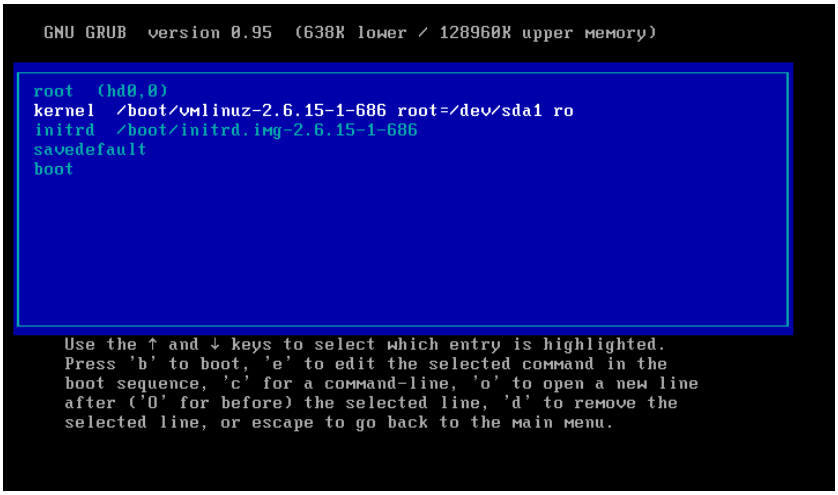
Curso 4451

Linux Security Administration in Cloud

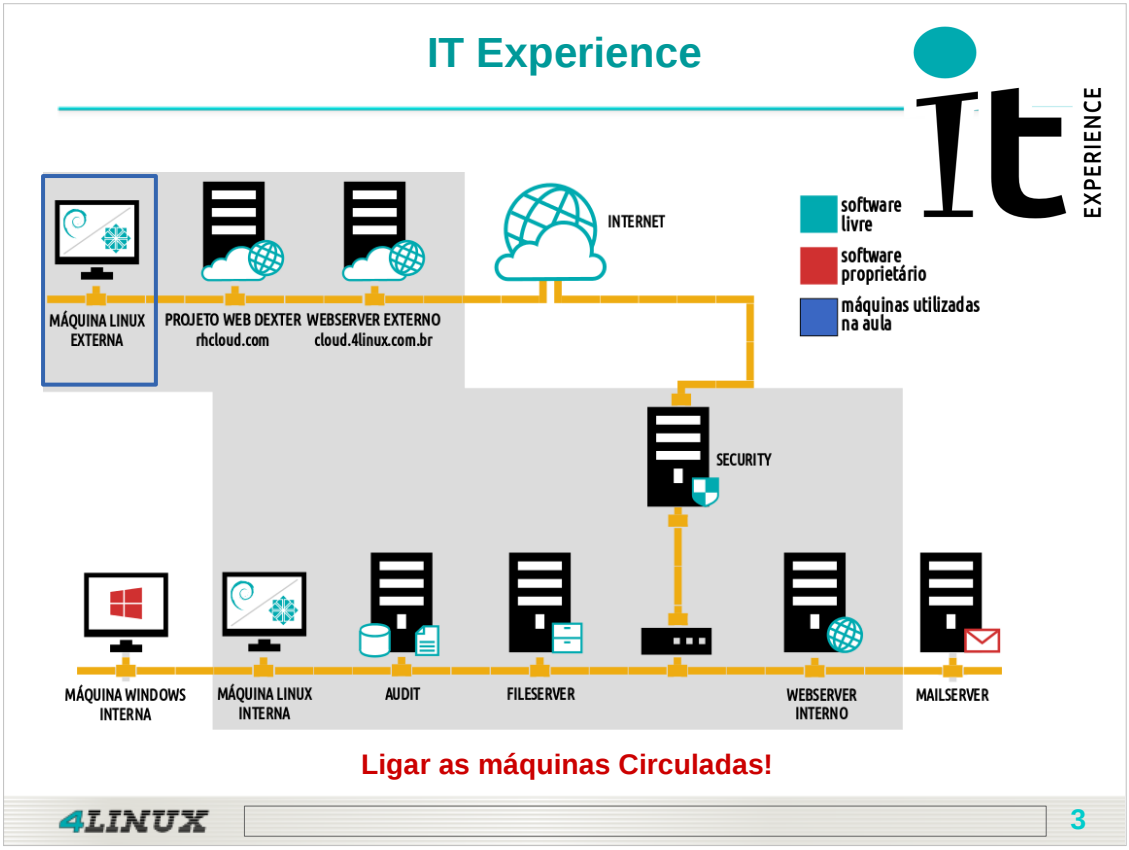
Gerenciadores de Boot



Fundamentação

Um “bootloader”, ou gerenciador de boot, é o software responsável por carregar o sistema operacional durante a inicialização do computador;

