lpi202

207{ Peso 8 - DNS
207.1{ Peso 3 - Configuração básica do servidor DNS - 26/04
Bind - principal servidor DNS no mundo
named - nome do daemon que controla do Bind
/etc/bind/named.conf - principal arquivo de configuração
directory - onde ficam os arquivos das zonas
version none - não mostra a versão do bind nas consultas
cache-only - não cuida de zonas
tipos de zonas - há vários tipos de zonas
hint - zona para dns forward
root.hints - contém os endereços dos servidores dns raiz
dig @a.root-servers.net
/usr/sbin/rndc - aplica as configurações do dns
rndc reload - faz o reload do dns
rndc flush - limpa o cache do dns
rndc reconfig - aplica as mudanças no named.conf
Bundy - nome antigo do Bind
Dnsmasq - Servidor DNS mais simples
dnsmasq.conf - arquivo de configuração
Djbdns - servidor dns com suporte a criptografia
é necessário ter o Daemontools
/etc/djbdns - pasta de configuração do Djbdns
tynedns.conf - principal arquivo de configuração
server - pasta com os arquivos de zona
PowerDNS - servidor DNS complexo e com muitos recursos
pdns e pdns-backend-mysql - pacotes do centos
/etc/pdns/pdns.conf - arquivo de configuração
pdns-server - pdns-backend-mysql - pacotes do debian
/etc/powerdns/pdns.conf - arquivo de configuração
}
207.2{ Peso 3 - Criando e mantendo zonas DNS - 29/04
named.conf - principal arquivo de configuração do Bind
version none - não mostra a versão o bind nas requisições
listen-on - IPs em que o Bind ficará ouvindo
blackhole - IPs que não podem usar o Bind
zone "empresa.com" IN { - início da configuração da zona empresa.com
type master; - este servidor é o responsável pelo domínio
allow-transfer - IPs dos servidores slave
type slave; - este servidor é o backup do master
master - IP do servidor master
tcp:53 - porta usada pela transferência entre servidores
type forward - tranfere as requisições desde domínio para outro servidor
forwarders - servidores que responderão por esse domínio
file "empresa.com.db"; - arquivo que contém a zona, caminho relativo ao "directory"

}; - fim da configuração da zona
directory - diretório onde ficarão os arquivos da zona
empresa.com.db - arquivo de zona
$TTL 3D - Tempo em que o registro ficará em cache nos servidores DNS
@ IN SOA empresa.com. hostmaster.empresa.com. - início da autoridade e e-mail do administrador (hostmaster)
serial - número que precisa ser alterado a cada atualização no dns
refresh - intervalo de atualização do slave
retry - intervalo para novas tentativas de comunicação com os slave
expire - prazo de validade do registro
minimum - tempo mínimo que um registro deve ficar em cache
H/D/W - valores em horas, dias e semanas
tipos de registros
ns - servidores de nome do domínio
mx - servidor responsável por receber e-mails para o domínio
quanto menor o número, maior a prioridade.
a - endereço ipv4
aaaa - endereço ipv6
cname - alias
ptr - dns reverso
reverso - traduz de ip para nome
zone "0.168.192.in-addr.arpa" - forma correta para criar a zona reversa para a rede 192.168.0.0/24
registros ptr precisam terminar com ".".
host - cliente de dns
host site servidor - consulta pelo endereço "site" no servidor dns "servidor".
host -a - traz todos os registros
dig - cliente de dns
dig @servidor endereço tipo consulta o "tipo" de registro do endereço "endereço" usando o servidor "servidor".
axfr - testa a transferência de zona
~/.digrc - personalização para o usuário
nslookup - outro cliente de dns
permite os modos interativo e não-interativo.
nslookup - servidor - entra no modo interativo usando servidor como dns
nslookup site servidor - procura pelo nome "site" no servidor dns "servidor"
/etc/resolv.conf - arquivo de configuração do cliente dns
named-checkzone - checa se a zona está configurada corretamente
named-checkzone zona arquivo_de_conf - formato do comndo
named_checkconf - checa a configuração do bind
-z - checa todas as zonas master
named-compilezone - converte uma zona para um formato humano
masterfile-format text - armazena zonas backup em arquivos texto (padrão binário)
map - imagem binária
text - texto
raw - outro formato binário}

