Hardening Linux

Allan Piter Pressi

About

Allan Piter Pressi
@allanpitter
allanpitter@gmail.com
(11)97041-9911

THIS IS NOT A COMPUTER

IT'S MY WIFE.

(KEEP YOUR FILTHY HANDS OFF HER)


Google

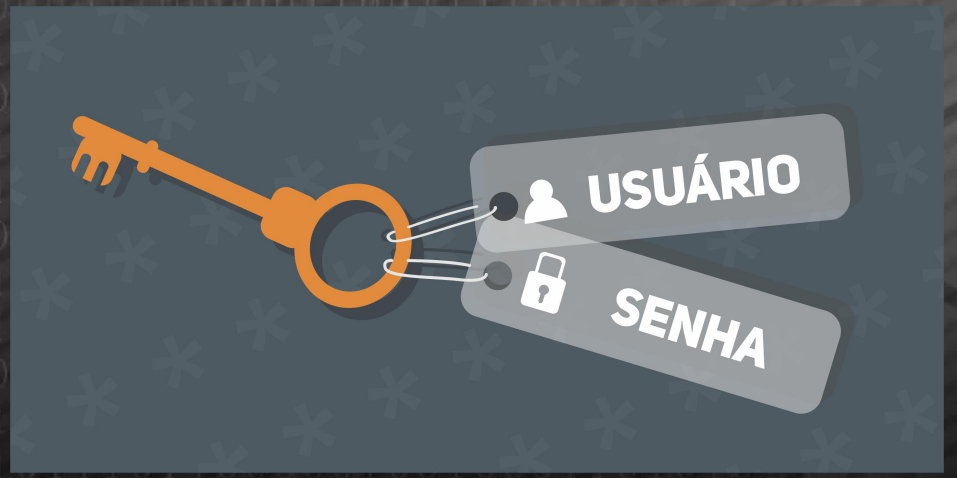

UBER


ifood


iRobot®


tinder


PAPAIZ
CR 25
PAPAIZ
CR 45
PAPAIZ
CR 70


USUÁRIO
SENHA

DEVOPS

SECDEVOPS

SECDEVDATAOPS

SECDEVDATAOPSCONT

SECDEVDATAOPSCONTFOR

HOW TO LEARNING ALL GH

Motivação

Um dos poucos mercados que podem competir com a tecnologia da computação quanto ao crescimento é aquele que usa a tecnologia com intenções criminosas ou maliciosas.

Motivação

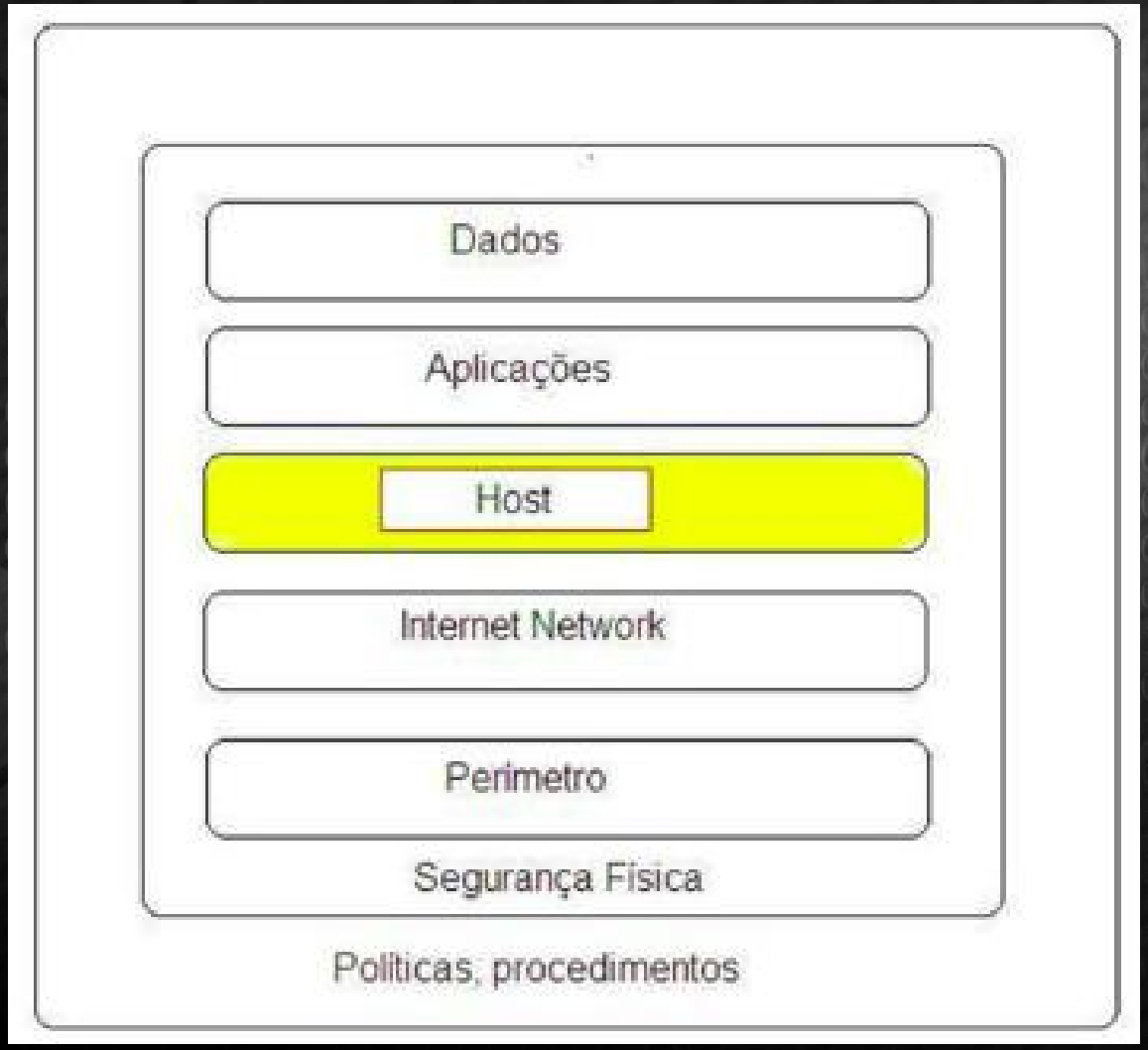
“Até mesmo um computador desligado pode ter seus dados roubados à distância. Basta que um engenheiro social habilidoso convença alguém a ligar o equipamento”.
Kevin Mitnick
Engenheiro Social

Defesa em Profundidade

Segurança integrada

A segurança integrada fornece um sistema lógico e uma visão holística dos desafios de segurança da organização atual. Esse método combina múltiplas tecnologias de segurança, utilizando o princípio de defesa em profundidade.

Segurança em Profundidade



Segurança - Tecnologias

Firewall	Serviços IPS/IDS	Analisadores de LOGs	Controle de Acesso
Auditoria	Services Pack/Updates	Antivírus Antispyware	Serviços de Rede
Código Seguro	Usuário	"HACKERS"	Governo

Hardening

Técnica de Segurança para fortalecer um sistema de forma a torná-lo menos vulnerável, também conhecido como blindagem.

Onde ocorrem problemas

- Serviços de Rede
- Sistemas Operacionais

Segurança

Serviços:
Programas que geralmente são servidores e ficam escutando determinadas portas para realizar transações.
São eles os mais atacados
Ex.: SNMP, SMTP, POP, HTTP(s), SSH, FTP, TELNET, NIS, NFS, ...

Segurança

Sistemas Operacionais: onde os serviço rodam
Ex.: Linux, SCO, Solaris, Window, NT, AIX, Digital , ...
Para possibilitar a interoperabilidade entre serviços e SOs, definem-se padrões
Request for comments - RFCs

Segurança

A maioria da configuração dos sistemas UNIX é feita através da edição de arquivos;
Saber qual arquivo deve ser mexido é uma tarefa árdua;
Porém é melhor do que mexer no registro do Windows;
Antes de cada configuração procure ler/estudar sobre o funcionamento do serviço/aplicativo.

Segurança

Procure manter sempre uma copia da configuração anterior antes de alterar qualquer arquivo;
Geralmente tais arquivos ficam localizados no diretório /etc;
São arquivos em texto puro;

Como tudo começou

- Na década de 60 não existia interoperabilidade
- Multiplexed Information and Computing Service (MULTICS), multitarefa
- O projeto MULTICS era muito caro
- Thompson e Ritchie buscavam um sistema mais viável
- Sem recursos financeiros, adotaram um velho PDP-7, da DEC
- O protótipo, desenvolvido em Assembler, recebeu o nome UNIX

A evolução do Unix

- Inicialmente escrito em Assembler, portado para linguagem B, baseada em BCPL
- Thompson e Ritchie criaram uma versão melhorada da linguagem B, chamada de C
- O UNIX foi reescrito num PDP-11, em C, e começou a transformar-se em um sistema de propósito geral
- Compilador, biblioteca, shell e sistema de arquivos
- Seria portado posteriormente a sistemas menores e até microcomputadores

O projeto GNU

- Criado por Richard Stallman, administrador de sistemas do MIT
- A idéia era fornecer software “livre” para UNIX
- Gnu’s Not UNIX e a Free Software Foundation fundados na década de 80
- Compilador (gcc), biblioteca (glibc) e shell (bash) foram os primeiros softwares a ser escritos
- Havia a necessidade de um kernel, que o projeto só incluiria a meados dos anos 90

O Projeto Linux

- Criado por Linus Torvalds, estudante da Universidade de Helsinki
- Estudo do modo protegido do processador 386

Lançado na Internet em 1991

- Adotado por dezenas, hoje milhões, de pessoas no mundo todo
- Colaborações de programadores independentes
- Kernel do sistema operacional, precisava de aplicações e utilitários

GNU/Linux

Combinação do kernel escrito por Torvalds com os utilitários e aplicações do projeto GNU da FSF
Publicado sob proteção da GNU GPL (General Public License)
Diversas empresas criaram “distribuições” com seu conjunto preferido de kernel e aplicações Linux
http://distrowatch.com/stats.php (791), Hoje ≃ 300.

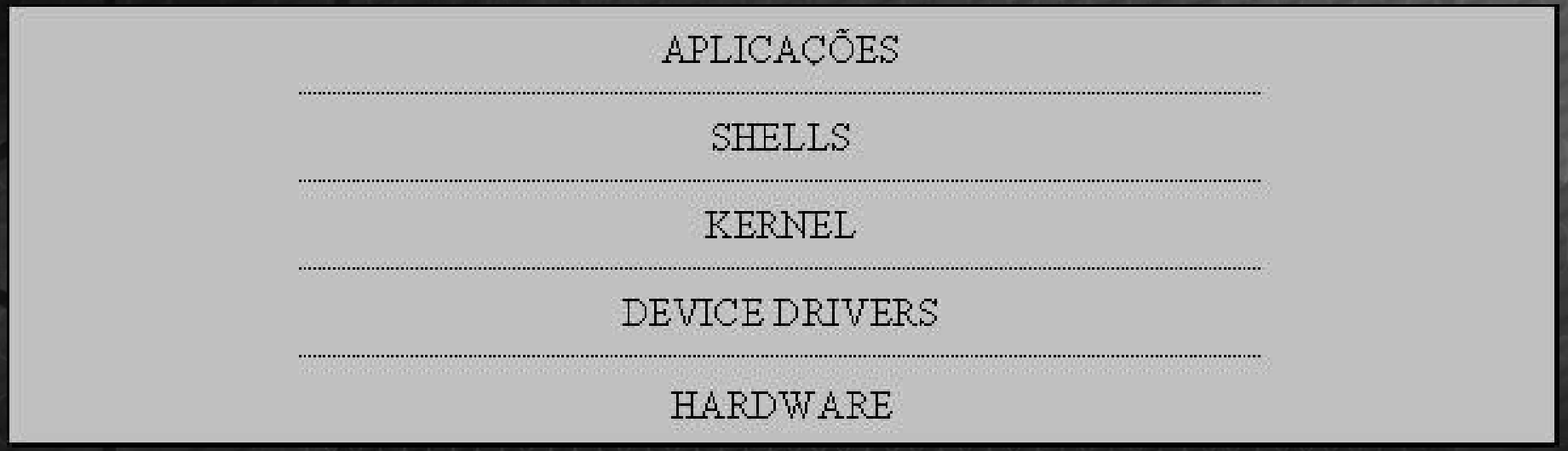
Licença GPL

- Chamada de *copyleft* pela sua natureza aberta
- Permite cópia, modificação, redistribuição e recompilação do software
- Exige distribuição do código fonte e da própria licença com seus devidos créditos
- Pode-se ganhar dinheiro com “free software” (software livre)

Arquitetura de Sistemas Linux/Unix

- Sistema multitarefa, multiplexação por divisão de tempo
- Sistema multiusuário, pseudoterminais
- Modular e baseado em programas pequenos
- Tarefas complexas executadas com combinações de diversos pequenos programas

Arquitetura Linux/Unix



Classificação DoD

Classificação de “trusted computing base”, do Orange Book, 1985

http://www.dynamoo.com/orange/fulltext.htm

Avalia 6 requisitos de segurança fundamentais:

1. Security Policy
2. Marking
3. Identification
4. Accountability
5. Assurance
6. Continuous Protection

Classificação DoD

Sistemas classificados segundo critério comum de avaliação, em 4 divisões:

A - Verified Protection

B - Mandatory Access Control

C - Discretionary Access Control

D - Minimal Protection

Contém referências de implementação de mecanismos de segurança

D - Minimal Protection

- Contém somente uma classe
- Reservada para aqueles sistemas que foram avaliados mas não se enquadraram em nenhuma classificação superior

C - Discretionary Access Control

- Separa usuários e dados,
- Utiliza algum tipo de controle capaz de forçar limitação de acesso baseado em usuário, ou seja, que usuário pode acessar que dado
- O controle de acesso a recursos é definido pelo dono do recurso

C - Discretionary Access Control

- Dividido em duas classes, C1 e C2

  C1
  - Identificação e autenticação de usuário por senha
  - Checagem de integridade do TCB
  - permissões simples DAC
  - Uso opcional de ACL
  - Documentação da segurança para usuários, administradores e para realização de testes

  C2
  - Todos da classe C1
  - ACLs
  - Proteção contra reutilização de objetos eliminados
  - Trilhas de auditoria (contabilização)

B - Mandatory Access Control

- A proteção do sistema é obrigatória, e não à discrição do usuário
- Se caracteriza pelo uso de rótulos (label) para classificação das informações, segundo o seu grau de sensibilidade.
- Tem como requisito, manter a integridade dos rótulos

B - Mandatory Access Control

- Se divide em 3 classes:
- B1 - Labeled Security Protection
  Mesmos requisitos de C2
  Suporte a rotulação dos dados
  Controle de integridade dos rótulos
  Controle de acesso aos objetos do sistema
  Controle de acesso sobre recursos e usuários
  Cada elemento do sistema tem um rótulo associado e os usuários têm diferentes “níveis de acesso”
  As permissões nos objetos são dadas de acordo com “sensitivity labels”

B - Mandatory Access Control

- B2 - Structured Protection
  Todos os tipos de controles de acesso devem ser implementados e aplicados a todos os usuários e recursos;
  Separação de dados em unidades classificadas;
  Permite a comunicação segura entre o sistema e o usuário
  Fornecer um processo de análise e auditoria de atualizações e de correções das versões dos componentes do sistema
  Possui conjunto de testes de segurança melhorados
  Tidos como “Relativamente resistentes à penetração”
  “Labels” hierárquicas
  Maiores informações de auditoria

B - Mandatory Access Control

- B3 - Security Domains
  Possui monitor de referência para controle de todos os acessos dos usuários aos recursos;
  Procedimentos para recuperação do sistema
  Documentação do processo de recuperação
  Sinalização de eventos
  Análise de segurança automatizada;
  Busca eliminar falhas de design e minimizar falhas de implementação - Reescrever o sistema
  Considerados “Altamente resistentes a penetrações”

A - Verified Protection

- Possui somente uma classe, com as seguintes características:
  Utilização de métodos formais para a verificação da segurança, garantindo que o controle de acesso pode proteger toda e qualquer informação sensível existente no sistema
  Documentação formal que demonstra que os requisitos de segurança são atendidos em todas as fases do projeto, desenvolvimento e implementação do sistema.