O papel do “bootloader” é fornecer uma lista de opções de sistemas operacionais disponíveis na máquina e que podem ser carregados.


IT Experience
IT EXPERIENCE
INTERNET
software livre
software proprietário
máquinas utilizadas na aula
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER
rhcloud.com
WEBSERVER EXTERNO
cloud.4linux.com.br
SECURITY
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
AUDIT
FILESERVER
WEBSERVER INTERNO
MAILSERVER
Ligar as máquinas Circuladas!
4LINUX
3

Anotações:

Objetivos da Aula

Aula 12

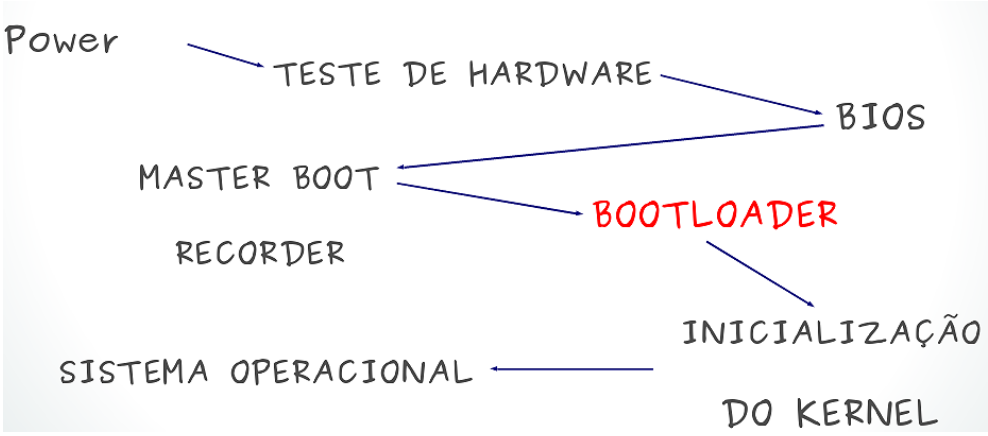
- Configurar comportamento do Grub 1;
- Adicionar senha ao Grub1;
- Configurar comportamento do Grub 2;
- Adicionar senha ao Grub2.

Anotações:

Gerenciadores de Boot

O que ocorre na Inicialização de um Sistema?

Se fizéssemos um esboço seria mais ou menos assim:



4LINUX 5

Fundamentação

Uma vez que o usuário escolheu qual sistema deseja "subir" o **"bootloader"** inicia o carregamento do kernel na memória RAM o qual passa a ter o controle sobre a máquina.

Há vários **"bootloaders"** diferentes disponíveis no mundo GNU/Linux;

Neste capítulo utilizaremos o Grub, provavelmente a ferramenta mais utilizada do gênero no cenário atual.

Gerenciadores de Boot

Servidor que utiliza o Grub versão 1

GRUB (Padrão CentOS):

- O grub (Grand Unified Boot Loader) é o “bootloader” usado em ambiente CentOS;
- Seus arquivos de configuração localizam-se em **“/boot/grub/”** quando utilizamos a versão 1, sendo o principal deles o **“menu.lst”**.

1 – Verifique o conteúdo do diretório /boot e do arquivo menu.lst:

```
1# ls /boot
```

4LINUX 6

Grub

O grub pode ser considerado um gerenciador bem “amigável” principalmente em sua primeira versão, usada em ambiente CentOS.

Seu principal arquivo de configuração, o **menu.ls**t é na verdade um link para **“/boot/grub/grub.conf”**.

Este arquivo é lido a cada boot, por isso não é necessário reinstalar o grub ao fazer alterações, como no caso de outros gerenciadores de boot como o lilo.