207.3{ Peso 2 - Segurança em servidores DNS - 01/05
Envenenamento de dns - permite fazer um site malicioso se passar por um legítimo
named - processo do Bind
-u - especifica o usuário
-t - especifica o diretório que servirá de jaula
DNSSEC - cuida da criptografia das comunicações entre os servidores dns
dnssec-keygen - gera as chaves usadas na criptografia
-a - tipo de chave (ex. DSA)
-b - tamanho da chave (ex. 768)
-r - gerador da chave (ex. /dev/uramdom)
-n - tipo do dono da (ex. ZONE)
dnssec-keygen -a RSA -b 768 -r /dev/uramdom -n ZONE suaempresa.com.br
Knome.+aaa+iiii.key - Knome-da-chave.+número_do_algoritmo+id.key - formato do nome da chave pública gerada
Ksuaempresa.com.br.+003+47654.key - exemplo de nome do arquivo de chave pública gerada
Knome.+aaa+iiii.private - Knome-da-chave.+número_do_algoritmo+id.private - formato do nome da chave privada gerada
Ksuaempresa.com.br.+003+47654.private - exemplo de nome do arquivo da chave privada gerada
hmac-md5 - criptografia usada na chave
$include arquivo.key - configuração no arquivo de configuração da zona
dnssec-signzone - assinatura da zona
-o - nome da zona
-r - gerador da chave
named.conf - pricipal arquivo de configuração do bind
file - apontar para o arquivo de zona signed
trusted-keys { - início da zona segura
"suaempresa.com." 256 3 3 "FRGTG..." - entrada dos dados da chave
} - fim da zona segura
allow-query - diz quais IPs e redes podem usar esse dns
allow-transfer - diz quem pode solicitar transferênia de zona (slaves)
forwarders - diz quais são os servidores que fazem recursividade
porta tcp 53 - porta usada para comunicação entre o master e o slave}}
208{ Peso 11 - Servidores Web
208.1{ Peso 4 - Implementando um servidor web - 04/05
Apache 1 - vários processos filho
Apache 2 - multi processor
/etc/apache, /etc/apache2, /etc/httpd - pastas de configuração padrão do Apache
httpd.conf, apache.conf, apache2.conf - principal arquivo de configuração
ServerType - como o servidor vai rodar
standalone - independente
inetd - debaixo do inetd, xinetd ou openbsd-inetd
ServerRoot - define o diretório de configuração do Apache
PidFile - local do arquivo de pid (padrão /var/run/httpd.pid)
ServerAdmin - e-mail do administrador do sistema

DocumentRoot - pasta dos arquivos do site (geralmente /var/www ou /var/www/htdoc)

ServerName - endereço do site

LoadModule nome caminho - carrega o módulo dinâmico "nome" que se encontra em "caminho"

AddModule modulo.c - carrega o módulo estático "modulo.c"

Port - porta usada pelo servidor, geralmente 80

User - usuário dono do processo servidor

Group - grupo do processo servidor

AddHandler - determina como o Apache tratará os arquivos baseado em sua exensão

Todas essas opções podem estar no arquivo principal ou nos arquivos dos sites

Opções de desempenho - ditam como o Apache deve trabalhar

Timeout - tempo aguardando por dados em uma conexão

KeepAlive - permite que mais de uma requisição seja feita usando a mesma conexão

MaxKeepAliveRequest - número máximo de requisições por conexão; 0 para desabilitar

KeepAliveTimeout - tempo limite entre a última requisição e o fechamento da conexão

MinSpareServers - número mínimo de processos servidores inativos

MaxSpareServers - número máximo de processos servidores inativos

MinSpareThreads - número mínimo de threads

MaxSpareThreads - número máximo de threads

StartServers - número inicial de processos, além do servidor

MaxClients - número máximo de processos. Na prática, número máximo de clientes

MaxRequestsPerChild - Número máximo de requisições que um processo pode receber; 0 para infinito

mods.available - módulos disponíveis

mods.enabled - módulos ativados (link simbólico)

sites.available - sites disponíveis

sites.enabled - sites ativados (links simbólico)

apachectl, apache2ctl - controla o processo apache

graceful - espera as conexões terminarem

configtest - checa os arquivos de configuração

<Directory /caminho > - início da seção que configura o acesso à pasta caminho

Options FollowSymLinks - obedece os links simbólicos

AllowOverride None - não permite (None) o uso do arquivo .htaccess na pasta

AllowOverride All - permite o uso do arquivo .htaccess

UserDir - permite ao usuário oferecer arquivos do seu drive home

</Directory> - fim da configuração de acesso à pasta

.htaccess - arquivo que contém as permissões de acesso

AccessFileName - muda o nome do arquivo .htaccess

mod_auth, mod_auth_basic, mod_authz_host, mod_access_compat - fornecem suporte a autenticação web via .htaccess

htpasswd - cria o arquivo das contas de acesso à pasta

-s - uso de sha1
-c - endereço do arquivo
htpasswd -s -c /etc/apache2/htpasswd ricardo - cria o usuário ricardo no arquivo htpasswd usando hash sha1
AuthType Basic - autenticação
AuthName "Teste" - mensagem exibida para o usuário
AuthUserFile "/etc/apache/htpasswd" - arquvo de senha
AuthGroupFile - permissão por grupo
Require valid-user - requer usuário autenticado
ErrorLog - localização dos arquivos de log
| - podemos mandar a log para um programa usando pipe
syslog:user - usa o syslog, facilite user (padrão local7), para armazenar as logs
LogFormat "formatos" nome - cria o tipo de log "nome" que tem o formato "formatos". Os formatos podem ser:
%h - host remoto
%l - log remoto, se houver
%u - usuário remoto, se disponível
%t - data e hora
%r - primeira linha da requisição
%s - status da requisição
%b - bytes enviados, menos cabeçalhos
%D - tempo gasto pela requisição
%{User-agent}i - tipo de navegador do cliente
access.log - arquivo de log de acessos
CustomLog - cria uma log personalizada
CustomLog /var/log/apache/access.log nome - cria a log access.log com o formato "nome" pré definido pelo LogFormat
<VirtualHost *> - define um host virtual
NameVirtualHost * - Em quais endreços e portas esse virtual host vai trabalhar
ServerName www.empresa.com - site
DocumentRoot - pasta raiz do site
ServerAlias - apelido para o site
</VirtualHost> - fim da configuração do site virtual
libapache-mod-perl - módulo que dá suporte ao perl
libapache2-mod-php - módulo que dá suporte ao php
RedirectMatch 404 regex - mostra mensagem de "página não encontrada" quando a solicitação casar com regex
Códigos de erro - relação dos códigos de retorno do Apache
200 - página ok
404 - página não encontrada
405 - método não permitido
100 - continuação
302 - redirecionamento
500 - erro interno}
208.2{ Peso 3 - Configurando o Apache para HTTPS - 07/05
mod_ssl - modulo ssl para apache1.x