Certificados pela NSA

- C2
  WindowsNT (4.0 SP6a C2 Update)
  VMS
- B1
  HP-UX BLS
  Trusted IRIX
- B2
  Trusted XENIX
- B3
  Getronics XTS/300

Premissas de Segurança Unix

- Sistemas UNIX, em geral, conformam com a classificação C1 do DoD/NSA
- Adição de recursos de níveis superiores da classificação deve ser considerada em função da criticidade do sistema
  ex: ACLs, auditoria, MAC
  Normalmente fornecidos através de patches ou pacotes do sistema operacional
- Os sistemas UNIX não são automaticamente mais seguros que outros sistemas
- É necessária administração consciente e atenta

Usuários e Grupos

Cada usuário possui um UserID (UID), usado para autenticação e criação de contexto de execução dos programas

Usuário root, o superusuário, o mais importante

Usuários podem ser colocados em grupos para melhor definir o acesso a recursos

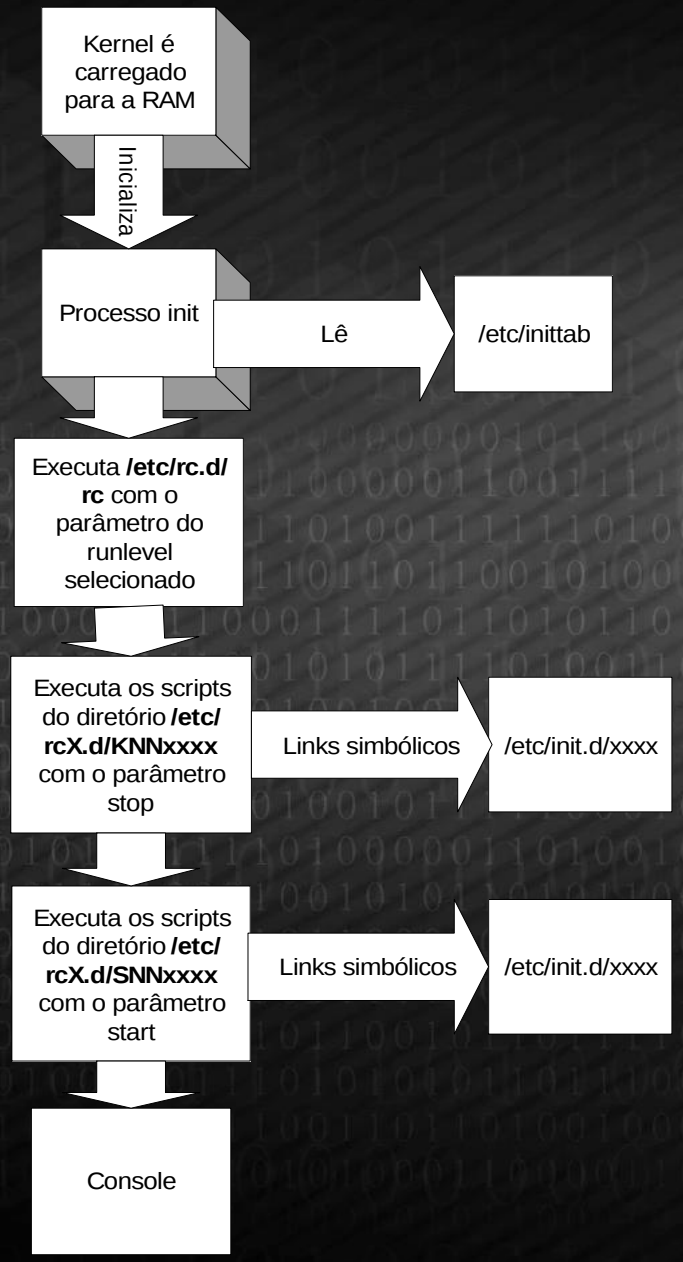
Conceito de Processos

- Instância de execução de um programa
- Pode ser criado e destruído
- É sempre filho de outro processo (exceção do init)
- Comunica-se com outros processos

Ambiente de um Processo

- Process ID (PID e Parent Process ID (PPID)
- Arquivos abertos
- Memória alocada
- Diretório de trabalho
- User ID e Group ID
- Variáveis de ambiente

Processo de Inicialização



Planejamento de Segurança em Linux

- A segurança é um processo e não um projeto
- Políticas e procedimentos devem apoiar a tecnologia; confiar apenas na tecnologia traz falsa impressão de segurança
- Controle de acesso de software não substitui controle de acesso físico
- Resolver problemas de instalação é mais difícil que planejar

A Instalação do Sistema

- Verificar se os devidos controles de acesso estão em uso
- Instalar o sistema de forma segura desde o início
  Prever espaço em disco, inclusive para logs
  Prever utilização de recursos em situação de ataque
  Instalar apenas o software necessário
  Não permitir a execução ilegal ou desnecessária de serviços
  Executar os serviços necessários de forma controlada
  Proteger usuários e senhas
  Implementar medidas de auditoria

Instalação do Linux

- Separar sistemas de arquivos de acordo com seu uso; logs preferencialmente em sistemas separados
- Escolher cuidadosamente todo o software envolvido
- Alguns sistemas UNIX não permitem a escolha de todo o software a ser instalado
  software pode ser instalado/desinstalado posteriormente
  cada distribuição possui suas ferramentas de instalação e remoção de software: rpm, apt, setld, smit

Instalação do Linux

- Software desnecessário pode gerar problemas
  Desperdício de recursos
  Serviços ilegais ou perigosos
  Vazamento de informações
  Invasões por exploits
- Em caso de servidores sem usuários interativos, criar na instalação usuários para administração
  Efetuar o “login” como o usuário comum, e somente utilizar o usuário root quando necessário
  A maioria dos UNIX não exige criação de usuários comuns, o que incentiva a má prática

Estrutura de Diretórios do Linux

- O diretório raiz (/)
- Todos os arquivos e diretórios do sistema Linux instalado no computador partem de uma única origem: o diretório raiz. Mesmo que estejam armazenados em outros dispositivos físicos, é a partir do diretório raiz – representado pela barra (/) – que você poderá acessá-los.
- Também vale lembrar que o único usuário do sistema capaz de criar ou mover arquivos do diretório raiz é o root, ou seja, o usuário-administrador. Isso evita que usuários comuns cometam erros e acabem comprometendo a integridade de todo o sistema de arquivos.

Estrutura de Diretórios do Linux

- Binários executáveis: /bin

- No diretório /bin estão localizados os binários executáveis que podem ser utilizados por qualquer usuário do sistema. São comandos essenciais, usados para trabalhar com arquivos, textos e alguns recursos básicos de rede, como o cp, mv, ping e grep.

Estrutura de Diretórios do Linux

- Binários do sistema: /sbin

- Assim como o /bin, este diretório armazena executáveis, mas com um diferencial: são aplicativos utilizados por administradores de sistema com o propósito de realizar funções de manutenção e outras tarefas semelhantes. Entre os comandos disponíveis estão o ifconfig, para configurar e controlar interfaces de rede TCP/IP, e o fdisk, que permite particionar discos rígidos, por exemplo.

Estrutura de Diretórios do Linux

- Programas diversos: /usr

- Se você não encontrar um comando no diretório /bin ou /sbin, ele certamente está aqui. O /usr reúne executáveis, bibliotecas e até documentação de softwares usados pelos usuários ou administradores do sistema. Além disso, sempre que você compilar e instalar um programa a partir do código-fonte, ele será instalado nesse diretório.

Estrutura de Diretórios do Linux

- Configurações do sistema: /etc

- No diretório /etc ficam arquivos de configuração que podem ser usados por todos os softwares, além de scripts especiais para iniciar ou interromper módulos e programas diversos. É no /etc que se encontra, por exemplo, o arquivo resolv.conf, com uma relação de servidores DNS que podem ser acessados pelo sistema, com os parâmetros necessários para isso.

Estrutura de Diretórios do Linux

- Bibliotecas: /lib

- Neste ponto do sistema de arquivos ficam localizadas as bibliotecas usadas pelos comandos presentes em /bin e /sbin. Normalmente, os arquivos de bibliotecas começam com os prefixos ld ou lib e possuem "extensão" so.

Estrutura de Diretórios do Linux

- Opcionais: /opt

- Aplicativos adicionais, que não são essenciais para o sistema, terminam neste diretório.

Estrutura de Diretórios do Linux

- Aquivos pessoais: /home

- No diretório /home ficam os arquivos pessoais, como documentos e fotografias, sempre dentro de pastas que levam o nome de cada usuário. Vale notar que o diretório pessoal do administrador não fica no mesmo local, e sim em /root.

Estrutura de Diretórios do Linux

- Inicialização: /boot

- Arquivos relacionados à inicialização do sistema, ou seja, o processo de boot do Linux, quando o computador é ligado, ficam em /boot.

Estrutura de Diretórios do Linux

- Volumes e mídias: /mnt e /media

- Para acessar os arquivos de um CD, pendrive ou disco rígido presente em outra máquina da rede, é necessário "montar" esse conteúdo no sistema de arquivos local, isso é, torná-lo acessível como se fosse apenas mais um diretório no sistema.

- Em /media ficam montadas todas as mídias removíveis, como dispositivos USB e DVDs de dados. Já o diretório /mnt fica reservado aos administradores que precisam montar temporariamente um sistema de arquivos externo.

Estrutura de Diretórios do Linux

- Serviços: /srv
- Dados de servidores e serviços em execução no computador ficam armazenados dentro desse diretório.

Estrutura de Diretórios do Linux

- Arquivos de dispositivos: /dev

- No Linux, tudo é apresentado na forma de arquivos. Ao plugar um pendrive no computador, por exemplo, um arquivo será criado dentro do diretório /dev e ele servirá como interface para acessar ou gerenciar o drive USB. Nesse diretório, você encontra caminhos semelhantes para acessar terminais e qualquer dispositivo conectado ao computador, como o mouse e até modems.

Estrutura de Diretórios do Linux

- Arquivos variáveis: /var

- Todo arquivo que aumenta de tamanho ao longo do tempo está no diretório de arquivos variáveis. Um bom exemplo são os logs do sistema, ou seja, registros em forma de texto de atividades realizadas no Linux, como os logins feitos ao longo dos meses.

Estrutura de Diretórios do Linux

- Processos do sistema: /proc

- Lembra da história de que tudo funciona como um arquivo no Linux? Pois o /proc é a prova disso. Nesse diretório são encontrados arquivos que revelam informações sobre os recursos e processos em execução no sistema. Quer um exemplo? Para saber há quanto tempo o Linux está sendo usado desde a última vez em que foi iniciado, basta ler o arquivo /proc/uptime.

Estrutura de Diretórios do Linux

- Arquivos temporários: /tmp

- Arquivos e diretórios criados temporariamente tanto pelo sistema quanto pelos usuários devem ficar nesse diretório. Boa parte deles é apagada sempre que o computador é reiniciado.

- Como fica fácil perceber, os nomes dos diretórios dão dicas do que pode ser encontrado em seu interior e, com alguns meses de uso, você estará navegando por eles com facilidade.

Estrutura de Diretórios do Linux

- Serviços: /usr
- Serviços e utilitários compatíveis com o Unix.