Gerenciadores de Boot

Servidor que utiliza o Grub versão 1

2 – Em seguida explore o arquivo menu.lst:

```
1# cat /boot/grub/menu.lst
```

- Basicamente, podemos dividir a configuração deste arquivo e, consequentemente, a configuração do grub por entradas;
- Cada sistema operacional possui uma entrada iniciada pela palavra **title** e seguida das opções referentes aquela versão de sistema;

Dentro de uma entrada do grub temos os seguintes itens:

title → Contém o nome do sistema, da forma como ele irá aparecer na tela de boot. Não é preciso que o nome indique corretamente o sistema, ou seja apelidos são permitidos;

root → Indica a localização do sistema no disco, no grub a numeração das partições começa em 0, isso significa que (hd0,0) é a primeira partição do primeiro disco rígido;

kernel → Indica o arquivo dentro do diretório /boot que será carregado no início do boot. Este nome segue o padrão "vmlinuz" conforme explicado no capítulo de kernel;

Initrd → indica a localização de um arquivo initrd ou intramfs, que será carregado junto com o Kernel.

Gerenciadores de Boot

Servidor que utiliza o Grub versão 1

Customizando Entradas no Grub:

- Entradas do grub1 podem ser customizadas dentro do arquivo menu.lst; alterações feitas aqui afetam diretamente as opções de inicializacao do grub;

As opções mais comuns a serem alteradas são as seguintes:

- **default 0** → Define qual sistema será inicializado, o valor 0 quer dizer que a primeira entrada do arquivo será utilizada.

Note que ele conta os sistemas listando a partir do zero.

A opção default

Em nosso sistema do ponto de vista do grub, o CentOS é o sistema "0" e a opção padrão de inicialização, por causa da opção **"default 0"** setada no arquivo menu.lst.

Caso tivéssemos um sistema Windows e um sistema Debian, ambos instalados em partições paralelas a do CentOS eles provavelmente seriam os sistemas “1”, e “2”. A depender da ordem em que foram instalados.

Note que ele conta os sistemas incluídos na lista a partir do zero.

Gerenciadores de Boot

- **Timeout 5** → Indica o tempo disponível para que as opções do grub sejam acionadas, caso nenhuma tecla seja presionada, o sistema inicializado será o default;
- **splashimage** → Define a imagem de fundo do grub. A imagem deverá ser disponibilizada no mesmo disco/partição do “bootloader”;
- **hiddenmenu** → Padrão de algumas distribuições como CentOS, esta opção define que o menu de opções do grub somente será exibido se alguma tecla for pressionada dentro do limite definido pela opção “**timeout**”.

Nomenclatura de Discos

Sabemos que no Linux os HDs e partições são acessados através de dispositivos especiais, localizados dentro do diretório "/dev" seguindo uma nomenclatura de acordo com a partição e o tipo de disco conectado.

Para "simplificar" esse formato os desenvolvedores do GRUB decidiram adotar sua própria nomenclatura, onde os HDs e partições são nomeados a partir do zero.

Ou seja, o "/dev/hda1"ou “/dev/sda1” é referenciado na configuração do grub como "(hd0,0)" (primeiro HD, primeira partição).

Gerenciadores de Boot

Servidor que utiliza o Grub versão 1

Colocando Imagem no Grub versão 1:

1 – Utilize a ferramenta convert para a conversão ao formato usado no grub:

```
1# apt-get install imagemagick -y
2# cd /root/logo
3# convert -resize 640x480 -colors 14 dexterlogo.png
dexterlogo.xpm
4# gzip dexterlogo.xpm
```

Pré requisitos para a imagem do grub:

No grub 1 a imagem a ser utilizada possui como pré-requisito o formato: 640x480 com até 14 cores;

Para que os pré-requisitos de formato sejam atendidos é possível utilizar ferramentas de conversão de imagem, em nosso exemplo utilizamos a ferramenta convert do pacote ImageMagick.