openssl - gera uma chave privada para o https
genrsa - gera chave rsa
-des3 - criptografia 3des
-out - arquivo gerado
1024 - tamanho da chave
openssl genrsa -des3 -out www.empresa.com.br.key 1024 - exemplo de uso
openssl - gera um arquivo de pedido de assinatura
req - gera um csr - Certificate Signing Request
-new - nova requisição
-key - caminho do arquivo de chave
-out - nome do arquivo de requisição gerado
openssl req -new -key www.empresa.com.br.key --out www.empresa.com.br.csr - exemplo de uso
o arquivo csr deverá ser enviado para a CA autenticar
openssl - cria um certificado auto assinado
x509 - tipo de certificado
-req - nova requisição
-in www.empresa.com.br.csr - arquivo .csr criado acima
-days 365 - número de dias de validade do certificado
-signkey www.empresa.com.br.key - arquivo da chave privada
-out www.empresa.com.br.crt - arquivo .crt gerado
/etc/ssl ou /etc/pki - local padrão dos certificados
Listem 443 - porta do https
SSLEngine on ou SSLEnable - ativa o suporte a criptografia
SSLCertificateKeyFile - local da chave privada (arquivo .key)
SSLCertificateFile - local do certificado gerado pelo CA (arquivo .crt)
SSLCertificatePrivateKey - local da chave privada ssl
SSLCipherSuite - define os protocolos de criptografia
SNI - Server Name Identification - habilita o ssl por nome do site para um mesmo ip}
208.3{ Peso 2 - Implementando um servidor proxy - 10/05
cache e filtro web - funções do proxy
squid.conf - principal arquivo de configuração do proxy
O Squid não roda com usuário root
acl - Access Control List - são os objetos (personagens) do squid
nome - nome da acl
tipo - tipo da acl
src - ip de origem
dst - ip de destivo
url_regex - expressão regular encontrada na url
dstdomain - site
time - data e hora
SMTWHFA hh:mm-hh:mm
arp - mac address do cliente
port - porta usada pelo site
proto - protocolo, como http, ftp, etc.
valor - valor da acl

acl lan src 192.168.0.0/24 - cria a acl chamada "lan" do tipo "ip de origem" com o valor "192.168.0.0/24"
http_port - porta usada pelo squid (padrão 3128)
cache_mgr - e-mail do administrator
cache_effective_user - usuário do squid
cache_effective_group - grupo do squid
http_access - define a permissão
allow - permite
deny - bloqueia
lan - qual acl (personagem se aplica)
http_access allow lan - libera o acesso para a rede local
auth_param - habilita a autenticação do usuário
schema - tipo de autenticação
basic - lê um arquvo de usuários e senha
digest - lê um arquivo de usuários:senha
ntlm - autentica num servidor Windows
programa - programa usado para autenticar
basic_fake_auth - só checa o usuário logado, não checa a senha
children 5 - máximo de 5 processos de autenticação
realm "Login" - texto exibido na tela de login
credentialsttl 2 hours - a credecial vale por duas horas
Exemplo de uso
auth_param basic program /usr/lib/squid/basic_fake_auth
auth_param basic children 5
auth_param basic realm "Teste do olonca"
auth_param basic credentialsttl 2 hours
acl autenticados proxy_auth REQUIRED
http_access allow autenticados}
208.4{ Peso 2 - Implementando um Nginx como um servidor web e proxy reverso - 13/05
/etc/nginx - pasta de configurações
nginx.conf - principal arquivo de configuração
user - usuário dono do nginx
worker_processes - número de processos rodando
pid - local do arquivo de pid
sites-enabled - arquivos de configuração dos sites virtuais
default - site padrão
root - local dos arquivos do site
index - página inicial
server_name - nome do site
nginx
-s - administração do serviço nginx
reload - recarrega as configurações
stop - para o serviço
quit - para o serviço sem desconectar as conexões ativas
-t - testa as configurações

location ~ \.php$ { - inicia uma configuração de proxy reverso encaminhando todos os sites .php

proxy_set_headers - altera um ítem do cabeçalho da requisição

X-Real-IP $remote_addr;

X-Forward-For $remote_addr;

Host $host;

proxy_pass http://site; - para onde encaminhar a requisição}}}

209{ Peso 8 - Compartilhamento de arquivos

209.1{ Peso 5 - Configuração do servidor SAMBA - 16/05

smbd - daemon que cuida do compartilhamento de arquivos e impressoras

nmbd - daemon que cuida dos nomes netbios

/etc/samba - pasta de configuração

smb.conf - principal arquivo de configuração

[global] - configurações que afetam todo o samba

server string = "Texto" - descrição do servidor vista pela rede

null passwords - permite usuários com senha nula

username map - caminho do mapeamento de usuários

root = admin administrador - mapeamento dos usuários locais admin e administrador para o usuário do Linux root

workgroup - nome do grupo netbios

logon script - script que será executado quando o usuário fizer logon

domain logons - ativa o login remoto

netbios name - nome netbios do servidor

preferred master - determina se esse servidor vai buscar ser o master da rede

os level - prioridade na eleição do master; maior número, maior prioridade

logon path - onde se localizam os arquivos de perfil do usuário

logon drive - letra a ser mapeada no desktop do usuário

logon home - diretório home do usuário

wins support - ativa ou não o suporte ao Wins

log file - localização dos arquivos de log

log file = $S.log - log por compartilhamento

log level - nível de detalhes da log do samba

security - define como será a autentição

user - Usuários locais

ad - usuários de um Active Directory

lmhosts - mapeamentos de ip/nomes_netbios

username map - arquivo que contém o mapeamento de usuário do Windows para o Linux