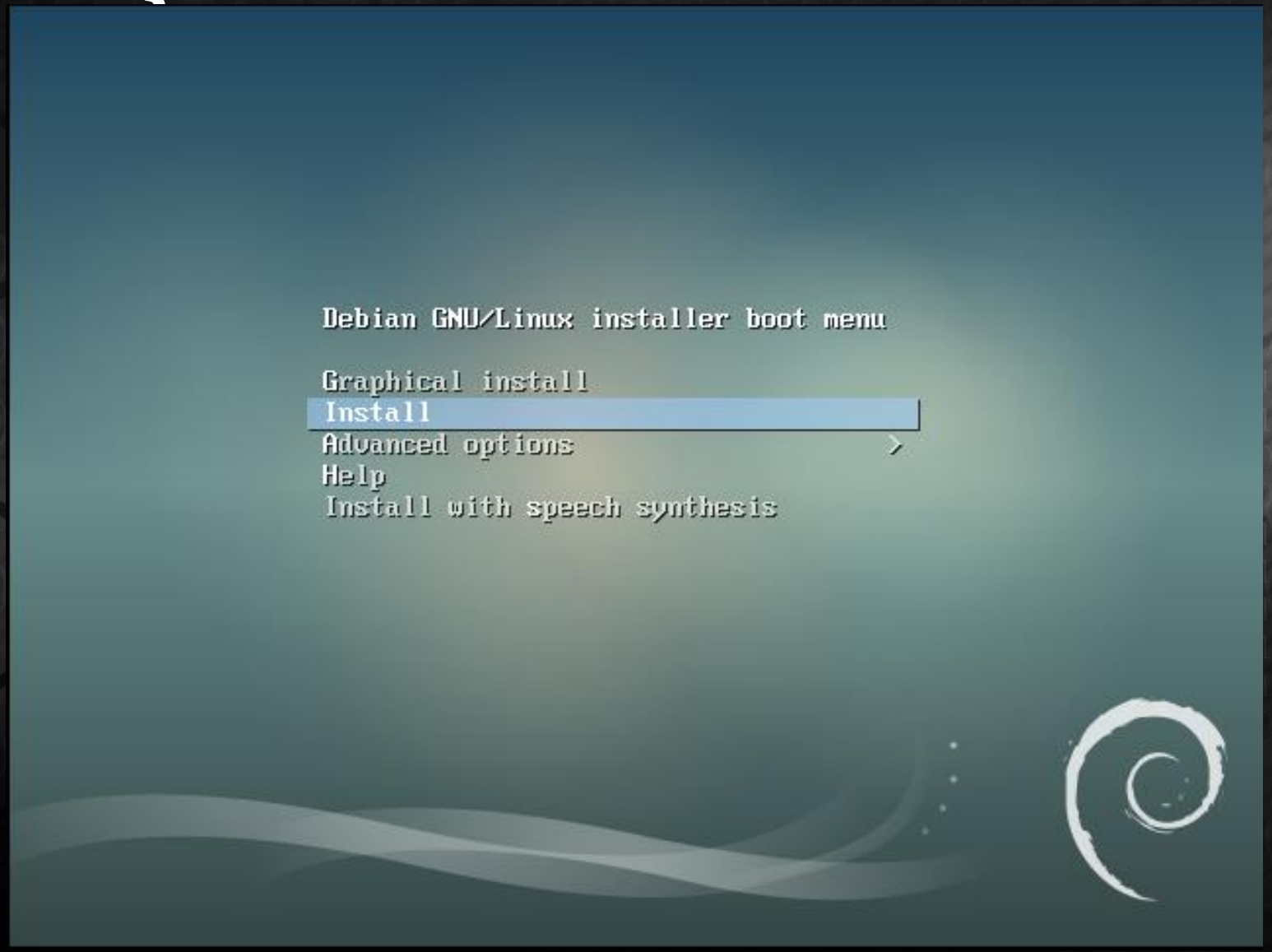
Estrutura de Diretórios do Linux

- Serviços: /swap
- Troca de Arquivos.

HANDS ON

Instalação do Sistema Debian

Instalação


Debian GNU/Linux installer boot menu
Graphical install
Install
Advanced options
Help
Install with speech synthesis

[!!] Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

C	-	No localization
Albanian	-	Shqip
Arabic	-	عربي
Asturian	-	Asturianu
Basque	-	Euskara
Belarusian	-	Беларуская
Bosnian	-	Bosanski
Bulgarian	-	Български
Catalan	-	Català
Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
German	-	Deutsch
Greek	-	Ελληνικά

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

[!!] Selecionar sua localidade

A localidade selecionada será usada para configurar seu fuso horário e também para, por exemplo, selecionar o "locale" do sistema. Normalmente este deveria ser o país onde você vive.

Esta é uma pequena lista de localidades baseada no idioma selecionado. Escolha "outro" se sua localidade não está listada.

País, território ou área:

- Brasil
- Portugal
- outro

<Voltar>

Instalação


[!!] Configure o teclado
Mapa de teclado a ser usado:
Inglês Americano
Albanês
Árabe
Asturiano
Bangladesh
Bielorrusso
Bengali
Belga
Bósnio
Português Brasileiro
Inglês Britânico
Búlgaro (layout BDS)
Búlgaro (layout fonético)
Birmanês
Francês Canadense
Multilinguagem canadense
Catalão
Chinês
Croata
Tcheco
Dinamarquês
Holandês
Dvorak
Butanês
Esperanto
Estoniano
<Voltar>

Instalação

[!] Configurar a rede

Por favor, informe o nome de máquina ("hostname") para este sistema.

O nome de máquina ("hostname") é uma palavra única que identifica seu sistema na rede. Se você não sabe qual deve ser o nome de sua máquina, consulte o seu administrador de redes. Se você está configurando sua própria rede doméstica, você pode usar qualquer nome aqui.

Nome de máquina:

servidor

<Voltar> <Continuar>

Instalação

[!] Configurar a rede

O nome do domínio é a parte de seu endereço Internet à direita do nome de sua máquina. Geralmente algo que finaliza com .com.br, .net.br, .edu.br, .org.br, .com, .net, .edu ou .org. Se você está configurando uma rede doméstica, você pode usar qualquer nome, mas certifique-se de usar o mesmo nome de domínio em todos os seus computadores.

Nome de domínio:

<Voltar> <Continuar>

[!!] Configurar usuários e senhas

Você precisa definir uma senha para o 'root', a conta administrativa do sistema. Um usuário malicioso ou não qualificado com acesso root pode levar a resultados desastrosos, portanto você deve tomar o cuidado de escolher uma senha que não seja fácil de ser adivinhada. Essa senha não deve ser uma palavra encontrada em dicionários ou uma palavra que possa ser facilmente associada a você.

Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.

O usuário root não deverá ter uma senha em branco. Se você deixar este campo vazio, a conta do root será desabilitada e a conta do usuário inicial do sistema receberá o poder de tornar-se root usando o comando "sudo".

Note que você não poderá ver a senha enquanto a digita.

Senha do root:

[ ] Mostrar a senha

<Voltar> <Continuar>

Instalação

[!!] Configurar usuários e senhas

Por favor, informe novamente a mesma senha de root para verificar se você digitou-a corretamente.

Informe novamente a senha para verificação:

[ ] Mostrar a senha

<Voltar> <Continuar>

Instalação

[!!] Configurar usuários e senhas

Uma conta de usuário será criada para você usar no lugar da conta de root para tarefas não-administrativas.

Por favor, informe o nome real deste usuário. Esta informação será usada, por exemplo, como a origem padrão para mensagens enviadas por este usuário bem como por qualquer programa que exiba ou use o nome real do usuário. Seu nome completo é uma escolha razoável.

Nome completo para o novo usuário:

<Voltar> <Continuar>

Instalação

[!!] Configurar usuários e senhas

Informe um nome de usuário para a nova conta. Seu primeiro nome é uma escolha razoável. O nome de usuário deverá ser iniciado com uma letra minúscula, que pode ser seguida de qualquer combinação de números e mais letras minúsculas.

Nome de usuário para sua conta:

usuario

<Voltar> <Continuar>

Instalação

[!!] Configurar usuários e senhas

Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.

Escolha uma senha para o novo usuário:

******_

[ ] Mostrar a senha

<Voltar> <Continuar>

Instalação

[!!] Configurar usuários e senhas

Por favor, informe novamente a mesma senha de usuário para verificar se você digitou-a corretamente.

Informe novamente a senha para verificação:

******_

[ ] Mostrar a senha

<Voltar> <Continuar>

[!] Configurar o relógio

Se o fuso horário desejado não estiver listado, por favor, volte ao passo "Escolher idioma" e selecione o país que usa o fuso horário desejado (o país onde você vive ou está localizado).

Selecione um estado ou província para definir seu fuso horário:

Ceará
Distrito Federal
Espírito Santo
Fernando de Noronha
Goiás
Maranhão
Minas Gerais
Mato Grosso do Sul
Mato Grosso
Pará
Paraíba
Pernambuco
Piauí
Paraná
Rio de Janeiro
Rio Grande do Norte
Rondônia
Roraima
Rio Grande do Sul
Santa Catarina
Sergipe
São Paulo

<Voltar>

Instalação

[!!] Particionar discos

O instalador pode guiá-lo através do particionamento de um disco (usando diferentes esquemas padrão) ou, caso você prefira, você pode fazê-lo manualmente. Com o particionamento assistido você ainda tem uma chance de, posteriormente, revisar e personalizar os resultados.

Se você optar pelo particionamento assistido para um disco inteiro, em seguida será solicitado qual disco deverá ser usado.

Método de particionamento:

Assistido - usar o disco inteiro
Assistido - usar o disco inteiro e configurar LVM
Assistido - usar disco todo e LVM criptografado
Manual

<Voltar>

Instalação

[!!] Particionar discos

Note que todos os dados no disco que você selecionar serão apagados, mas não antes que você tenha confirmado que realmente deseja fazer as mudanças.

Selecione o disco a ser particionado:

SCSI1 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

<Voltar>

Instalação

[!] Particionar discos

Selecionado para particionamento:

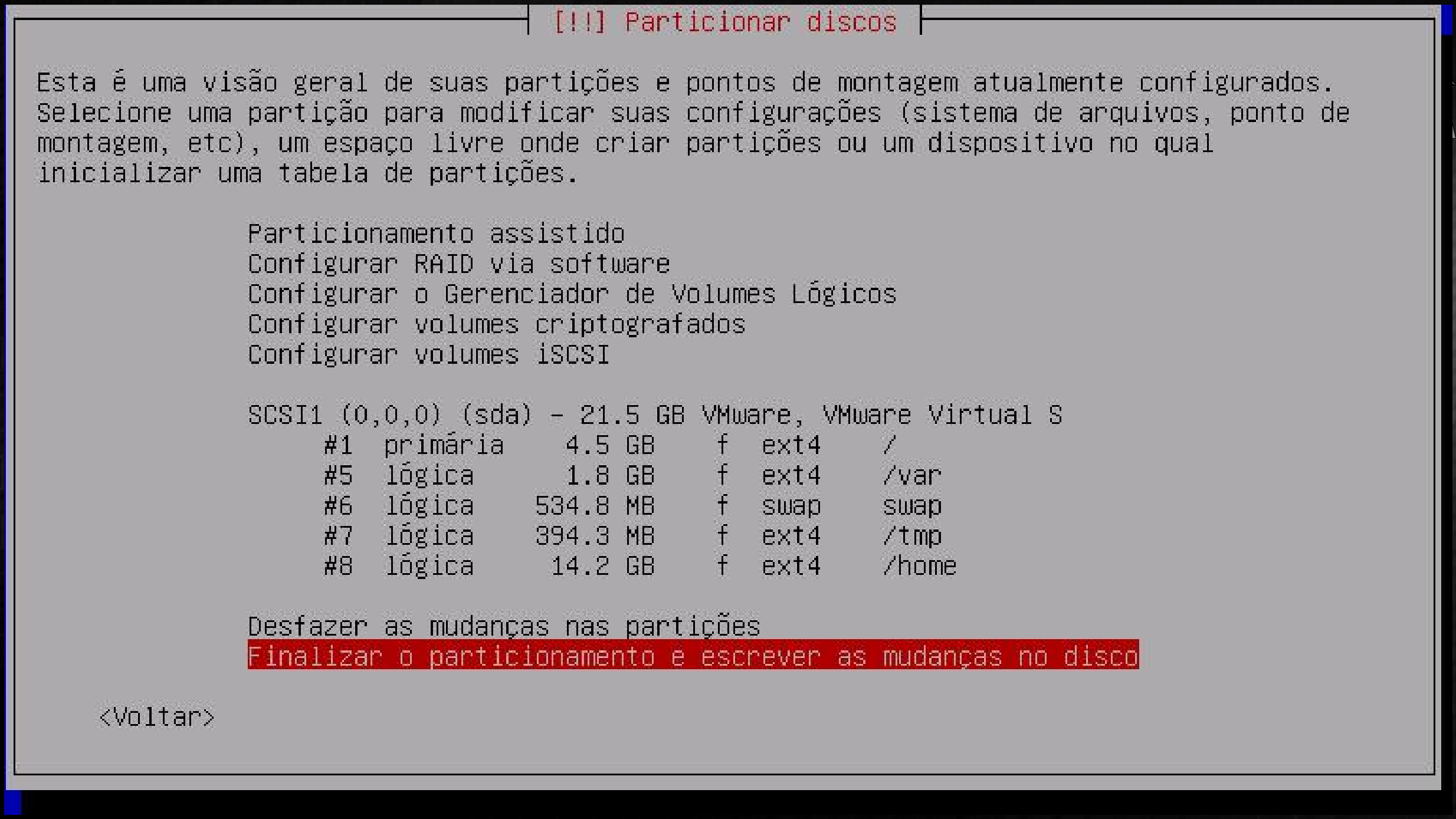
SCSI1 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB

O disco pode ser particionado usando um dentre diversos esquemas diferentes. Se você não tiver certeza, escolha o primeiro esquema.

Esquema de particionamento:

Todos os arquivos em uma partição (para iniciantes)
Partição /home separada
Partições /home, /var e /tmp separadas

<Voltar>


[!!] Particionar discos
Esta é uma visão geral de suas partições e pontos de montagem atualmente configurados. Selecione uma partição para modificar suas configurações (sistema de arquivos, ponto de montagem, etc), um espaço livre onde criar partições ou um dispositivo no qual inicializar uma tabela de partições.
Particionamento assistido
Configurar RAID via software
Configurar o Gerenciador de Volumes Lógicos
Configurar volumes criptografados
Configurar volumes iSCSI
SCSI1 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
#1 primária 4.5 GB f ext4 /
#5 lógica 1.8 GB f ext4 /var
#6 lógica 534.8 MB f swap swap
#7 lógica 394.3 MB f ext4 /tmp
#8 lógica 14.2 GB f ext4 /home
Desfazer as mudanças nas partições
Finalizar o particionamento e escrever as mudanças no disco
<Voltar>

Instalação

[!!] Particionar discos

Se você continuar, as mudanças listadas abaixo serão escritas nos discos. Caso contrário, você poderá fazer mudanças adicionais manualmente.

As tabelas de partição dos dispositivos a seguir foram mudadas:
   SCSI1 (0,0,0) (sda)

As seguintes partições serão formatadas:
   partição #1 de SCSI1 (0,0,0) (sda) como ext4
   partição #5 de SCSI1 (0,0,0) (sda) como ext4
   partição #6 de SCSI1 (0,0,0) (sda) como swap
   partição #7 de SCSI1 (0,0,0) (sda) como ext4
   partição #8 de SCSI1 (0,0,0) (sda) como ext4

Escrever as mudanças nos discos?