Gerenciadores de Boot

Servidor que utiliza o Grub versão 1

Colocando Imagem no Grub:

2 – Mova o arquivo gerado para o diretorio /boot/grub:

```
1# mv dexterlogo.xpm.gz /boot/grub/
2# vim /boot/grub/menu.lst
splashimage=(hd0,0)/grub/dexterlogo.xpm.gz
```

3 – Salve o arquivo e reinicialize a máquina para verificar a alteração:

```
3# init 6
```


Anotações:

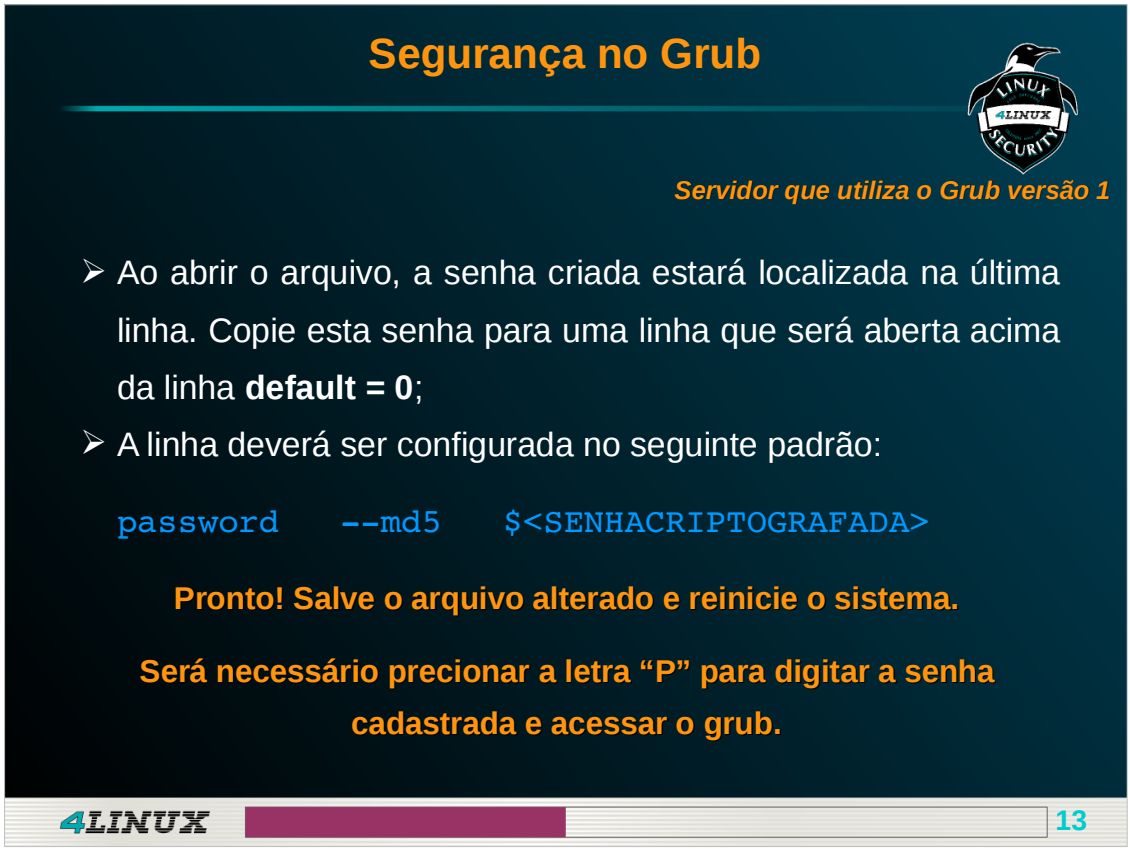
Segurança no Grub

Servidor que utiliza o Grub versão 1

- Para melhorar a segurança de nossos servidores, colocaremos uma senha no grub, prevenindo acessos não autorizados ao modo de manutenção do sistema;
- Primeiro gere uma senha e a direcione para um arquivo:

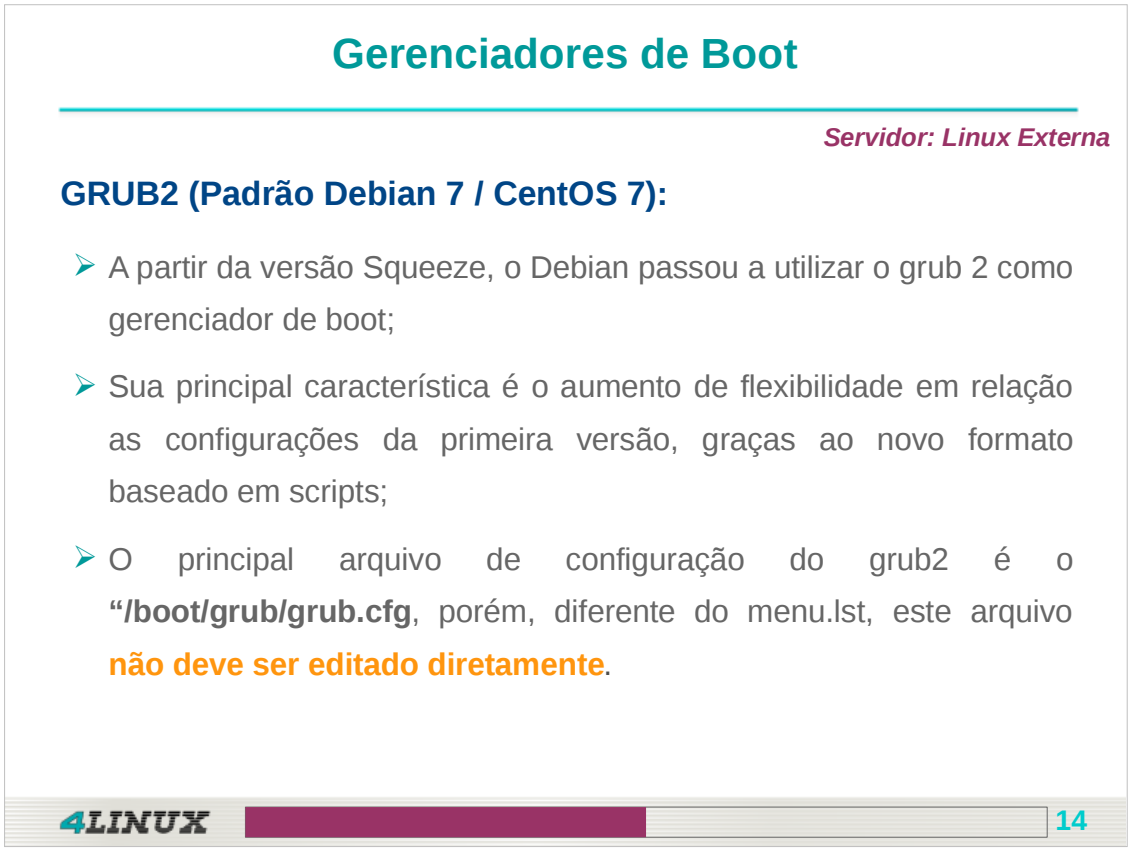
```
1# grub-md5-crypt | tee /root/arquivo
2# tail -n1 arquivo >> /boot/grub/menu.lst
3# vim /boot/grub/menu.lst
```


Anotações:



Porque colocar senha no GRUB?

A importância de termos senha no Grub é que se o mesmo estiver livre de senha, qualquer pessoa na hora da inicialização pode editá-lo e inicializá-lo para ganhar poderes de root sem saber a senha.



GRUB2

GRUB2 é um software Open Source. Ele é descendente do GRUB (Grand Unified Bootloader). Foi completamente reescrito para dar ao usuário flexibilidade e performance significativamente aumentadas.

GRUB vs GRUB2

- O arquivo /boot/grub/menu.lst do GRUB foi substituido por /boot/grub/grub.cfg no GRUB2.

- O principal arquivo de menu /boot/grub/grub.cfg não é para ser editado mesmo pelo "root"

- O grub.cfg é sobrescrito sempre que houver uma atualização, um kernel for adicionado/removido ou o usuário executar update-grub.

Gerenciadores de Boot

Servidor: Linux Externa

GRUB2 (Padrão Debian):

Ao invés de editar o arquivo grub.cfg, opções deverão ser editadas através dos scritps disponíveis em **"/etc/grub.d"**, ou através do arquivo "**/etc/default/grub".**

1 – Verifique quais são os scripts disponíveis em /etc/grub.d:

```
1# ls /etc/grub.d/
```

NOTA: Alterações são inseridas no arquivo grub.cfg, de acordo com os scripts desse diretório. Esses scripts são executados pela ordem de seu numeral, do menor, para o maior.

- O usuário pode criar um arquivo personalizado em /etc/grub.d/40_custom com suas próprias entradas.