[netlogon] - compartilhamento padrão usado na rede Windows

path - localização da pasta netlogon

%N - nome do servidor

%U - nome do usuário

[homes] - compartilhamento das pastas dos usuários

coments = "Texto"

read only = se é somente leitura (yes/no)

browseable = se é visto pela rede (yes/no)

[printers] - compartilhamento de impressoras
path - caminho do spool
printable - se a impressora está aceitando trabalhos
public - se precisa ou não de autenticação
testparm - verifica os arquivos de configuração do samba
smbpasswd - cria contas de usuário no samba
-a - cria a conta
-x - exclui uma conta
-d - bloqueia um conta
-e - desbloqueia uma conta
-n - senha nula
-m - conta de máquina
a conta de máquina deve existir no Linux com o nome final $
nmblookup - testa o servidor wins
-B - endereço de broadcast
-W - domínio
nbtscan - traz o nome netbios da máquina passando como parâmetro o seu ip
smbstatus - status sobre os mapeamento e sua utilização
-p - lista os processos ativos
-S - lista os compartilhamentos em uso
-u - mostra apenas os compartilhamentos usados pelo usuário especificado
smbcontrol - envia comandos para os daemons do samba
all - envia para todos os daemons
reload-config - faz o reload sem desconectar os usuário
smbclient - cliente do samba
-R - especifica a ordem de resolução de nomes
smbclient -L \\servidor -U usuário - lista os compartilhamentos no servidor utilizando o login usuário
mount -t cifs - monta um ompartilhamento Windows (-t smbfs - mais antigo)
-o username=usuário,password=senha - passando usuário e senha para montar o compartilhamento
mount.cifs - comando novo para montar compartilhamentos
smbmount - comando usado nas versões antigas
fstab - para montar o mapeamento Windows no boot
credentials=arquivo - arquivo que contém a senha e somente o root tem acesso
username = usuário - define o usuário que vai montar o compartilhamento
password = senha - define a senha do usuário que vai montar o compartilhamento
/var/log/samba - pasta com os logs
/etc/krb5.conf - arquivo de configuração do kerberos
[libdefaults] - configurações globais
default_realm = FPANET.INET - domínio padrão
[realms] - configuração dos domínios
FPANET.INET = { - início da configuração do domínio FPANET.INET
kdc = 172.20.1.1 - endereço do ad
default_domain = FPANET.INET - domínio padrão
} - fim da configuração do domínio

[domain_realm] - alias de domínio
.fpanet.inet = FPANET.INET - alias do domínio fpanet.inet
net ads join -U administrator - comando para adicionar o Linux como membro do domínio
Klist - mostra os tiquetes do kerberos
winbindd - cuida da autenticação no domínio
pbedit - manipula todos os bancos de usuários do Samba
wbinfo - traz informações do domínio
-u - usuários
-g - grupos
net - ferramenta de administração do samba
ads - gerenciamento de domínios
info - mostra informações sobre o domínio
join - coloca a estação no domínio
leave - remove uma máquina do domínio
dns - administração do dns dinâmico
register - registra no dns
unegister - tira do dns
password - muda a senha do usuário
printer - administra as impressoras
workgroup - lista os grupos da rede
gpo - administra as gpo do domínio
% - separa o usuário de sua senha
groupmap list - mostra o mapeamento de grupos do Windows para Linux
domain - lista os domínios da rede
service - lista os serviços ativos
time - mostra data e hora
status - informações sobre a sessão atual
sessions - lista os arquivos abertos
shares - lista os compartilhamentos
dbcheck - verifica a localização do banco de dados do Active Directory}
209.2{ Peso 3 - Configuração do servidor NFS - 19/05
portmapper - necessário ao nfs
rpc.nfsd - dispara eventos do nfs
rpc.mountd - cuida das solicitações de montagem
rpc.rquotad - controla as cotas, se houver
rpc.lockd - controla as travas para o nfs
rpc.statd - notificação de reinício do nfs
/etc/exports - arquivo de configuração dos compartilhamentos
/diretório ip1(permissão) ip2(permissão) - compartilha o "diretório" para os ips com suas respectivas permissões
ro - somente leitura
rw - leitura e escrita
no_root_squash - permite montagem como root
exportfs -a - ativa as mudanças feitas no arquivo /etc/exports
exportfs -ua - desativa os compartilhamentos
exportfs -o - compartilha pela linha de comandos