    <Sim> <Não>

Instalação


Instalando o sistema básico
48%
Desempacotando debian-archive-keyring...

Instalação

[!] Configurar o gerenciador de pacotes

Seu CD ou DVD de instalação foi lido; sua identificação é:

Debian GNU/Linux 9.5.0 _Stretch_ - Official amd64 NETINST 20180714-10:25

Agora, você tem a opção de ler CDs ou DVDs adicionais para serem usados pelo gerenciador de pacotes (apt). Normalmente, eles deveriam ser do mesmo conjunto do CD/DVD de instalação. Se você não possui CDs ou DVDs adicionais, este passo pode ser ignorado.

Se você deseja ler outro CD ou DVD, por favor, insira-o agora.

Ler outro CD ou DVD?

<Voltar> <Sim> <Não>

[!] Configurar o gerenciador de pacotes

O objetivo é encontrar um espelho do repositório Debian que esteja perto de você na rede -- esteja ciente de que países próximos, ou mesmo seu próprio país, podem não ser a melhor escolha.

País do espelho do repositório Debian:

digitar informação manualmente
Alemanha
Argentina
Armênia
Austrália
Bangladesh
Bielo-Rússia
Brasil
Bulgária
Bélgica
Canadá
Cazaquistão
Chile
China
Cingapura
Colômbia
Coreia, República da
Costa Rica
Croácia
Czechia
Dinamarca
El Salvador

<Voltar>

[!] Configurar o gerenciador de pacotes

Por favor, selecione um espelho do repositório Debian. Você deverá usar um espelho em seu país ou região se não souber qual espelho possui a melhor conexão de Internet até você.

Normalmente, ftp.<código de seu país>.debian.org é uma boa escolha.

Espelho do repositório Debian:

ftp.br.debian.org
debian.c3sl.ufpr.br
debs.pelotas.ifsul.edu.br
sft.if.usp.br
deb.debian.org
debian-archive.trafficmanager.net
debian.pop-sc.rnp.br
linorg.usp.br
mirror.unesp.br
alcateia.ufscar.br

<Voltar>

Instalação

[!] Configurar o gerenciador de pacotes

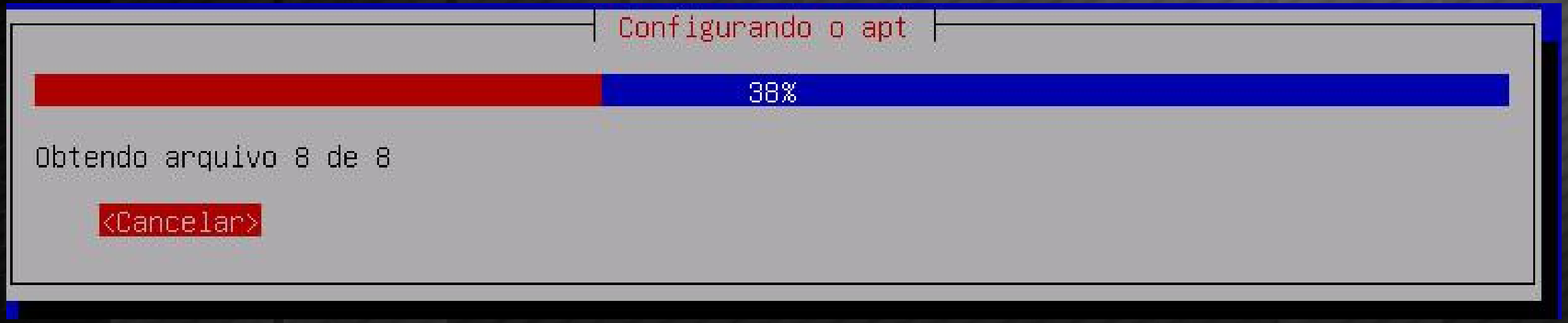
Se você precisa usar um proxy HTTP para acessar locais fora de sua rede local, insira a informação de proxy aqui. Caso contrário, deixe em branco.

A informação sobre o proxy deverá ser fornecida no formato padrão "http://[[usuário][:senha]@]máquina[:porta]/".

Informação sobre proxy HTTP (deixe em branco para nenhum):

<Voltar> <Continuar>

Instalação



Instalação

[!] Configurando popularity-contest

O sistema pode fornecer anonimamente aos desenvolvedores da distribuição estatísticas sobre os pacotes mais utilizados em seu sistema. Esta informação influencia decisões como quais pacotes deverão ser colocados no primeiro CD da distribuição.

Caso você opte por participar, o script de envio automático será executado uma vez por semana, enviando as estatísticas para os desenvolvedores da distribuição. As estatísticas coletadas podem ser visualizadas em http://popcon.debian.org/.

Sua escolha pode ser modificada posteriormente através da execução do comando "dpkg-reconfigure popularity-contest".

Participar do concurso de utilização de pacotes ?

<Sim> <Não>


[!] Seleção de software
No momento, somente o básico do sistema está instalado. Para refinar seu sistema e deixá-lo de acordo com suas necessidades, você pode optar por instalar uma ou mais das coleções de software pré-definidas a seguir.
Escolha o software a ser instalado:
[ ] ambiente de área de trabalho no Debian
[ ] ... GNOME
[ ] ... Xfce
[ ] ... KDE
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] servidor web
[ ] servidor de impressão
[ ] servidor SSH
[*] utilitários de sistema padrão
<Continuar>

Instalação

[!] Instalar o carregador de inicialização GRUB em um disco rígido

Parece que esta nova instalação será o único sistema operacional neste computador. Se isso for verdade, será seguro instalar o carregador de inicialização GRUB no registro mestre de inicialização de seu primeiro disco rígido.

Aviso: Se o instalador falhou ao detectar outro sistema operacional que esteja presente em seu computador, modificar o registro mestre de inicialização fará com que os sistemas operacionais não detectados não possam ser inicializados temporariamente, porém o GRUB poderá ser configurado posteriormente para permitir a inicialização dos outros sistemas operacionais.

Instalar o carregador de inicialização GRUB no registro mestre de inicialização?

<Voltar> <Sim> <Não>

[!] Instalar o carregador de inicialização GRUB em um disco rígido

Você precisa fazer com que seu novo sistema recém-instalado seja inicializável, instalando o carregador de inicialização GRUB em um dispositivo inicializável. A maneira usual de fazer isso é instalar o GRUB no registro mestre de inicialização de seu primeiro disco rígido. Se preferir, você pode instalar o GRUB em outro local de seu disco rígido, em outro disco ou até mesmo em um disquete.

Dispositivo no qual instalar o carregador de inicialização:

Informar manualmente o dispositivo
/dev/sda

<Voltar>

Instalação

[!!] Finalizar a instalação

Instalação completada

A instalação está completa, portanto é hora de inicializar em seu novo sistema.
Certifique-se de remover a mídia de instalação, para que seja possível inicializar em seu novo sistema ao invés de reiniciar a instalação.

<Voltar>

<Continuar>

GNU GRUB versão 2.02~beta3-5

*Debian GNU/Linux
 Opções avançadas para Debian GNU/Linux

Use the ↑ and ↓ keys to select which entry is highlighted.
Pressione 'Enter' para iniciar o SO selecionado, 'e' para editar
os comandos antes da inicialização or 'c' para linha de comando.

Instalação

```
Debian GNU/Linux 9 servidor tty1

servidor login:
```

```
Debian GNU/Linux 9 servidor tty1

servidor login: root
Password:
Linux servidor 4.9.0-7-amd64 #1 SMP Debian 4.9.110-1 (2018-07-05) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@servidor:~# _
```

Passos Iniciais

#

Root

$

Usuário

Terminais

F1 - F6

Comandos Básicos

Na teoria, não há diferença entre teoria e prática. Mas, na prática, há.

Jan L.A van de Snepscheut

Comandos Básicos

Os comandos GNU/Linux possuem algumas características particulares. Eles devem ser digitados em letras minúsculas, ou seja, são CASE-SENSITIVE.

No mundo *NIX(Linux,Unix), o conceito de comandos é diferente do padrão MS-DOS. Um comando é qualquer arquivo executável, podendo ou nãoser criado por você.

É no shell que os comandos são executados. Ele é o responsável pela interação entre o usuário e o sistema operacional, pois ele é que interpreta os comandos e os traduz para uma linguagem simples e inteligível para kernel.

Comandos Básicos

Tipos de Comandos:

#Internos - Que estão dentro do shell.

#externos - Que estão localizados em diretórios específicos.

Comandos Básicos

Iniciar e Terminar uma sessão:

login - cancela/inicia uma nova sessão
logout (ctrl+d) - termina a sessão
exit - Encerra o sehll de comandos corrente

Comandos Básicos

Reiniciar ou Desligar o computador:

#reboot
#halt

Comandos Básicos

Comandos de Ajuda

#man ls (página de manual)
#info ls (Informações do comandos)
#pinfo ls (Browser de informações de sistema)
#whatis ls (manuais online)
#apropos directory (informações a partir de uma palavra chave)

Comandos Básicos

Comandos de Navegação:

cd - muda o diretório

#cd /etc
#pwd
#cd /usr/bin
#cd ..
#cd /
#cd ou cd ~

Comandos Básicos

#pwd (Exibe o caminho do diretorio atual)
#tree (exibe a arvore de diretorios.)

ls ou dir (exibe o conteúdo dos diretórios)
ls
ls /usr/bin
#ls -r /usr/bin (ordem alfabetica reversa)
#ls -a (exibe arquivos ocultos)
#ls -l (listagem formato longo)
#ls -F (exibe arquivos diferenciando o tipo de arquivo)
#ls -d/*
#ls -d/*/*

Comandos Básicos

#ls -R (lista recursivamente dentro do diretório)

Comandos Básicos

Metacaracteres:

? - Corresponde à um único caractere;
* - Corresponde a todos os caracteres;
[ ] - Qualquer caracter dentro dos colchetes;
[a-z] - Corresponde a uma faixa de caracteres;

Comandos Básicos

Expressões regulares:

? - O item precedente é opcional e deve coincidir no máximo uma vez
* - O item precedente deverá coincidir zero ou mais vezes;
+ - O item precedente deverá coincidir uma ou mais vezes;
[ ] - Qualquer caracter dentro do colchete;
[a-z] - Faixa de caracteres;
^abc - padrão abc no inicio da linha
abc$ - padrão abc no final da linha
\<abc - padrão abc no inicio da linha
abc\> - padrão abc no final da linha

Comandos Básicos

Expressões regulares:
{n} - o item precedente deverá coincidir exatamente n vezes;
\{\n} - o item precedente deverá coincidir exatamente n vezes;
{n,} - o item precedente deverá coincidir n ou mais vezes;
\{n,\} - o item precedente deverá coincidir exatamente n vezes;
{,m} - o item precedente deverá coincidir no mínimo m vezes;
....

Comandos Básicos

Let's go:
#mkdir /exercicios (cria um diretorio)
#cd /exercicios
touch arquivo1 arquivo2 arquivo3 sessao1 sessao2 sessao3 sapo satisfacao
#ls
#ls arquivo?
#ls se*
#ls *1
#ls sessao[12]
#ls sessao[1-9]
#rm -ri *

Comandos Básicos

Comandos para localizar arquivos:
find
#cd /exercicios
#touch arquivo1.doc
#find / -name arquivo1.doc
#find /exercicios -name arquivo1.doc
#find /usr/bin -type f -atime +5 (arquivos não acessados a +5 horas)
#find /usr/bin -type f -mtime +5 (arquivos não modificados a +5 horas)
#find /xyz -type f -exec chmod 755 {} \;
#find /etc -type f -exec grep -i mouse {} \;

Comandos Básicos

grep, fgrep, egrep (procura em um ou mais arquivos por linhas que contém um padrão de busca)

#cd /exercicios
#grep -n root /etc/passwd
#cat > procura.txt
root
<enter>
<ctrl+d>
#ls
#grep -f procura.txt /etc/passwd

Comandos Básicos

#whereis ls (localiza arquivo, binário, código-fonte, man page)
#which ls (procura um comando que esteja na variável de ambiente PATH

Comandos Básicos

Manipulação de arquivos e diretórios:

#cd /exercicios
#touch arquivo1.doc (atualiza a data de acesso ao arquivo/cria um novo arquivo caso não exista)
#rm arquivo1.doc (apaga o arquivo)
#mkdir temp1 dir1 dir2 dir3 (cria diretórios)
#mkdir -p pai/filho (cria pai e dentro dele o diretorio filho
#tree
#rmdir temp1 (apaga o diretorio temp1)
#rmdir pai
#rm -rf pai

Comandos Básicos

MV - Move ou renomei arquivos
#cd /exercicios
#mkdir origem destino
#touch /exercicios/origem/arquivo1.doc
#tree
#mv /exercicios/origem/arquivo1.doc /exercicios/destino
#tree
#touch arquivo1.doc
#ls
mv arquivo1.doc arquivo2.doc

Comandos Básicos

CP - copia um ou mais arquivos

#cd /exercicios
#touch arq1.doc
#cp arq1.doc arq2.doc
#touch /exercicios/origem/doc1.doc
#tree
#cp -r /exercicios/origem /exercicios/destino

Comandos Básicos

ln - Cria link para arquivos ou diretórios

```
#cd /exercicios
#mkdir temp
#touch /exercicios/temp/arquivo1.doc
#tree
#ln /exercicios/temp/arquivo1.doc link1.doc
#tree
#ls -l
```

Comandos Básicos

#date MMDDHHmmAAAA (Exibe/Altera Data e hora do sistema)

#cal 09 2018 (Exibe o calendario)

#uname -a (informações do sistema operacional)

Comandos Básicos

Comandos de Paginação:

#cat /etc/passwd
#tac /etc/passwd
#more /etc/passwd
#less /etc/passwd

Comandos Básicos

Comandos de Filtragem

```
#head /etc/passwd
#head -5 /etc/passwd
#tail /etc/passwd
#tail -5 /etc/passwd
#wc -l /etc/passwd
#nl /etc/passwd
```

Comandos Básicos

#cd /exercicios
#cat > file1.txt
Eu
Linux
Nao
<enter><ctrl+d>
#cat > file2.txt
uso
porque
trava
<enter><ctrl+d>

Comandos Básicos

#nl file1.txt > file1.txt.nl
#nl file2.txt > file2.txt.nl
#join file1.txt.nl file2.txt.nl (junta os dois arquivos)

#ls /etc
#ls /etc | tr 'a-z' 'A-Z' (troca as letras minusculas por maiusculas)

Comandos Básicos

Sort - Ordena os dados de um arquivos
#cd /exercicios
#cat > usuarios.txt
Sandro
Guilherme
Allan
<enter><ctrl+d>

#sorte usuarios.txt

Comandos Básicos

cut - seleciona trechos de cada linha

#less /etc/passwd
#cut -f 1,5 -d: /etc/passwd (exibe as colunas 1 e 5 do arquivo passwd)

Comandos Básicos

Paste - Exibe lado a lado o conteúdo de arquivos
#cd /exercicios
#cat > f1.txt
guest
nobody
<enter><ctrl+d>
#cat > f2.txt
500
501
<enter><ctrl+d>
#paste -d, f1.txt f2.txt

Comandos Básicos

tee - Exibe a saida de um programa e a escreve em um arquivo simultaneamente

#ls -l /bin | tee ls.out

diff - Exibe em tela a diferenças entre dois arquivos texto
#diff -f f1.txt f2.txt

Comandos Básicos

Comandos de compactação:

#cd /exercicios
#mkdir documentos1
#cd documentos1
#touch a1.doc a2.doc a3.doc
#mkdir documentos2
#cd documentos2
#touch b1.doc b2.doc b3.doc

Comandos Básicos

#cd ../..
#tree documentos1

Avaliação

Ao final do dia de sábado mais especificamente as 15h30:
- Gerar informações sobre sua máquina virtual
- Gerar informações do histórico de comandos
- Gerar informações dos arquivos de configuração
- Enviar via FTP
- No FTP criar um diretorio com seu nome ex: allan_piter
- Subir os arquivos no diretorio criado.

