8 # lingering context has been cleared. Without this it is possible
9 # that a module could execute code in the wrong domain.
10 session [success=ok ignore=ignore module_unknown=ignore default=bad]      pam_selinux.so close
11 session required      pam_loginuid.so
12 # SELinux needs to intervene at login time to ensure that the process
13 # starts in the proper default security context. Only sessions which are
14 # intended to run in the user's context should be run after this.
15 # pam_selinux.so changes the SELinux context of the used TTY and configures
16 # SELinux in order to transition to the user context with the next execve()
17 # call.
18 session [success=ok ignore=ignore module_unknown=ignore default=bad]      pam_selinux.so open
19 session optional      pam_keyinit.so force revoke
20 session required      pam_limits.so
21 session required      pam_env.so readenv=1
22 session required      pam_env.so readenv=1 user_readenv=1 envfile=/etc/default/locale
23 @include common-session
24 session optional      pam_gnome_keyring.so auto_start
25 @include common-password
```

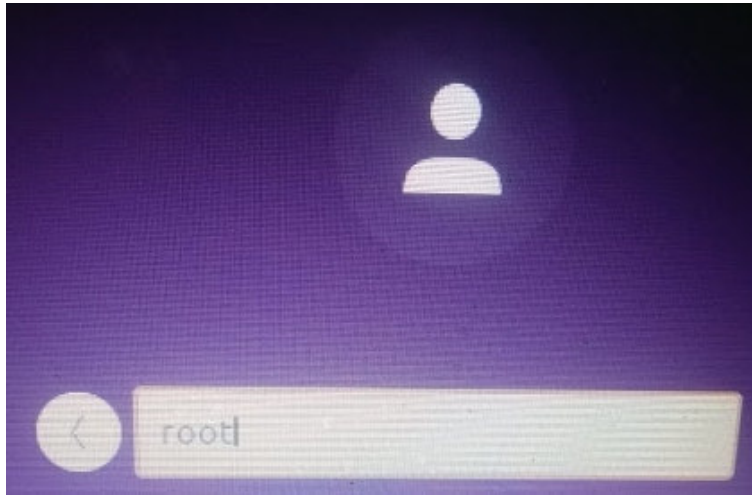
Salve e feche o arquivo. Reinicie o computador.

reboot

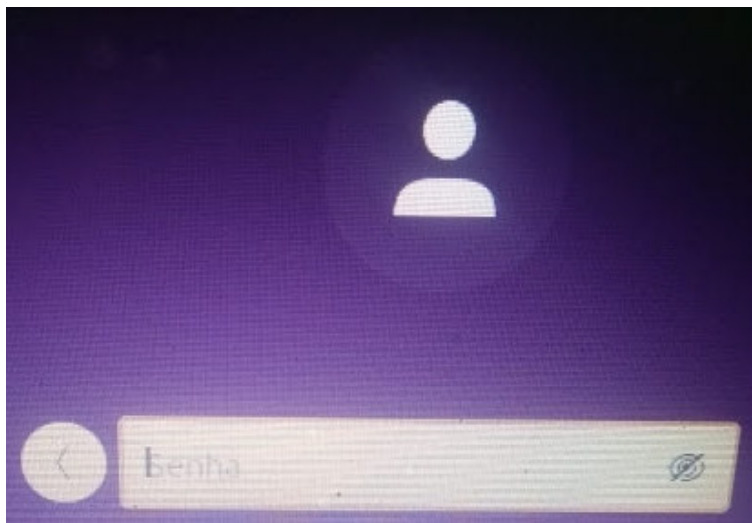
Na tela de login click em "Não está listado?".



Para o nome de usuário digite root

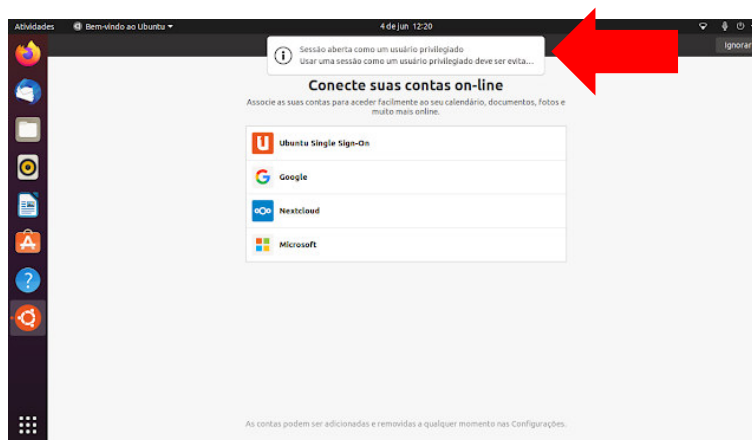


Digite a senha que você definiu para o Root.

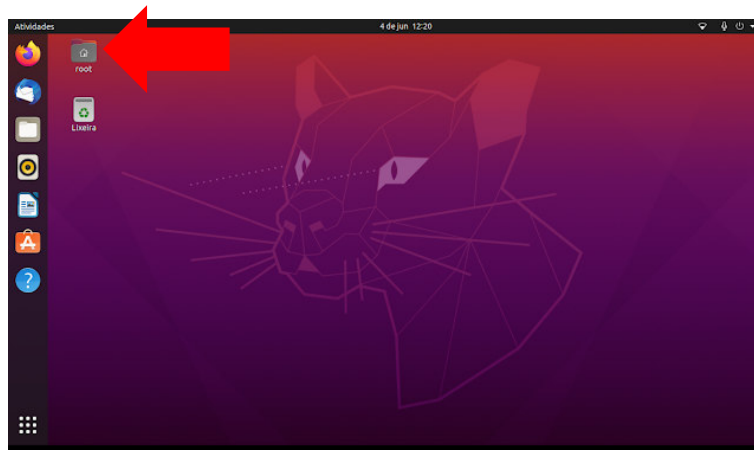


Pronto! Muito cuidado ao usar a sessão como root.

O Ubuntu avisa: **“Sessão aberta como um usuário privilegiado. Usar uma sessão como um usuário privilegiado deve ser evitado por motivos de segurança. Se possível, você deve abrir uma sessão como um usuário normal.”** Daqui para a frente é por sua conta e risco.



Note que a pasta de usuário é o root (em algumas versões será Home). Ao abrir o terminal o usuário será o [root@...:~#](#).



Para desativar a senha do Root use o comando abaixo.

```
passwd --lock root
```

Se desativado o acesso Root mesmo que a senha esteja correta, após a reinicialização, será apresentada a mensagem “**Desculpe, isto não funcionou. Por gentileza, tente novamente**”.

Para ativar novamente o Root use:

```
sudo passwd --unlock root
```