mount -t nfs seridor:/pasta /ponto_de_montagem - monta o compartilhamento "pasta" do "servidor" no "ponto_de_montagem"
showmount -e servidor - mostra os compartilhamentos disponíveis em "servidor"
nfsstat - gera estatísticas no nfs
-m - mostra informações no cliente
-3 - somente dados do nfs versão 3
/proc/net/rpc/nfsd,nfs - arquivos consultados pelo nfsstat
rpcinfo - mostra informações sobre o serviço rpc
-p - mostra as portas mapeadas
-m - mostra dados estatísticos}}
210{ Peso 11 - Administração dos clientes de rede
210.1{ Peso 2 - Configuração do DHCP - 22/05
atributo passado ao cliente - cada atributo em um valor
1 - máscara de rede
2 - time offset
3 - roteador padrão
4 - servidor ntp
discovery - pacote enviado pelo cliente para descobrir os servidores dhcp
offer - resposta do servidor para o cliente que enviou o discovery
request - solicitação de endereço enviado pelo cliente ao servidor
ack - resposta possitiva do servidor para um cliente que enviou um request
nack - resposta negativa do servidor para um cliente que enviou um request
dhcpd - principal servidor dhcp do Linux
porta 67 e 68 udp - portas usadas pelo dhcp server e client respectivamente
porta 647 - porta usada pelo failover
/etc/dhcpd.conf - arquivo de configuração
default-lease-time - tempo mínimo para renovação
max-lease-time - tempo máximo para utilização do ip
option - opções que podem ser passadas para os clientes
domain-name - nome do domínio que o cliente faz parte
domain-name-servers - ip dos servidores dns separados por ","
domain-search - domínios para pesquisa, separados por "," (cada domínio deve estar entre "")
ddns-update-style - atualização automática de dns
router - gateway padrão
subnet 192.168.0.0 netmask 255.255.255.0 { - início da configuração da vlan 192.168.0.0/24
range 192.168.0.100 192.168.0.200 - ip inicial e final do range disponível
netmask - máscara de rede
option - configurações opcionais que afetam essa vlan
routers 192.168.0.1 - configura a rota padrão dos clientes para 192.168.0.1
} - fim da configuração da subnet
host cliente1 { - início da configuração personalizada do "cliente1"
hardware ethernet 00:01:02:03:04:05 - especifica o mac address afetado por essa regra
fixed-address 192.168.0.201 - especifica o endereço ip para o cliente

filename - nome do arquivo de kernel a ser enviado para o cliente via bootp
server-name - endereço do servidor tftp para bootp
} - fim da configuração do "cliente1"
dhcpd.leases - arquivo com os endereços já disponibilizados
bootp - Bootstrap - boot via rede
/var/lib/dhcp/dhcpd.lease - banco de dados do dhcpd
dhcpd -lf /var/lib/dhcp/dhcpd.lease eth0 - sobe o dhcp na eth0 lendo o arquivo de lease especificado
dhcrelay - necessário para fornecer dhcp para outras vlans de forma centralizada
dhcrelay -i eth0 servidor - sobe o dhcrelay na interface eth0 e encaminha as requisições para o servidor dhcp especificado
/var/log/daemon.log - log das requisições do dhcp
dhcpcd, dhclient e pump - cliente de dhcp
radvd - faz anúncios de router advertisement (ra) para a rede ipv6
o encaminhamento ipv6 precisa estar habilitado
radvd.conf - arquivo de configuração
AdvSendAdvert on - habilita as respostas ra
prefix 2001:db8::/64 - prefixo da rede ipv6
AdvAutonomous on - os clientes podem gerar um endereço ipv6 automaticmaente usando o prefixo fornecido
clients - quais clientes estão autorizados a usar o radvd}
210.2{ Peso 3 - Autenticação PAM - 25/05
pam - Pluggable Authentication Modules
/etc/pam.conf - principal arquivo de configuração
/etc/pam.d - pasta com os arquivos personalizados para cada serviço ou programa
tipo controle módulo argumento - estrutura dos arquivos
tipo - grupo de serviços
account - checa se o usuário tem permissão para acessar, se a senha expirou, etc
auth - checa a autenticidade do usuário usando senha ou outro dispositivo
password - usado para a troca do mecanismo de autenticação, como a senha
session - procedimentos de pré e pós autenticação, loga as autenticações
controle - procedimentos adotados dependendo da resposta do módulo
requisite - ítem deve ser satisfeito no login
required - só pode ser usado para autenticação mas, em caso de negativa, outros requisitos podem ser tentados
sufficiente - basta essa autenticação para a autenticação ser aceita
optional - só tem efeito se for o único ítem satisfeito
módulo - qual módulo deve ser usado
/lib/security ou /usr/lib/security - local dos módulos
pam_securetty.so - login local
pam_nologin.so - desabilita o login de todos os usuários se o arquivo /etc/nologin existir
pam_limits.so - aplica as configurações de /etc/security/limits.conf
pam_lastlog.so - mostra informações sobre o último login do usuário
pam_ldap.so - autenticação via ldap
pam_motd.so - mostra a mensagem do motd quando o usuário se autentica

pam_sss.so - suporte ao serviço sssd (System Security Services Daemon)
pam_cracklib.so - define a conplexidade mínima da senha
pam_listfile.so - permite ou bloqueia o acesso a serviços baseados na existência ou não de certos arquivos
pam_unix.so - módulo para autenticação usando o arquivo /etc/passwd
pam_userdb.so - módulo para autenticação usando uma base de dados
pam_access.so - módulo que provê acesso anônimo ao ftp
argumentos - dependem do módulo

nsswitch.conf - diz qual é a ordem de autenticação, consultas dns e lista de usuários e grupos
passwd: compat winbindd - consulta por usuários primeiro no arquivo passwd e depois no domínio
group: compat winbindd - consulta por grupos primeiro no arquivo passwd e depois no domínio
hosts: files dns - consulta por nomes de hosts primeiro no arquivo resolv.conf e depois no dns}