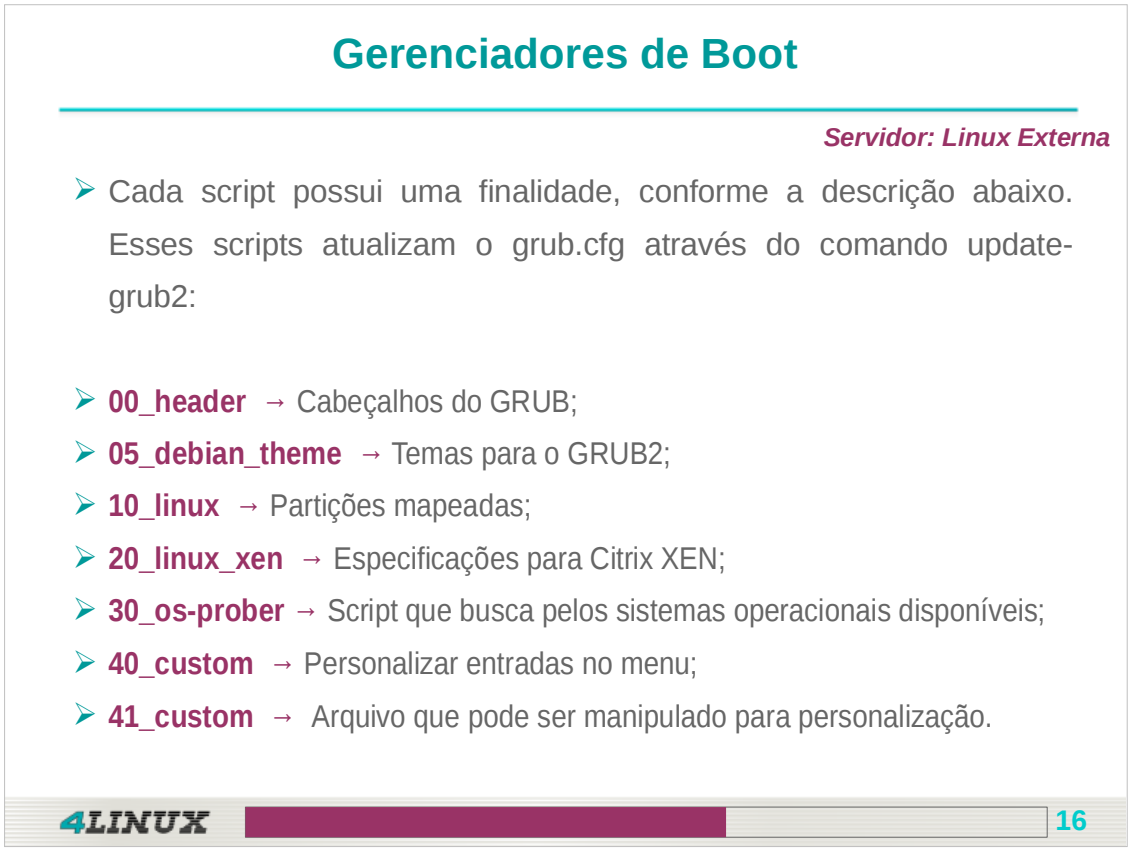
- O arquivo de configuração principal para alterar as configurações do menu é o /etc/default/grub.

- Existem vários arquivos para configurar o menu - /etc/default/grub mencionado acima e todos os arquivos da pasta /etc/grub.d/.

- Mudou a numeração das partições. A primeira partição agora é 1 em vez de 0. O primeiro dispositivo no entanto continua 0 (não mudou).

- Buscas automáticas para outros sistema operacionais como Windows sempre que update-grub é executado.

- Nenhuma mudança na configuração dos arquivos acontecerá até que o comando update-grub seja executado.



/etc/grub.d/ (diretório)

Os arquivos nessa pasta são lidos durante a execução do comando update-grub e suas instruções são incorporadas ao /boot/grub/grub.cfg.

A colocação dos ítens de menu no grub.cfg é determinada pela ordem em que os arquivos são executados nessa pasta. Arquivos com numeral no início são executados primeiro começando pelo menor. 10_linux é executado antes de 20_mentest que é executado antes de 40_custom.