FTP: 159.203.117.115
Usuário:aluno
Senha:uno@@2018

Comandos Básicos

Comando TAR
-c : cria um novo arquivo tar.
-j ou --bzip2 : compacta/descompacta os arquivos usando bzip2.
-J ou --xz : descompacta os arquivos .xz e .lzma.
-t : lista o conteúdo do arquivo tar.
-x : extrai o conteúdo do arquivo tar.
-v : mostra mensagens.
-f arquivo : define o nome do arquivo tar.
-z ou --gzip ou --gunzip : compacta/descompacta os arquivos usando gzip/gunzip.
-Z ou --compress ou --uncompress : compacta/descompacta os arquivos usando compress.

Comandos Básicos

#tar -cvf documentos.tar documentos1 (criar o arq documentos.tar)
#rm -ri documentos1 (apaga o dir documentos1)
#tar -tvf documentos.tar (exibe o conteúdo do arquivo)
#tar -xvf documentos.tar (extrai o arquivo)
#tar -cvzf textos.tar.gz documentos1 (gera arquivo compactado - gzip)
#rm -ri documentos1
#tar -tvzf textos.tar.gz
#tar -xvzf textos.tar.gz
#tar -cvjf textos.tar.gz documentos1 (gera arquivo compactado - bzip2)
#tar -ri documentos1
#tar -tvjf textos.tar.gz
#tar -xvjf textos.tar.gz

Trabalhando com o VI

Crie um arquivo:
#apt install vim
#vim /tmp/texto
Estou fazendo um teste no vi. O vi e um editor de texto muito poderoso.
Ideal para escrever programas. Apos a edicao, salve o arquivo.

Para entrar em modo edição pressione <i> ou <insert>.
Pressione <ESC> para sair do modo inserção.
Para salvar e sair do modo de inserção pressione :wq ou :x
Para sair sem salvar :q!

Trabalhando com o VI

- Abra o arquivo e pressione /vi , será mostrado a primeira ocorrência da palavra dentro do arquivo, para visualizar as ocorrências tecle <n>.

- pressione :%s/vi/vim/g (substitui vi por vim)

- yy (copia a linha atual), :5,10y (copia da linha 5 a linha 10)

- p (cola a linha copiada)

- dd ou 5,10d - Recorta ou Apaga uma linha

- u (desfaz a alteração)

Trabalhando com o VI

- <v> + <seta> - copia a letra, palavra ou frase
- :5 (vai para a quinta linha)
- :syntax on (deixa texto com cores)
- :set nu (numera as linhas)

Edite o arquivo vimrc
#vim /etc/vim/vimrc

Para aprender sozinho utilize o vimtutor
#vimtutor

Alias, Variáveis e Arquivos de Ambiente de Usuários

#alias ls ='ls --color=auto' (cria um apelido para um comando)
#unalias ls (remove o apelido)

Edite o arquivo bashrc (/etc/bash.bashrc) e no final (shift+g) insira:
alias cds='cd /etc/init.d; ls'
Salve e saia
#source /etc/bash.bashrc (recarrega o arquivo)

Edite o arquivo bashrc do usuário para listar apenas arquivos e outro para listar diretórios

Alias, Variáveis e Arquivos de Ambiente de Usuários

#vim /root/.bashrc
alias larq="ls -l | grep '^-' | more"
alias ldir="ls -l | grep '^d' | more"

Trabalhando com Variáveis
#LINUX=tux
#echo $LINUX
#set | grep LINUX (verifica se a variável aparece na relação do comando set)
#env | grep LINUX (verifica se a variável aparece na relação do comando env)

Alias, Variáveis e Arquivos de Ambiente de Usuários

#export LINUX (Exporta a variável para que ela possa ser válida em todos os shells)
#echo $PATH (exibe o conteúdo da variável PATH)

Questões de segurança

Por questões de segurança altere o conteúdo dos seguintes arquivos:

/etc/issue (Arquivo que exibe um banner antes do login)
/etc/motd (Arquivo que exibe um banner depois do login)
/etc/issue.net (Arquivo que é exibido após o usuário conectar remotamente a máquina)

Instalação de Programas(Pacotes)

Comandos para instalar programas (apt, aptitude, apt-get, dpkg)

#apt-get install aptitude (instala o programa dos repositórios do debian)
#apt-cache search mplayer (pesquisa nos repositorios se o pacote está disponível)
#apt-get update (atualiza a lista de pacotes disponíveis)
#apt-get clean (limpa o cache)
#apt-get upgrade (atualização de pacotes)
#apt-get remove --purge mplayer

/etc/apt/source.list (lista de repositórios)
/var/lib/apt/lists (relação dos pacotes que podem ser instalados)

Instalação de Pacotes

Existem outras formas de instalar pacotes que podem variar de distribuição para distribuição:

RPM, Yum, Yast, etc.

Gerenciamento de Processos

Visualizar os processos em execução:
#ps aux | more
Árvore de processos:
#pstree
#ps axf | more
Processos em tempo real
#top

Prioridade de Processos

Prioridade vão de -20 (Maior prioridade) a +19 (menor prioridade)

#nice -n 19 /etc/init.d/cron start (inicia o agendador de tarefas)
#ps lax | grep cron

Mudando a prioridade de um processo em execução
#pgrep cron
#renice -19 -p 377
#reinice -17 -p $(pgrep cron)

Matando processo

#killall -9 bash
#kill -9 $(lsof -t -u usuario)
#man 7 signal (visualizar os sinais disponível para processos)
#kill -15 384 ou kill -9 $(pgrep cron)
#pgrep cron

Usuários, Grupos e Permissões

#adduser usuario (adiciona um usuário)
#useradd -g users -m -s /bin/bash usuario2 (adiciona um usuário)
#passwd usuario2 (adiciona/altera a senha)
#logout

Logando com o usuario ou usuario2 verifique suas informações
$ id
$ w
$ who

Arquivos importantes (/etc/passwd e /etc/shadow)

Política de senhas

#chage -l usuario
#chage -m 3 usuario (permite mudar a senha daqui a 3 dias)
#chage -M 30 -W 10 usuario (senha valida por 30 dias, 10 dias antes avisa)
#chage -I 4 usuario (terá prazo de 4 dias para reativar a sua conta)
#adduser user1 (adiciona o usuário)
#passwd -l user1 (desabilita a conta do usuário)
#passwd -u user1 (habilita a conta do usuário)
#userdel -r user1 (remove a conta do usuário)

Grupos

#groupadd linux (adiciona um grupo linux no sistema)
#grep linux /etc/group (verifica se foi criada a entrada linux no arquivo)
#adduser torvalds
#gpasswd -a torvalds linux (adiciona o usuario ao grupo linux)
#grep linux /etc/group
#groupmod -n unix linux (muda o nome do grupo)
#groupdel unix (apaga o grupo)

Permissões

#mkdir /tmp/permissao
#cd /tmp/permissao
#touch arquivo
#ls -l arquivo

Permissões:
r - leitura(4) , w - escrita(2), x - execução(1)

#chmod u+x,g+w,o-r arquivo
#ls -l
#chmod a-rwx arquivo
#rm -f arquivo

Serviços Linux

Serviço SSH

#apt install ssh
#more /etc/ssh/sshd_config

Verificando se serviço subiu adequadamente
cat /etc/services | grep ssh
netstat -an | grep 22
fuser -v 22/tcp

Serviço SSH

Para utilizar o serviço:
ssh <hostname>
ssh <usuario>@<hostname>
ssh -l <usuario> <ip do servidor>

#ssh -l tux 10.10.10.10 -e du -hs /usr (executa um comando remoto)

Serviço NTP

#apt -y install ntp

Arquivo de configuração do NTP
/etc/ntp.conf

#systemctl restart ntp

Status
#ntpq -p

Servidor Web

Instalar Apache2 para Configure HTTP Server. HTTP usa 80/TCP.

#apt -y install apache2

vi /etc/apache2/conf-enabled/security.conf

linha 25: Alterar

ServerTokens Prod

vi /etc/apache2/mods-enabled/dir.conf

linha 2: adicione o nome dos arquivos principais que serão acessados por este diretorio

DirectoryIndex index.html index.htm

vi /etc/apache2/apache2.conf

linha 70: adicione o nome do servidor

ServerName www.servidor.com.br

vi /etc/apache2/sites-enabled/000-default.conf

linha 11: altere o email do webmaster email

ServerAdmin webmaster@servidor.com.br

systemctl restart apache2

PHP

```
# apt -y install php php-cgi libapache2-mod-php php-common php-pear php-mbstring

# a2enconf php7.0-cgi
Enabling conf php7.0-cgi.
To activate the new configuration, you need to run:
  service apache2 reload

# vi /etc/php/7.0/apache2/php.ini
# linha 924: descomente e adicione timezone
date.timezone = "America/Sao_Paulo"
# systemctl restart apache2
```

PHP

Crie uma página teste.php

vi /var/www/html/teste.php
<?php phpinfo(); ?>

Banco de Dados

Instalando o Serviço Mariadb
apt -y install mariadb-server

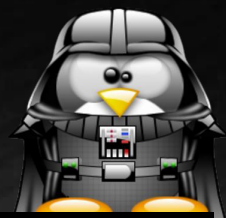
Aplicando segurança ao Banco de Dados
mysql_secure_installation

Testando
#mysql -u root -p
MariaDB [(none)]> select user,host,password from mysql.user;
MariaDB [(none)]> show databases;
MariaDB [(none)]> exit;

FTP

```
# apt -y install vsftpd
# vi /etc/vsftpd.conf
# linha 14: change it if listens Pv4
listen=YES
# linha 22: change it if not listen IPv6
listen_ipv6=NO
# linha1431: uncomment
write_enable=YES
# linha 99,100: uncomment ( allow ascii mode transfer )
ascii_upload_enable=YES
ascii_download_enable=YES
# linha 122: uncomment ( enable chroot )
chroot_local_user=YES
```

FTP



```
# linha 123: uncomment ( enable chroot list )
chroot_list_enable=YES
# linha 125: uncomment ( enable chroot list )
chroot_list_file=/etc/vsftpd.chroot_list
# linha 131: uncomment
ls_recurse_enable=YES
# add to the end : specify chroot directory
# if not specified, users' home directory equals FTP home directory
local_root=public_html
# turn off seccomp filter
seccomp_sandbox=NO
# vi /etc/vsftpd.chroot_list
# add users you allow to move over their home directory
debian
# systemctl restart vsftpd
```

SAMBA

Install SAMBA

```
# apt -y install samba
```

Configure o SAMBA

```
# mkdir /home/share
# chmod 777 /home/share
# vi /etc/samba/smb.conf
```

SAMBA

```
# line 25: add
unix charset = UTF-8
# 30行目：line 30: change if need (Windows' default)
workgroup = WORKGROUP
# line 48: uncomment and change IP address you
allow
interfaces = 127.0.0.0/8 10.0.0.0/24
# line 55: uncomment and add
bind interfaces only = yes
map to guest = Bad User
```

```
# add to the end
# any share name you like
[Share]
   # shared directory
   path = /home/share
   # writable
   writable = yes
   # guest OK
   guest ok = yes
   # all are processed as guests
   guest only = yes
   # fully accessed
   create mode = 0777
   # fully accessed
   directory mode = 0777

# systemctl restart smbd
```

NFS

Compartilhar diretorios linux

```
# apt -y install nfs-kernel-server
# vi /etc/idmapd.conf
# line 6: uncomment and change to your domain name
Domain = srv.world
# vi /etc/exports
# write settings for NFS exports
/home 10.0.0.0/24(rw,no_root_squash)
# systemctl restart nfs-server
#service portmap start
#showmount -e 10.0.0.1
#mkdir /nfs
#mount -t nfs 10.0.0.1:/home /nfs (Monta o volume)
#exportfs
```

DNS

Instalar o DNS
#apt -y install bind9 bind9utils dnsutils

Fazendo o primeiro teste:
#dig @localhost -t any wikipedia.com

Verificando quem esta respondendo
#nslookup www.wikipedia.com

DNS

Ajustando o ambiente:
1. Editar o arquivo /etc/resolv.conf
nameserver 127.0.0.1

Fazendo um teste:
#ping www.google.com

Verificando que está respondendo:
#nslookup www.google.com

DNS

Para que o servidor linux possa responder para a rede deve ser feitas as seguintes alterações:

```
#echo "1" > /proc/sys/net/ipv4/ip_forward
#iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

-Caso deseje que os clientes da rede passem a resolver nomes pelo novo DNS, basta apontar para o servidor linux.

DNS

Fazendo o ajuste do servidor

1 - Edite o /etc/resolv.conf
domain linuxserver.int
search linuxserver.int
nameserver 127.0.0.1

2 - Configure o arquivo para imutável
#chattr +i /etc/resolv.conf

DNS

Configurações de Segurança:
Edite o arquivo /etc/bind/named.conf.options (opções globais)

Realizar a seguinte alteração:

```
listen-on-v6 { none; };
listen-on-v4 { localhost; 172.16.21.128;  };
allow-transfer { none; };
allow-query { localhost; 172.16.21.0/24; };
allow-recursion { localhost; 172.16.21.0/24; };
version none;
```

DNS

Configurações de Zonas
Edite o arquivo /etc/bind/named.conf.local , e realizar as seguintes inclusões:

```
zone "linuxserver.int" {
        type master;
        file "/etc/bind/linuxserver.db";
};
```

Criar o arquivo linuxserver.db
vim /etc/bind/linuxserver.db

DNS

linuxserver.db

```
$TTL  3600
@     IN     SOA   linuxserver.int.       root.linuxserver.int. (
                   1                ; Serial (comentario)
                   604800           ; Refresh [1h]
                   86400            ; Retry [10m]
                   2419200          ; Expire [1d]
                   604800 )         ; Negative Cash TTL[1h]
```

DNS

Configurações gerais (continuação)

```
@       IN      NS      linuxserver.int.
@       IN      A       172.16.21.128
@       IN      A       192.10.0.1;
        IN      MX 5    linuxserver.int.

maquina1        IN      A       192.10.10.10
maquina2        IN      A       192.10.10.20
www     IN      CNAME           linuxserver.int.
```

Salvar e Sair

DNS

Reiniciar o serviço:

#/etc/init.d/bind9 restart

Verificando se o serviço subiu
#netstat -patun | grep :53

Verificando configurações:
#named-checkconf

Deu erro ou funcionou?

DNS

Ajustar a configuração do named.local.options

Alterar listen-on-v4 para listen-on , checar a configuração, restartar o serviço e testar novamente.

DNS

DNS Reverso (Consulta pelo IP)

1 - Editar o arquivo named.conf.local

#vim /etc/bind/named.conf.local

Adicionar ao fim do arquivo

```
zone "10.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/10.168.192.db";
};
```

DNS

DNS Reverso (Consulta pelo IP)

1 - Criar o arquivo 10.168.192.db
#vim /etc/bind/10.168.192.db

```
$TTL    3600
@       IN      SOA     linuxserver.int.  root.linuxserver.int. (
                        1                 ; Serial (comentario)
                        604800 ; Refresh [1h]
                        86400             ; Retry [10m]
                        2419200           ; Expire [1d]
                        604800 )          ; Negative Cash TTL[1h]
        IN      NS      linuxserver.int.
20      IN      PTR     cliente20.linuxserver.int.
```

HARDENING Linux

O que é hardening?

É a proteção do sistema por meio da redução de suas possíveis vulnerabilidades.

Devemos:

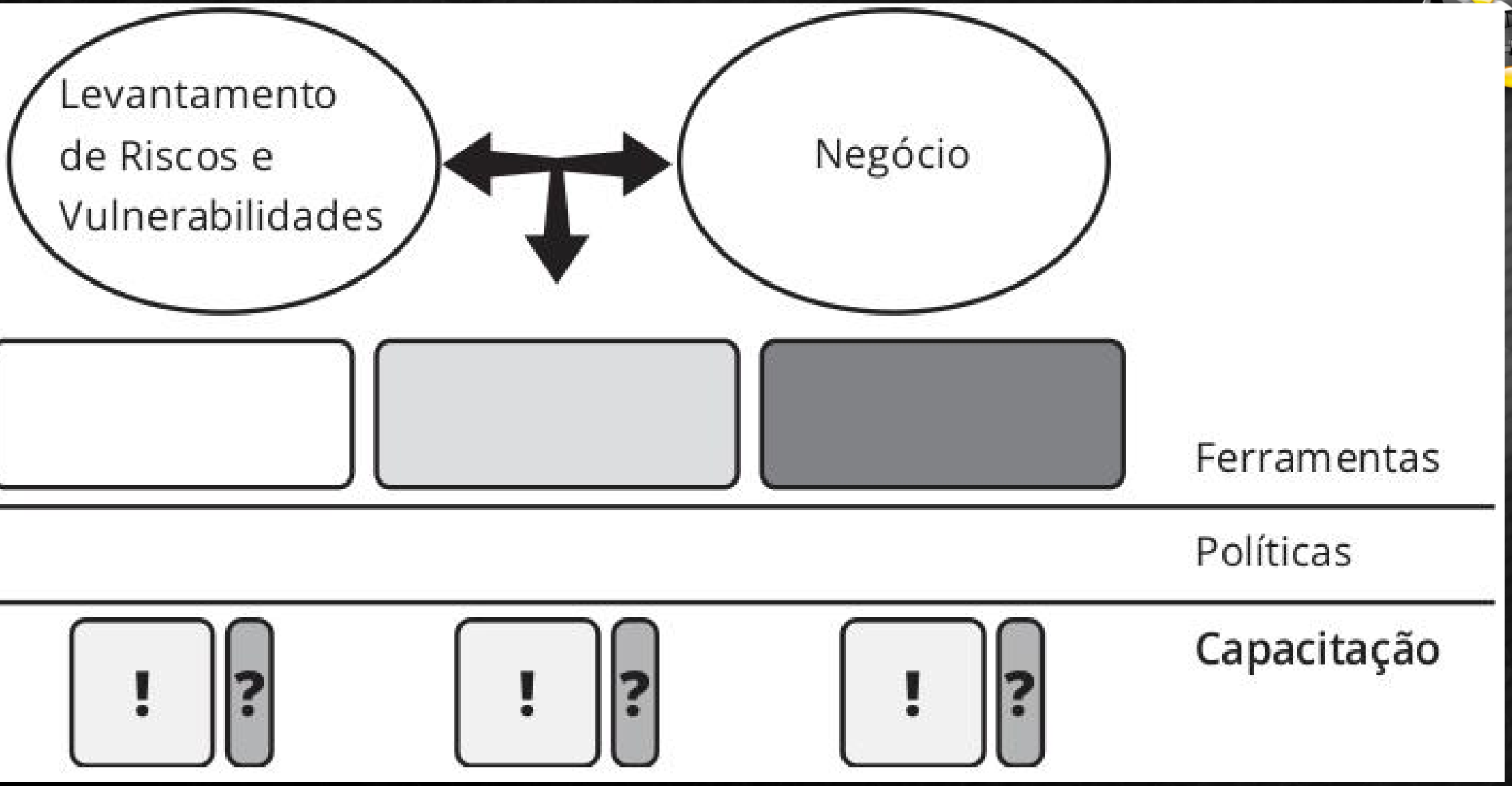
- Configurar o sistema.
- Instalar pacotes destinados a algum procedimento de segurança.
- Modificar o permissionamento para melhorar e reforçar a segurança.

Um ataque de fork bomb no Linux é facilmente efetuado executando a seguinte instrução em uma shell:

```
$:(){:|:&};:
```

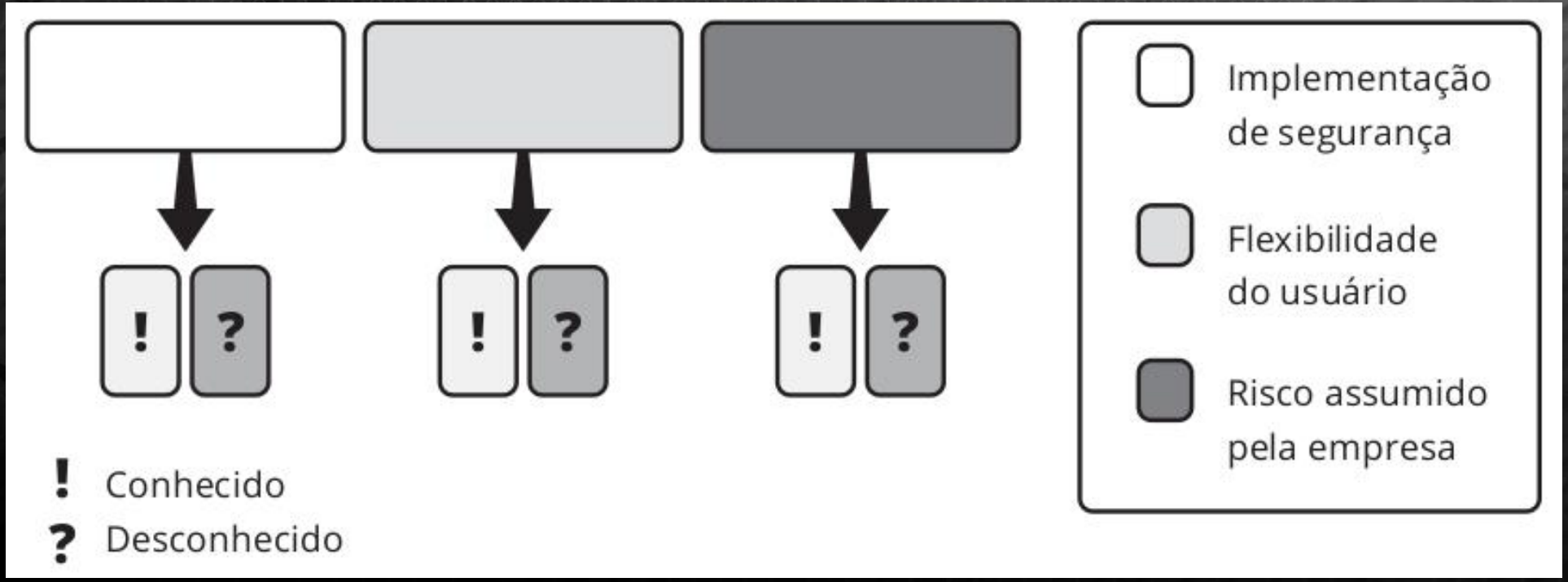
Esse é um exemplo de função que é executada de forma recursiva. É um meio conhecido e frequentemente usado por administradores de sistemas para testar as limitações dos processos de usuário, embora os limites de execução de processos de usuário em um sistema Linux possa ser configurado via /etc/security/limits.conf e PAM. É comum não ter nenhuma definição estabelecida em um sistema Linux. Dessa forma, um usuário comum pode causa uma Denial of Service (DoS) através de um fork bomb.

Se não existe segurança **100%** então o que existe?


Levantamento de Riscos e Vulnerabilidades
Negócio
Ferramentas
Políticas
Capacitação
!
?
!
?
!
?

Vulnerabilidade conhecida: servidor com um sistema legado que naquele momento não pode ser desligado, por exemplo;

Vulnerabilidade desconhecida: uma vulnerabilidade do Sistema Operacional que ainda não foi reportada pelo fabricante ou uma correção não publicada.



Baseline:

- A remoção ou desativação de serviços desnecessários;
- Remoção de contas de usuários-padrão;
- Desinstalação de pacotes desnecessários;
- Definição do processo de atualização;
- Definição de controles para auditoria;
- Definir controles para limites do uso dos recursos pelas aplicações e/ou usuários;
- Instalação de pacotes de ferramentas de segurança e auditoria.

Pós Instalação

Listando os pacotes instalados
```
# dpkg -l | awk ‘{print $2,$3}’ | sed ‘1,7d’
```

gravando o resultado em um arquivo
```
# dpkg -l | awk ‘{print $2,$3}’ | sed ‘1,7d’ > /root/pacotes
```

Lista de pacotes desnecessários:

lynx: cliente http/ftp que possibilita transferência de malware;
wget: cliente http/ftp que possibilita transferência de malware;
netcat (nc): “canivete suíço” que possibilita transferência de malware ou até mesmo criar backdoors;
hping: montador de pacotes que possibilita criar backdoors via rawsocket.

Muitos outros aplicativos podem entrar nessa lista, como: nmap, tcpdump, telnet (client), ftp (client) e shred, pois, devido aos recursos que proporcionam, devem ser devidamente avaliados.

Caso a remoção do pacote seja a melhor decisão, esta pode ser realizada da seguinte forma:

```
# apt-get remove --purge wget
```

Em distribuições Like Debian com Ubuntu, um aplicativo interessante é o apticron, que informa por e-mail pacotes que devem ser atualizados. O apticron é um shell script que usa as informações do apt-listchanges. Para instalar o apticron:

```
# apt-get install -y apticron
```

Durante a instalação é inserida uma entrada no /etc/cron.d, similar a esta:

```
# cat /etc/cron.d/apticron
15 * * * * root if test -x /usr/sbin/apticron; then /usr/sbin/
apticron --cron; else true; fi
```

As configurações do apticron ficam no /etc/apticron. Normalmente basta inserir o e-mail do administrador. Segue um exemplo de configuração:

```
# cat /etc/apticron/apticron.conf | grep -v ^#
EMAIL="allanpitter@gmail.com"
DIFF_ONLY="1"
LISTCHANGES_PROFILE="apticron"
NOTIFY_NEW="0"
CUSTOM_SUBJECT="Unochapeco Security: Aviso de atualização de
pacotes"
```

Atualizações de segurança via Debsecan: debsecan (Debsecan tool – Debian Security Analyzer) sobre registro de vulnerabilidade do CVE (www.mitre.org).

Essa ferramenta verifica a base de pacotes instalados, correlacionando com informações de vulnerabilidades publicadas.

Para instalar a ferramenta
#apt -y install debsecan

Uso:
debsecan --suite strech --only-fixed --format packages

Arquivos com permissão de Suid bit.

Suid bit
Permissão que só trabalha com arquivos executáveis serve para o propósito de um usuário comum poder executar um determinado binário com o poder do “dono” efetivo. Essa permissão é representada pela letra “s”.

Remoção de Suid bit

```
# cd /root
# mkdir listasec
# cd listasec
# find  / -perm -04000 > /root/listasec/lista.suid
# cat /root/listasec/lista.suid
# ls -l /bin/su
```

Como retirar todas as permissões de Suid bit dos binários:

```
# chmod -s -Rv /
```

Logo após remover as permissões:

ls -l /bin/su
Logo após remover o Suid bit de todo o sistema, basta definir a permissão de Suid bit somente para os dois binários que julgarmos realmente necessário.

chmod +s /usr/bin/passwd
chmod +s /bin/su
ls -l /usr/bin/passwd
ls -l /bin/passwd

Segurança no sistema de arquivos

Na instalação de um sistema Linux, as boas práticas nas instalações aconselham a particionar o disco e colocar os principais diretórios em partições separadas. Isso pode proporcionar maior segurança, pois cada partição tem sua tabela separada e pode ter regras de montagem melhor elaboradas.

As definições de montagem que devem ser avaliadas para esse contexto são:
Nodev: tira o suporte a arquivos de dispositivos;
Noexec: desabilita o suporte à execução dos arquivos;
Nosuid: deixa desabilitado o suporte ao direito especial de suidbit;
Noatime: desativa o registro de tempo/data de acesso dos arquivos (denominado atime);
Ro: define que será somente leitura.

Hands On

Adicione um usuário:
adduser novousuario

Faça uma cópia das shells do seu sistema para o diretório “home” desse usuário e atribua às shells a permissão de Suid bit.

mkdir /home/novousuario/teste
cp /bin/*sh* /home/novousuario/teste/.
chmod 4755 /home/novousuario/teste/*sh*

Efetue login em outro terminal com um usuário comum que foi criado anteriormente e tente executar uma dessas shells.
$ cd teste
$ ./sh
# id

Hand On

Para resolver isso, basta remontar a partição onde está montado o “/home”, mas com a opção de nosuid.