210.3{ Peso 2 - Usando o cliente de LDAP - 28/05

ldapscripts - pacote que contém os comandos para incluir, consultar, alterar e excluir dados do servidor ldap

ldapsearch - faz pesquisas do servidor ldap
-x - autenticação simples
-b - base dn
-s - escopo da pesquisa
-LLL - formata (-L) a saída sem comentário (-L) e sem informações sobre a versão (-L)
(objectClass=*) - filtro padrão)

ldif - Ldap Data Interchange Format - formato do arquivos de inserção do ldap
dn - distinguished name
o - organization name
c - country
cn - common name
sn - surname
add - adiciona um novo registro

ldapadd - adiciona ítens na base ldap
-f - arquivo ldif
-W - pede a senha
-D - binddn

ldapmodify - modifica um objeto na base de dados ldap

ldapdelete - delete ítens da base ldap

ldapaddgroup - adiciona grupos de usuários no ldap

ldapdeletegroup - apaga um grupo

ldapadduser - adiciona usuários ao ldap

ldapdeleteuser - apaga um usuário

ldapaddusertogroup - adiciona um usuário a um grupo

ldapdeleteuserfromgroup - remove um usuário de um grupo

ldappasswd - altera a senha de um objeto do ldap

ldapaddmachine - cria uma conta de máquina}
210.4{ Peso 4 - Configurando um servidor OpenLDAP - 31/05
/etc/ldap - pasta dos arquivos de configuração
slapd.conf - principal arquivo de configuração
object class - define os atributos que podem ser associados ao objeto
rootdn - usuário administrador do ldap
rootpw - senha do administrador do ldap
*.schema - arquivos de esquema de objetos do ldap
slappasswd - criptografa a senha
/var/lib/ldap - local da base de dados ldap
slaptest - testa o servidor ldap
slapindex - corrige o banco de dados
slapcat - faz um dump do banco ldap
slapadd - adiciona objetos no banco
-j - especifica de qual linha começar a importação
-f - localização do arquivo de configuração
-q - quit mode
-l - arquivo de imput
slapd_db_recover - corrige inconsistência no bano de dados ldap
loglevel - tipo de log
0 - sem debug
1 - chamadas de função
8 - gerenciamento de conexões
16 - log de pacote enviados e recebidos
64 - log do processamento dos arquivos de configuração
slurpd - responsável pelo replicação
636 - porta usada pelo ldap ssl}}
211{ Peso 8 - E-mail
211.1{ Peso 4 - Usando um servidor de e-mail - 05/06
MTA - Mail Transfer Agent
Sendmail - MTA mais antigo
/etc/mail - pasta padrão de configuração
access - permissões de envio e recebimento de e-mail
OK - aceita para entrega local
RELAY - Aceita o e-mail para encaminhamento
REJECT - Rejeita o envio
DISCARD - Ignora a mensagem
makemap hash /etc/mail/access.db < /etc/mail/access - cria o arquivo binário usado pelo Sendmail
local-host-names - nomes para a máquina local
virtusertable - redirecionamentos (necessário rodar o comando makemap)
genericstable - endereço de saída (makemap)
genericsdomain - domínios locais
mailertable - redirecionamentos de e-mails vindos de fora
domaintable - mapeamentos de domínios
aliases - alias de e-mails

destinatário: email1@domain, email2@domain
sendmail.cf - principal arquivo de configuração
m4 - utilitário para alterar o sendmail.cf
smtpd_sasl_auth_enable = yes - habilita a autenticação
smtpd_sasl_type = dovecot - mecanismo de autenticação
smtpd_sasl_path = private/auth - caminho dos arquivos de autenticação
smtpd_tls_security_level=encrypt - habilita a senha criptografada
Postfix - MTA mais usado
/etc/postfix - principal pasta de configuração
main.cf - principal arquivo de configuração
myorigin - nome do dominio dos e-mails originados no servidor
mydestination - domínios hospedados localmente
mynetworks - de quais redes o servidor encaminha mensagens (clientes internos)
mynetworks_style - outra forma de utilizar o mynetworks
relay_domains - quais domínios serão reencaminhados
relayhost - endereço do servidor rsponsável por envios para a internet
mailbox_size_limit - quota das caixas postais
mailq_path - pasta das filas de e-mail
mailbox_command - encaminha as mensagens entrantes para um programa externo
master.cf - configuração de comandos e como devem ser executados
virtual - semelhante ao mydestination

master/bounce/cleanup/error/flush/load/pickup/pipe/postdrop/qmgr/sendmail/showq/smtp/smtpd - processos
postsuper - gerencia o Postfix
-d - remove um e-mail da fila
ALL - remove todos os e-mail
Exim - MTA padrão do Debian
/etc/exim - pasta de configurações
exim.conf - principal arquivo de configuração
Qmail - só distribuído em código fonte
/var/qmail/control - pasta de configuração do Qmail
/var/spool/mail, /var/spool/mailq e /var/mail - local de armazenamento das mensagens
/var/log/mail? - arquivos de log
newaliases - converte o arquivo de alias em um arquivo binário
postconf -d - mostra todos os parâmetros relacionados à configuração do Postfix
tipos de caixas postais
mailbox - tudo dentro de um único arquivo, como o pst
maildir - cada mensagem é um arquivo
postqueue -p - mostra as mensagens pendentes da fila
postscreen_tls_security_level - habilita o tls
postcat - lista uma mensagem na fila
qshape - mostra menagens na fila com seus tempos
MDA - Mail Delivery Agent}
211.2{ Peso 2 - Gerenciamento da entrega de e-mail - 08/06