Gerenciadores de Boot

Servidor: Linux Externa

Gerando o Arquivo grub.cfg:

O comando update-grub2 verifica o conteúdo dos arquivos descritos anteriormente, executando os scritps e criando o arquivo grub.cfg.

1 – Faça um teste apagando o arquivo grub.cfg:

```
1# rm -rf /boot/grub/grub.cfg
2# ls /boot/grub/ | grep grub.cfg
```

2 – Execute o comando update-grub2 para gerar um novo arquivo:

```
3# update-grub2
4# cat /boot/grub/grub.cfg
```


Anotações:

Gerenciadores de Boot

Servidor: Linux Externa

Colocando Imagem no Grub2:

Para adicionar uma imagem a inicialização faremos uma alteração no script **05_debian_theme**:

1 – Copie o logo da empresa dexter para uma pasta criada em /boot/grub/:

```
1# cd /root/logo
2# mkdir /boot/grub/imagem_bg/
3# mv dexterlogo.png /boot/grub/imagem_bg/
```

Adicionando imagens no GRUB2

No grub2 as restrições em relação a resolução de imagens são menores, dessa forma é possível adicionar uma imagem diretamente no grub pulando o processo de conversão.

/boot/grub/grub.cfg

É o que mais se assemelha ao /boot/grub/menu.lst do GRUB mas diferentemente desse o grub.cfg não se destina a ser editado. Cada seção é claramente delimitada com "(### BEGIN)" e a referência do arquivo na pasta /etc/grub.d a partir da qual a informação foi gerada. grub.cfg é atualizado executando o comando update-grub e é automaticamente modificado quando há uma atualização ou instalação/remoção de Kernel.

Por padrão, e sempre que o comando update-grub é executado, este arquivo é feito "somente leitura". Isto porque a intenção é que o arquivo não seja editado manualmente.

Gerenciadores de Boot

Servidor: Linux Externa

O arquivo /etc/default/grub:

Além dos scripts, uma saída para edição é o arquivo **"/etc/default/grub".** Sua organização é mais simples, o que facilita a criação de entradas e configurações.

1 – Verifique o conteúdo deste arquivo:

```
1# cat /etc/default/grub
```

NOTA: Alterações efetuadas aqui também serão validadas após execução do comando update-grub2.

Principais informações disponíveis no arquivo **/etc/default/grub:**

- GRUB_DEFAULT → Configura a entrada padrão do GRUB no menu de inicialização.

- GRUB_TIMEOUT → Configura o tempo

- GRUB_HIDDEN_TIMEOUT → Permite ocultar o menu do GRUB.

- GRUB_GFXMODE=640×480 → Descomente essa linha para mudar a resolução. Ela fornece resoluções suportadas pela placa de vídeo do usuário (640×480, 800×600, 1280×1024, etc).

- GRUB_DISABLE_LINUX_RECOVERY → Adicione ou descomente essa linha se não desejar o "Recovery" mode no menu.

Gerenciadores de Boot

Servidor: Linux Externa

Recuperação de Senhas de Root:

Caso um administrador perca a senha de root do servidor, é possível utilizar uma funcionalidade do próprio GRUB para definir uma nova senha.

Validaremos essa possibilidade utilizando o servidor WebServer Interno e Audit.

Para isso, reinicialize os servidores e acompanhe os procedimentos indicados pelo instrutor do curso.

Anotações:

Segurança no Grub2

Servidor: Linux Externa

- De forma similar ao procedimento efetuado no grub, também é possível definir uma senha para o grub2;
- Primeiro gere uma senha e a direcione para o sricpt 00_header:

```
1# (echo 123456;echo 123456) | grub-mkpasswd-pbkdf2 >>
/etc/grub.d/00_header
2# vim /etc/grub.d/00_header
```

- Em seguida, localize a senha gerada ao final do arquivo e edite conforme o próximo slide.

Anotações:

Segurança no Grub2

Servidor: Linux Externa

O final do seu arquivo deverá ficar no seguinte padrão:

```
cat << EOF
set superusers="user"
password_pbkdf2 user grub.pbkduuuf2.sha512.10000.FA7AFA733BF4619
B004F7ED4E09F5940ABF6DFA8DC169CC0337996FEC6DBD38501724D
DEBD568099DC2E636306CEBF6BFD424B58673699DC0B9C2DECE8C5
7C26.EE466A01C960477A05BD1EA4AAA5F44158542323A8B3BEA12B5
C10949FF7BFFB9C5414A19E68F24C60B2FA1F44B13EC78FEA896B95
866B7D68D5A963335929
EOF
# update-grub2
```

Salve o arquivo alterado, atualize o grub e tente acessá-lo reinciando o sistema.