```
# mount -o remount,rw,nosuid /home
# mount
```

Refaça o teste.

Outra opção é com o parametro no exec instalado.

```
# mount -o remount,rw,noexec /home
# mount
```

Refaça o teste.

Questão

Quais os diretórios ou partições devem ser tratadas da mesma forma?

Segurança no sistema de arquivos

O comando stat, usado para verificar informações de metadados de sistema de arquivos de um arquivo:

```
# stat /etc/passwd
```

Hands on

```
# touch /root/teste1
# touch /tmp/teste2
# stat /root/teste1
# stat /tmp/teste2
# cat /root/teste1
# cat /tmp/teste2
# stat /root/teste1
# stat /tmp/teste2
```

Segurança no sistema de arquivos

Ponto de Montagem	nosuid	nodev	noexec	noatime
/boot	X	–	–	–
/	–	–	–	–
/home	X	X	X	–
/usr	X	X	–	–
/tmp	X	X	X	–
/var	X	X	X	–
/var/log	X	X	X	X
/var/spool/squid	X	X	X	X
/var/personal	X	X	X	X

Segurança no sistema de arquivos

```
# vi /etc/fstab


/dev/hda1      /boot           ext3    defaults,nosuid                 0 2
/dev/hda3      /               ext3    defaults                        0 1
/dev/hda4      /home           ext3    defaults,nosuid,noexec          0 2
/dev/hda5      /usr            ext3    defaults,nosuid                 0 2
/dev/hda6      /tmp            ext3    defaults,nosuid,noexec          0 2
/dev/hda7      /var            ext3    defaults,nosuid,noexec          0 2
/dev/hda8      /var/log        ext3    defaults,nosuid,noexec,noatime  0 2
/dev/hda9      /var/spool/squid ext3   defaults,nosuid,noexec,noatime  0 2
/dev/hda10     /var/personal   ext3    defaults,nosuid,noexec,noatime  0 2
/dev/hda2      none            swap    sw                              0 2
/dev/hdb       /media/cdrom0   iso9660 ro,user,noauto                  0 0
/dev/fd0       /media/floppy0  auto    rw,user,noauto                  0 0
```

Segurança no terminal

Em muitos momentos, um administrador pode inicialmente concentrar seus esforços para mitigar a possibilidade de ameaças remotas. Mas se o esforço for exclusivo para esse ponto de vista, deve-se assumir que o todo não é mitigado, pois servidores que não estão conectados diretamente à internet também estão correm riscos.

Desabilitar o uso de ‘CTRL+ALT+DEL’

#systemctl mask ctrl-alt-del.target
#systemctl daemon-reload

Segurança no Terminal

Limitar o número de terminais permitidos

Editar o arquivo /etc/systemd/ logind.conf
NAutoVTS = 3

Reinicie o servidor para verificar as alterações.

Bloquear o terminal com a variável TMOUT
TMOUT=15

Definido o valor 15, ela foi definida para fechar o terminal após 15 segundos de ociosidade.

Segurança no Terminal

Exemplificando o /etc/profile:
echo “export TMOUT=300” >> /etc/profile
Exemplificando o /root/.bashrc:
echo “export TMOUT=300” >> /root/.bashrc
Exemplificando o /etc/skel/.bashrc:
echo “export TMOUT=300” >> /etc/skel/.bashrc

Segurança no terminal

Bloquear o terminal com o programa Vlock

apt-get install vlock

vlock –a

Bloquear o login do root nos terminais texto
vi /etc/securetty
Comentar os terminais em que deseja bloquear o root
tty1
#tty2
...
#ttyXX

Segurança

Determinar datas de expiração para contas de usuários

chage -M 30 -W 5 -I 2 teste
chage -l teste
Onde:

-M: é o tempo máximo de validade da conta;
-W: é o tempo de aviso;
-I: é o tempo antes de a conta ser desativada.

Segurança

Remover shells válidas de usuários que não precisam delas.

cat /etc/passwd | less

Instalação de pacotes específicos

Embora um sysadmin deva ter em mente que prepara um servidor utilizando as boas práticas de segurança, com o objetivo de que este não seja vítima de algum tipo de incidente de segurança, ele também deve assumir que, se não existe segurança 100%, existe sempre um risco assumido ainda que não seja mensurável. Diante desse contexto, é recomendável que durante o processo de hardening seja feita a instalação de aplicações que poderão auxiliá-lo em execução de Auditorias futuras ou em uma Resposta a Incidente de Segurança.

Segurança

Instalação de pacotes específicos

apt-get install –y rkhunter chkrootkit unhide debsecan mtr-tiny apticron htop vim vlock whowatch lsof

Algumas ferramentas:
rkhunter: serve para fazer a identificação de rootkit e apoio à Resposta Incidente;
chkrootkit: identifica o rootkit e dá apoio à Resposta Incidente;
unhide: ferramenta para identificação de rootkit e apoio à Resposta Incidente;
lsof: útil para a gestão de processos;
htop: arrojada ferramenta para a gestão de processos;
lock: ferramenta de travamento de terminal texto;
debsecan: para o suporte à gestão de atualizações de segurança;
apticron: útil para o suporte à gestão de atualizações de segurança;
whowatch: ferramenta interessante para a gestão de uso de terminais;
vim: editor de texto.

Segurança

É recomendável também a atualização de todo o sistema, não somente dos pacotes que estão com notificação de vulnerabilidade, pois antes de instalar e configurar os serviços para os quais se destina o servidor, é o melhor momento para atualização completa do sistema.

apt-get install update && apt-get install –y upgrade

Segurança - Hands On - Exercicios

1 - Execute o chkrootkit e rkhunter, avalie os resultados e descreva as diferenças entre os dois.

2 - Avalie o baseline proposto (planilha xls) e apresente suas observações. Como deve ser configurado um baseline para a sua organização?

Procurar por Senhas Fracas

O John the Ripper é uma ferramenta de bruteforce clássica do mundo Unix, que tenta descobrir as senhas do arquivo /etc/shadow usando uma WordList (lista com senhas a serem tentadas) padrão que pode ser incrementada ou usada randomicamente.

#apt -y install john
cd /usr/share/john
cat password.lst

Serviços de Rede

Podemos ver algumas portas padrão do sistema no arquivo /etc/services. Exemplos de algumas portas:

```
 # cat /etc/services
 # cat /etc/services | grep -i ssh
```

Serviços que estão rodando

```
#netstat -ntlp
#fuser -v 22/tcp
#lsof -i
```

Portscanner

NMAP

#apt -y install nmap

nmap -sT –n –P0 10.0.0.1

nmap -sT –n –P0 localhost

nmap -sT –n –P0 -p 22 localhost

nmap -sU –n –P0 10.0.0.1

nmap -sU –n –P0 localhost

nmap -sU –n –P0 -p 53 localhost

nmap -sU –sT –n –P0 10.0.0.1

nmap -sU –sT –n –P0 -F 10.0.0.1

nmap -sU -sT –n –P0 -p- 10.0.0.1

nmap -sV –n –P0 10.0.0.1

Descobrindo mais sobre seu sistema

Fingerprint de serviço

AMAP -= Scanner de fingerprint de serviço desenvolvido pelo THC (www.thc.org).

amap -sT -d -b -o amap_report.txt 12.18.1.14

Httprint

Ferramenta útil na identificação ou levantamento de informações do servidor HTTP, como versão, tipo e recurso disponível – SSL e suporte a uma linguagem específica, como PHP.

Exemplo de uso:
httprint -s signatures.txt -o httprint_report.html -h 12.18.1.14

Segurança

O Nikto.pl é um scanner de vulnerabilidades web que pode ser usado na enumeração e identificação de possíveis vulnerabilidades.

```
# nikto.pl -list-plugins
# ./nikto.pl -update
# ./nikto.pl -host 12.18.1.14
# ./nikto.pl -host 12.18.1.14 -Format htm -output nikto_report.html
```

Segurança

As ferramentas que se destacam na realização desse tipo de teste são THC Hydra e Medusa.

```
# hydra -l root -P PASSFILE.txt -o LOG.txt 12.18.1.14 ssh
# medusa -u root -P PASSFILE.txt -h 12.18.1.14 -M ssh
```

Firewall

Funções

- proteger a máquina contra acessos indesejados
- proteger a máquina contra tráfego indesejado
- proteger serviços que estejam rodando na máquina
- bloquear a passagem de coisas indesejadas
- conexões vindas da Internet para sua segura rede local

Firewall - O que proteger?

- Quais serviços proteger?
- Que tipo de conexões eu posso deixar passar?
- Que máquinas terão acesso livre?
- Que serviços terão prioridade no processamento?
- Que máquinas/redes NUNCA deverão ter acesso?
- Qual o volume de tráfego que o servidor manipulará?
- O que pode passar de uma rede para outra?

Firewall

Tipos de Firewall

- Firewalls de aplicação
  - Proxies (SMTP, HTTP etc.)
- Firewalls baseados em estado
  - Tabelas de estados
- Firewalls de pacotes
  - Endereços e portas

Iptables

- surgiu no kernel do Linux 2.4
- substitui o ipchains
- muita flexibilidade na programação de regras
- mais opções para controle de tráfego
- controle independente do tráfego da rede
    - nova organização das etapas de roteamento de pacotes

Características

- Especificação de portas/endereço de origem/destino
- Suporte a protocolos TCP/UDP/ICMP
- Suporte a interfaces de origem/destino de pacotes
- Manipula serviços de proxy na rede
- Tratamento de tráfego dividido em chains
  - melhor controle do tráfego
- Permite um número ilimitado de regras por chain

Firewall

- Possui mecanismos internos para rejeitar pacotes
  - duvidosos ou mal formados
- Suporte a módulos externos
  - expansão das funcionalidades oferecidas
- Suporte completo a roteamento de pacotes
- Suporte a especificação de tipo de serviço
  - priorizar o tráfego de determinados tipos de pacotes
- Permite especificar exceções

Firewall - Regras

O que são regras?

Comandos passados ao iptables para que ele realize uma determinada ação

As regras são armazenadas dentro dos chains e processadas na ordem que são inseridas

As regras são armazenadas no kernel

- são perdidas a cada reinicialização
- devem ser gravadas em um arquivo

Firewall

O que são chains?

Locais onde as regras do firewall são armazenadas para sua operação:

- Existem dois tipos de chains
  - os embutidos (como os INPUT, OUTPUT e FORWARD)
  - os criados pelo usuário
- Os nomes dos chains
  - embutidos devem ser especificados sempre em maiúsculas
  - são case-sensitive (input é diferente de INPUT)

Firewall

O que são tabelas?

Locais usados para armazenar chains e regras com determinada característica em comum

Podem ser referenciadas com a opção -t <tabela>

- Existem 3 tabelas disponíveis no iptables
  - filter
  - nat
  - mangle

Firewall

A tabela filter

- Esta é a tabela padrão, contém 3 chains padrões
  - INPUT: dados que chegam a máquina
  - OUTPUT: dados que saem da máquina
  - FORWARD: dados que são redirecionados
- INPUT e OUTPUT
  - somente são atravessados por conexões de localhost

Firewall

A tabela nat

- Usada para dados que geram outra conexão
- Possui 3 chains padrões:
  - PREROUTING: quando os pacotes precisam ser modificados logo que chegam
  - OUTPUT: quando os pacotes gerados localmente precisam ser modificados antes de serem roteados
  - POSTROUTING: quando os pacotes precisam ser modificados após o tratamento de roteamento

Firewall

A tabela mangle

- Utilizada para alterações especiais de pacotes
- Possui 5 chains padrões:

– INPUT: quando os pacotes precisam ser modificados antes de serem enviados para o INPUT da tabela filter

– FORWARD: quando os pacotes precisam ser modificados antes de serem enviados para o FORWARD da tabela filter

– PREROUTING: quando os pacotes precisam ser modificados antes de ser enviados para o PREROUTING da tabela nat

Firewall

A tabela mangle

- Utilizada para alterações especiais de pacotes
- Possui 5 chains padrões:

– POSTROUTING: quando os pacotes precisam ser modificados antes de serem enviados para o POSTROUTING da tabela nat

– OUTPUT: quando os pacotes precisam ser modificados antes de serem enviados para o OUTPUT da tabela nat

Firewall

MANIPULANDO CHAINS
Adicionando regras - A
ping 127.0.0.1
iptables -t filter -A INPUT -d 127.0.0.1 -j DROP
ping 127.0.0.1

Firewall

Listando regras - L

- iptables -t filter -L INPUT
- iptables -L INPUT –n
- iptables -L INPUT -n --line-numbers

Firewall

Apagando uma regra - D

- iptables -t filter -D INPUT 1
- iptables -t filter -D INPUT -d 127.0.0.1 -j DROP

Inserindo uma regra - I

- iptables -t filter -I INPUT 1 -d 127.0.0.1 -j ACCEPT

Firewall

Criando um novo chain - N

- iptables -t filter -N internet
- iptables -t filter -A internet -s 200.200.200.200 -j DROP
- iptables -t filter -A INPUT -j internet

Limpando as regras de um chain - F

- iptables -t filter -F INPUT
- iptables -t filter -F

Apagando um chain do usuário - X

- iptables -t filter -X internet
- iptables -X

Firewall

Especificando a política de um chain - P

- iptables -L OUTPUT
- iptables -t filter -P OUTPUT DROP
- iptables -L OUTPUT

Firewall

Especificando um endereço

- Origem e destino
  - -s | –src | –source
  - -d | –dst | –destination
- Opções
  - IP ou par rede/máscara: 10.0.0.1 ou 10.0.0.0/8
  - endereço fqdn: www.aptans.com
- iptables -A INPUT -s 10.0.0.0/24 -j DROP

Firewall

Especificando um protocolo

- Protocolo
  - -p | –protocol
- Opções
  - tcp
  - udp
  - icmp
- iptables -A INPUT -s 10.0.0.0 -p UDP -j DROP

Firewall

Especificando portas

- Origem e destino
  - --sport | --source-port
  - --dport | --destination-port
- iptables -A OUTPUT -d 10.0.0.1 -p tcp --dport :1023 -j DROP

Firewall

Especificando uma exceção

- iptables -t filter -A INPUT –p TCP ! -s 10.0.0.1 -j DROP
- iptables -A INPUT -s 10.0.0.1 ! -p TCP -j DROP

Firewall

Especificando um alvo

- Opções

-j ACCEPT
-j DROP
-j REJECT
-j LOG

- iptables -A INPUT -s 10.0.0.1 -i eth0 -j REJECT

Firewall

Redirecionamento de portas

- Proxies e programas externos
  – -j REDIRECT
- iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 \
-j REDIRECT --to-port 8080

Port Knocking - Manto da Invisibilidade

Atua ouvindo conexões em determinadas portas previamente determinadas e executa comandos quando as sequências de conexões são enviadas corretamente.
Assim, podemos deixar nossas portas fechadas e abrir quando é conveniente e depois fechá-las novamente. Isso ajuda bastante a segurança em nosso servidor, pois se um possível atacante scanear nosso servidor, ele verá que está tudo fechado (nesta dica, iremos abordar somente a configuração do SSH, mas para os demais serviços, a lógica é a mesma).
Isto dificultará bastante o trabalho dele, para utilizar o knockd, precisamos instalá-lo em nosso servidor e no cliente.

Port Knocking

Execute o seguinte comando, para instalar o knockd no servidor e no cliente:

```
# aptitude install knockd
# more /etc/knockd.conf
# Edit o arquivo /etc/default/knockd
```

- Altere a opção "START_KNOCKD=0" para "=1" e,
- Altere a opção KNOCKD_OPTS="-I eth0"

Depois disso, podemos iniciar nosso port knocking:

```
# /etc/init.d/knockd start
```

Port Knocking

Com nosso servidor já configurado. é hora de testar. Em nosso cliente, iremos executar os seguintes comandos:

```
# knock 192.168.0.55 7000:tcp 8000:tcp 9000:tcp
```

Feito isso execute iptables -nL no servidor, e veja se a regra foi criada. Agora é só conectar-se normalmente ao SSH:

```
# ssh user@ip_maquina
```

Quando encerramos nossa conexão com o SSH, não podemos esquecer de fechar a porta do SSH no servidor, para isso execute o comando abaixo:

```
# knock 192.168.0.55 9000:tcp 8000:tcp 7000:tcp
```

40 dicas

1: criptografar a comunicação de dados

Todos os dados transmitidos através de uma rede estão abertos para monitoramento.

Criptografe dados transmitidos sempre que possível com senha ou usando chaves/certicados.

40 dicas

2: Evitar o uso de serviços FTP, Telnet e Rlogin / Rsh
Na maioria das con gurações de rede, os nomes de usuários, senhas, comandos FTP / telnet /rsh e arquivos transferidos podem ser capturados por qualquer pessoa na mesma rede usando um sniffer de pacotes. A solução comum para esse problema é usar o OpenSSH , o SFTP ou o FTPS (FTP sobre SSL), que adiciona criptogra a SSL ou TLS ao FTP.

40 dicas

3: Minimize o software para minimizar a vulnerabilidade
Você realmente precisa de todos os tipos de serviços da Web instalados? Evite instalar software desnecessário para evitar vulnerabilidades no software.

40 dicas

4: um serviço de rede por sistema ou instância de VM
Execute serviços de rede diferentes em servidores separados ou instância de VM . Isso limita o número de outros serviços que podem ser comprometidos. Por exemplo, se um invasor conseguir explorar com êxito um software como o Apache, ele terá acesso a todo o servidor, incluindo outros serviços, como MySQL / MariaDB / PGSql, servidor de e-mail e assim por diante.

40 dicas

5: Mantenha o kernel e o software do Linux atualizados
A aplicação de patches de segurança é uma parte importante da manutenção do servidor Linux. O Linux fornece todas as ferramentas necessárias para manter seu sistema atualizado e também permite atualizações fáceis entre as versões. Toda atualização de segurança deve ser revisada e aplicada o mais rápido possível.

40 dicas

6: use as extensões de segurança do Linux
O Linux vem com vários patches de segurança que podem ser usados para proteger contra programas mal con gurados ou comprometidos. Se possível, use o SELinux e outras extensões de segurança do Linux para impor limitações na rede e em outros programas. Por exemplo, o SELinux fornece uma variedade de políticas de segurança para o kernel do Linux.

40 dicas

7: SELinux

Eu recomendo fortemente o uso do SELinux, que fornece um Controle de Acesso Mandatório (MAC) exível. No Controle de Acesso Discricionário do Linux (DAC) padrão, um aplicativo ou processo executado como usuário (UID ou SUID) tem ermissões do usuário para objetos, como arquivos, soquetes e outros processos. A execução de um kernel MAC protege o sistema contra aplicativos maliciosos ou defeituosos que podem dani car ou destruir o sistema. Veja a documentação o cial do Redhat , que explica a con guração do SELinux.

40 dicas

8: contas de usuário e diretiva de senha forte
Use os comandos useradd / usermod para criar e manter contas de usuário. Veri que se você tem uma política de senha boa e forte. Por exemplo, uma boa senha inclui pelo menos oito caracteres e uma mistura de alfabetos, números, caracteres especiais, alfabetos superiores e inferiores, etc. O mais importante é escolher uma senha que você possa lembrar. Use ferramentas como " John the ripper " para descobrir senhas de usuários fracos no seu servidor.

40 dicas

9: envelhecimento da senha
O comando chage altera o número de dias entre alterações de senha e a data da última alteração de senha. Essa informação é usada pelo sistema para determinar quando um usuário deve alterar sua senha. O arquivo /etc/login.defs de ne a con guração especí ca do site para o conjunto de senhas de sombra, incluindo a con guração de envelhecimento da senha. Para desativar a duração da senha, digite:
chage -M 99999 userName

40 dicas

10: Restringindo o uso de senhas anteriores

Você pode impedir que todos os usuários usem ou reutilizem as mesmas senhas antigas no Linux. O parâmetro do módulo pam_unix remember pode ser usado para con gurar o número de senhas anteriores que não podem ser reutilizadas.

40 dicas

11: bloqueando contas de usuário após falhas de login
No Linux, você pode usar o comando faillog para exibir registros faillog ou para de nir limites de falha de login. O faillog formata o conteúdo do log de falhas do /var/log/faillog database/
log le. Ele também pode ser usado para manter contadores e limites de falhas. Para ver tentativas de login com falha, insira: faillog Para desbloquear uma conta após falhas de login, execute:
faillog -r -u userName

40 dicas

12: Como posso veri car se as contas não têm senhas vazias?
Digite o seguinte comando
awk -F: '($2 == "") {print}' /etc/shadow
Bloquear todas as contas de senha vazias:
passwd -l accountName

40 dicas

13: Certi que-se de que nenhuma conta não raiz tenha o UID de nido como 0
Apenas a conta root tem o UID 0 com permissões completas para acessar o sistema. Digite o
seguinte comando para exibir todas as contas com o UID de nido como 0:
awk -F: '($3 == "0") {print}' /etc/passwd

40 dicas

14: Desativar login root

Nunca mais faça o login como usuário root. Você deve usar o sudo para executar comandos no nível da raiz conforme e quando necessário. O sudo aumenta muito a segurança do sistema sem compartilhar a senha do root com outros usuários e administradores. O sudo também oferece recursos simples de auditoria e rastreamento .

40 dicas

15: Segurança do servidor físico

Você deve proteger o acesso ao console físico dos servidores Linux. Con gure o BIOS e desative a inicialização de dispositivos externos, como DVDs / CDs / pen USB. De na a senha do BIOS e do boot loader para proteger essas con gurações. Todas as caixas de produção devem ser bloqueadas em IDCs (Internet Data Center) e todas as pessoas devem passar por algum tipo de veri cação de segurança antes de acessar seu servidor.

40 dicas

16: Desativar serviços indesejados
Desative todos os serviços e daemons desnecessários (serviços executados em segundo plano).
Você precisa remover todos os serviços indesejados da inicialização do sistema. Digite o seguinte comando para listar todos os serviços iniciados no momento da inicialização no nível de execução # 3:
chkconfig --list | grep '3:on'
Para desabilitar o serviço, digite:
service serviceName stop
chkconfig serviceName off

40 dicas

#17: encontrar portas de rede de escuta
Use o seguinte comando para listar todas as portas abertas e programas associados:
netstat -tulpn
OU use o comando ss da seguinte forma :
$ ss -tulpn
nmap -sT -O localhost
nmap -sT -O server.example.com

40 dicas

18: Excluir X Windows

X Windows no servidor não é necessário. Não há razão para executar o X Windows em seu correio dedicado e servidor web Apache. Você pode desativar e remover o X Windows para melhorar a segurança e o desempenho do servidor.

40 dicas

19: Con gurar Iptables e TCPWrappers

Iptables é um programa aplicativo de espaço do usuário que permite configurar o firewall (Net Iter) fornecido pelo kernel do Linux. Use o firewall para filtrar o tráfego e permitir apenas o tráfego necessário. Use também o TCPWrappers, um sistema ACL de rede baseado em host para filtrar o acesso à Internet. Você pode evitar muitos ataques de negação de serviço com a ajuda de Iptables.

40 dicas

20: Kernel do Linux /etc/sysctl.conf Endurecimento
O arquivo /etc/sysctl.conf é usado para con gurar os parâmetros do kernel no tempo de
execução. O Linux lê e aplica as con gurações do /etc/sysctl.conf no momento da inicialização.
Exemplo de arquivo /etc/sysctl.conf :

40 dicas

```
# Ativar execshield
kernel.exec-shield = 1
kernel.randomize_va_space = 1
# Ativar proteção contra falsificação de IP
net.ipv4.conf.all.rp_filter = 1
# Desativar roteamento de origem de IP
net.ipv4.conf.all.accept_source_route = 0
# Ignorando a solicitação de difusões
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_messages = 1
# Certifique-se de que os pacotes falsificados sejam registrados
net.ipv4.conf.all.log_martians = 1
```

40 dicas

21: partições de disco separadas

A separação dos arquivos do sistema operacional dos arquivos do usuário pode resultar em um sistema melhor e seguro. Certifi que-se de que os seguintes sistemas de arquivos estejam montados em partições separadas

40 dicas

22: cotas de disco

Verifique se a cota de disco está ativada para todos os usuários.

40 dicas

23: Desativar o IPv6
O IPv6 (Internet Protocol version 6) fornece uma nova camada de Internet do conjunto de
protocolos TCP / IP que substitui o IPv4 (Internet Protocol version 4) e oferece muitos
benefícios. Se você NÃO estiver usando o IPv6, desative-o

40 dicas

24: Desabilitar SUID indesejados e binários SGID

Todos os arquivos habilitados para SUID / SGID podem ser usados incorretamente quando o executável SUID / SGID tiver um problema de segurança ou bug. Todo usuário local ou remoto pode usar tal arquivo.

40 dicas

25. Utilize ferramentas diversas de auditoria.

40 dicas

26: Arquivos No owner

Arquivos não pertencentes a qualquer usuário ou grupo podem representar um problema de segurança. Basta encontrá-los com o seguinte comando que não pertence a um usuário válido
e a um grupo válido.

```
find /dir -xdev \( -nouser -o -nogroup \) -print
```

40 dicas

27: Use um serviço de autenticação centralizada.

Sem um sistema de autenticação centralizado, os dados de autenticação do usuário se tornam inconsistentes, o que pode levar a credenciais desatualizadas e contas esquecidas que deveriam ter sido excluídas em primeiro lugar. Um serviço de autenticação centralizado permite manter o controle central sobre dados de autenticação e conta do Linux / UNIX. Você pode manter os dados de autenticação sincronizados entre os servidores. Não use o serviço NIS para autenticação centralizada. Use o OpenLDAP para clientes e servidores.

40 dicas

28: Kerberos

O Kerberos executa a autenticação como um serviço de autenticação confiável de terceiros, usando o segredo criptográ co compartilhado sob a suposição de que os pacotes viajando ao longo da rede insegura podem ser lidos, modificados e inseridos. O Kerberos baseia-se na criptogra a de chave simétrica e requer um centro de distribuição de chaves.

40 dicas

29: registro e auditoria

Você precisa con gurar o log e a auditoria para coletar todas as tentativas de hackers e crackers. Por padrão, o syslog armazena dados no diretório / var / log /. Isso também é útil para descobrir uma con guração incorreta do software, o que pode abrir seu sistema para vários ataques.

40 dicas

30: Monitore mensagens de log suspeitas com o Logwatch / Logcheck Leia seus logs usando o comando logwatch (logcheck). Essas ferramentas facilitam sua vida de leitura de registros.

40 dicas

31: Contabilidade do sistema com auditd

O auditd é fornecido para auditoria do sistema. É responsável por gravar registros de auditoria no disco.

40 dicas

32: Secure OpenSSH Server

O protocolo SSH é recomendado para login remoto e transferência remota de arquivos. No entanto, o ssh está aberto para muitos ataques.

40 dicas

33: Instale e use o sistema de detecção de intrusões

Um sistema de detecção de invasão de rede (NIDS) é um sistema de detecção de intrusão que tenta detectar atividades maliciosas, como ataques de negação de serviço, varreduras de portas ou até tentativas de invadir computadores, monitorando o tráfego da rede.

40 dicas

1: criptografar a comunicação de dados

Todos os dados transmitidos através de uma rede estão abertos para monitoramento.

Criptografe dados transmitidos sempre que possível com senha ou usando chaves/certicados.

40 dicas

34: Desativar dispositivos USB/firewire / thunderbolt
35: Desativar serviços não utilizados
36: Use fail2ban / denyhost como IDS
37: servidor seguro Apache / PHP / Nginx
38: Protegendo Arquivos, Diretórios e E-mail
39. Backups
40. Outra recomendação: SBNC Avançado.

MUITO OBRIGADO.