Procmail - principal MDA do Linux
/etc/procmailrc - principal arquivo de configuração
~/.procmailrc - arquivo de configuração do usuário
:0 - início da regra
:0: - início da regra com lock
:0 c - copia a mensagem para a próxima ação
condição expressão_regular - condição a ser testada
ação - ação a ser tomada caso a condição seja verdadeira
urgente - nome de uma pasta para onde enviar a mensagem
! destino@domínio - encaminha a mensagem para o e-mail especificado
| comando - usa a mensagem como stdin de comando
/usr/bin/procmail - programa que processa as mensagens
Sieve - linguagem de programação para filtrar e-mail
:contain - semelhante ao grep
keep - ação padrão
redirect - encaminha mensagem para outro destinatário
redirect:copy - copia uma mensagem para outro destinatário
size :over 500K - mensagens maiores do que 500K
size :under 1k - mensagens menores do que 1K
elsif - elif
fileinto "foldername" - salva mensagem na pasta "foldername"
comandos - ação, controle e teste
discard - descarta a mensagem
:days - número de mensagens diárias que o remetente receberá de avisos de férias}
211.3{ Peso 2 - Gerenciamento da entrega remota de e-mail - 11/06
IMAP, POP3 - principais protocolos de entrega de e-mail ao usuário
Courier - servidor de IMAP e POP3
/etc/courier - pasta de configuração
imapd - arquivo de configuração do protocolo IMAP
ADDRESS - ip em que o IMAP vai ouvir
PORT - porta, geralmente 143
IMAP_CHECK_ALL_FOLDERS - checa todas as pastas, não só a INBOX
IMAP_ENHANCEDIDLE - avisa quando novas mensagens chegam
MAXDAEMONS - Número máximo de clientes
pop3d - arquivo de configuração do protocolo POP3
POP3DSTART - inicia o suporte ao POP3
Dovecot - outro servicor de IMAP e POP3
/etc ou /etc/dovecot - pasta de configuração
dovecot.conf - principal arquivo de configuração
mail_location - localização das mensagens
mbox_read_locks e mbox_write_locks - parâmetros que habilitam o lock
mail_privileged_group = mail - cria pontos de bloqueio para lock no /var/mail
mbox_very_dirty_syncs = yes - melhora a performance
protocols - quais protocolos o Dovecot vai utilizar
mechanisms - quais métodos de autenticação serão aceitos (pode usar o PAM para autenticação)

doveconf - mostra os parâmetros de configuração do dovecot
doveadm - comando de administração do Dovecot
-D - debug
expunge - remove mensagens que casam com uma dada consulta
reload - faz o reload do Dovecot
stop - pára o Dovecot
kick - desconecta os usuários por ip ou nome
who - mostra quem está logado no Dovecot
auth - testa a autenticação do usuário}}
212{ Peso 14 - Segurança
212.1{ Peso 3 - Configurando um roteador - 14/06
sysctl -w net.ipv4.ip_forward=1 - habilita do rotamento
Endereços públicos - usados na internet
Endereços privados - usados em redes locais
10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 - relação dos ips privados
169.254.0.0/16 - APIPA
fe80::/16 - endereço link local ipv6
route - administra a tabela de roteamento
-n - não resolve nomes
add -net ip netmask máscara dev interface - adiciona uma rota manual
del - remove um rota
iptables - manipula o módulo de firewall netfilter
-t - tabela (padrão é filter)
filter - tabela de firewall
INPUT - pacotes destinados ao firewall
OUTPUT- pacotes originados pelo firewall
FORWARD - pacotes que atravessam o firewall
nat - tabela para alterações em IPs e portas
PREROUTING - antes do pacote ser roteado
-j DNAT - nat de destino
--to-destination, --to - ip de destino a ser atribuído ao pacote
REDIRECT - direcionar o pacote para outra porta no mesmo host
--to-port - nova porta de destino
POSTROUTING - depois do pacote ser roteado
-j SNAT - nat da origem
--to-source, --to - ip de origem a ser atribuído ao pacote
-j MASQUERADE - faz o nat automático dos pacotes da rede privada para a rede pública
mangle - para marcações nos pacotes
-A - adiciona uma regra no final da lista
-I - adiciona uma regra no começo da lista
-R - altera uma regra
-D - apaga uma regra
-N - cria uma nova chain
-X - apaga uma chain
-P - altera a regra padrão

-L - lista as regras
-F - apaga todas as regras
-Z - zera os contadores
-s - ip ou rede de origem
-d - ip ou rede de destino
-i - interface de entrada
-o - interface de saída
-p - protocolo
udp - protocolo udp
tcp - protocolo tcp
icmp - protocolo icmp
--dport - porta de destino
--sport - porta de origem
-j - ação
DROP - ignora o pacote
REJECT - bloqueia (avisa a origem)
ACCEPT - permite
-m - módulo
--state - checa a relação deste pacote com as demais conexões
INVALID - desconhecido
ESTABLISHED - conexão estabelecida
NEW - abre uma nova conexão
RELATED - abre uma nova conexão, porém relacionada a uma conexão já existente
! - inverte a ação

iptables-save - salva as regras de fiewall em um arquivo
iptables-restore - restaura as regras de firewall previamente salvas pelo iptables-save
ip - ferramenta para manipulação das configurações de rede
link - mostra informações sobre o link (mii-tool)
address - configuração de ip (ifconfig)
route - tabela de roteamento (route)
neigh - tabela de mac-address (arp)}