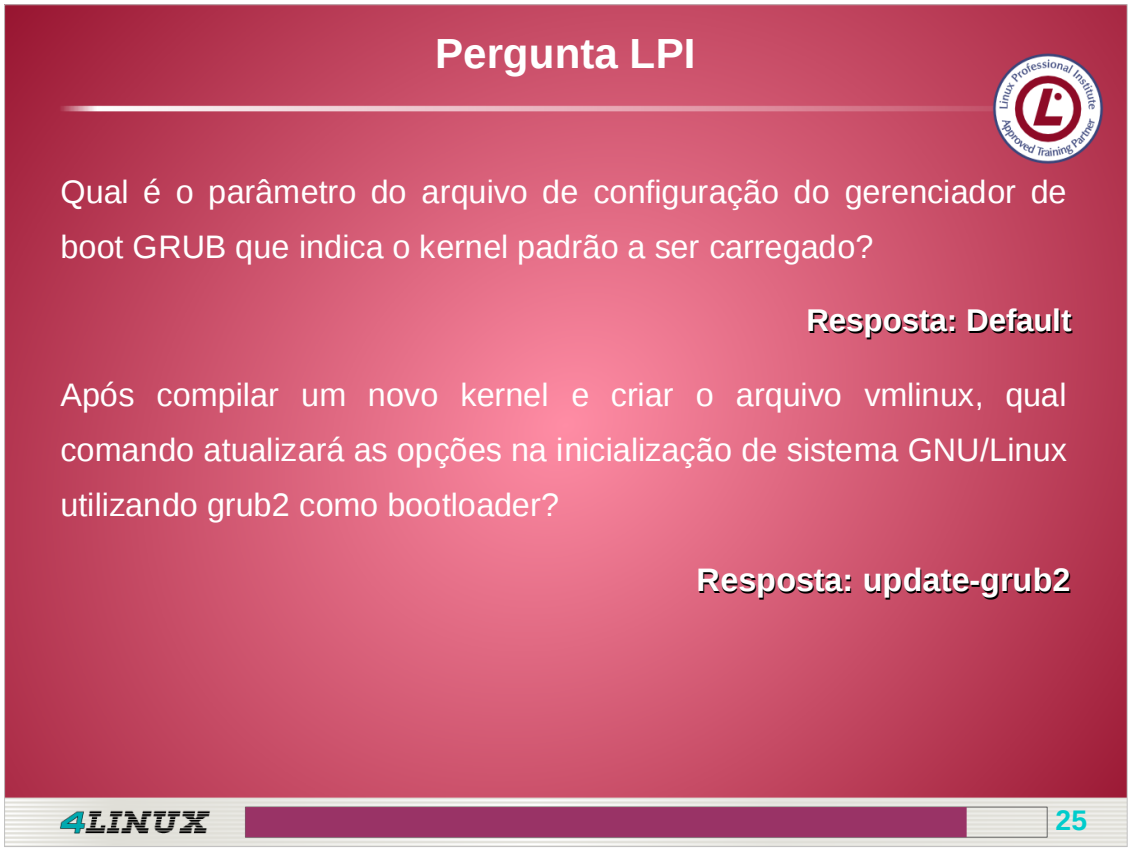
Anotações:

Pergunta LPI

Qual é o parâmetro do arquivo de configuração do gerenciador de boot GRUB que indica o kernel padrão a ser carregado?

Após compilar um novo kernel e criar o arquivo vmlinux, qual comando atualizará as opções na inicialização de sistema GNU/Linux utilizando grub2 como bootloader?

Anotações:



REPOSTA CORRETA: Default

Seja na versão 1 ou 2 do GRUB o parâmetro que representa a opção padrão de kernel a ser utilizado caso nada seja especificado na inicialização é a opção **“default”.**

REPOSTA CORRETA: update-grub2

O comando utilizado para atualizar o arquivo de configuração /boot/grub/grub.cfg é o comando **update-grub** ou **update-grub2.**

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participes das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!