212.2{ Peso 2 - Segurança em servidores FTP - 17/06

ftp ativo - cliente abre conexão com servidor e servidor abre conexão com cliente na próxima porta
ftp passivo - cliente abre conexão com servidor que avisa ao cliente para se conecar em outra porta porta
vsftpd - servidor de ftp com chroot nativo
/etc/vsftpd.conf - principal arquivo de configuração
listen=yes - necessário quando não estiver rodando sob o inetd
anonymous_enable - habilita o acesso anônimo
write_enable - permissão para gravação
anon_upload_user - permite que o usuário anônimo faça upload
chroot_local_user - permite o chroot
local_enable - permite autenticação local
chroot_list_file - arquivo que contém os usuários que farão ou não chroot
se chroot_local_user=yes, usuários em chroot_list_file não farão chroot

se chroot_local_user=no, usuários em chroot_list_file farão chroot
pure-ftpd - outro servidor de ftp
/etc/pure-ftpd.conf - arquivo de configuração
MaxClientsNumber - número máximo de clientes
MaxClientsPerIP - número de conexões por ip
NoAnonymous yes - desabilita o acesso anônimo
TLS 1 - habilita o sftp
parâmetros usados na linha de comandos do pure-ftp
-i - desabilita o upload anônimo
-m - previne upload anônimo se a máquina estiver com alto volume de cpu
-n - habilita a quota
--ipv4only, -4 - usa somente ipv4
--chrooteveryone, -A - faz o chroot de cada cliente
--daemonize, -B - roda como daemon
--anonymousonly, -e - habilita a conexão anônima
pure-pw - gerencia usuários do pure-ftp
proftpd - outro servidor de ftp
/etc/proftpd/proftpd.conf - principal arquivo de configuração
UseIPv6 on - habilita o suporte a ipv6
ServerName - nome do servidor
DefaultRoot ~ - faz com que o usuário faça chroot
RequireValidShell - vai permitir ou não que usuários sem shell façam login
Port - porta usada pelo ftp
MaxInstances - número máximo de conexões simultâneas
ServerType - standalone ou inetd}
212.3{ Peso 4 - Shell seguro (SSH) - 20/06
/etc/ssh - Pasta de configuração do ssh
sshd_conf - arquivo de configuração do servidor
PermitRootLogin - permite ou não login pelo root
Protocol - versao do protocolo (o 2 é mais seguro)
Port - porta usada pelo servidor ssh
IgnoreRhosts - ignora ou não acessos sem senha vindos dos IPs cadatrados em ~/.rhosts e ~/.shosts
PubkeyAuthentication - habilita a autenticação via chave público/privada
X11Forwarding - permite ou não a passagem de telas gráficas
AllowTCPForwarding - permite o redirecionamento de portas
ssh_config - configuração dos clientes
ssh - cliente ssh
-X - permite passagem de telas gráficas
-i - especifica a chave pública
-p - porta
-l - especifica o usuário
usuário@servidor - padrão para conexão ao servidor ssh
ssh_host_rsa_key - chave privada do ssh
~/.ssh - pasta do cliente
know_hosts - chave dos servidores que você já conectou

authorized_keys - arquivo com as chaves públicas dos hosts que podem se conectar sem senha ao meu servidor
id_rsa - chave privada
id_rsa_pub - chave pública
ssh-keygen - cria o par de chaves para autenticação
-t - tipo de chave
-b - tamanho da chave
ssh-copy-id - copia a chave pública para o servidor
ssh-agent - armazena a chave num chaveiro que vale para a sessão atual
ssh-add - adiciona a chave na sessão atual
ssh -fNL porta1:localhost:porta2 usuário@ip - redirecionamento de portas (túnnel)
-f - executar em segundo plano
-N - sem sessão na máquina local
-L - porta local
porta1 - a porta que será aberta na máquina local
localhost - para onde o tráfego será destinado
porta2 - para qual porta no destino o tráfego será destinado
usuário@ip - login na máquina local que o túnel rodará
exemplo - ssh -fNL 2222:172.20.1.1:3389 ricardo@localhost
scp - cópia de arquivos via ssh}
212.4{ Peso 3 - Tarefas de segurança - 23/06
lastb - lista os últimos logins mal sucedidos
IDS - Intrusion Detection System
fail2ban, snort, openvas, nessus - ferramentas de segurança
jail.conf - arquivos de regras do fail2ban
NVT - Network Vulnerability Test
nmap - scanner de portas
-sU - procura por portas udp
-sV - tenta determinar o software e versão que está usando a porta
-p - portas a escanear
-O - tenta descobrir a versão do sistema operacional
-A - escaneia todas as portas abertas e tenta descobrir a versão do sistema operacional
Bugtraq, CERT e CIAC - sites de avisos de segurança
netcat - ferramenta de rede
-z - escaneia as portas de um host}
212.5{ Peso 2 - OpenVPN - 26/06
/etc/openvpn/ - pasta de configuração
openvpn.conf - arquivo de configuração
client - a máquina será o cliente
dev tun - tipo de interface utilizada
proto udp - protocolo utilizado
remote 200.2.3.4 1194 - endereço ip e porta do servidor
push "route ip máscara" - essa rede deve ser alcançada pelo túnel
udp 1194 - porta usada pelo openvpn}}