

Mini-Curso

Segurança Linux

Alexandro Silva

- Apresentação
- Objetivo
- Ementa
- Bibliografia
- Planejamento das aulas
- Avaliação

Apresentação

Professor

- Atua no mercado OpenSource a mais de 10 anos
- Sysadmin do Projeto Gnome
- Consultor em Segurança da Informação e Tecnologias OpenSource
- Membro oficial do Ubuntu Internacional nas áreas de segurança e documentação

Objetivo

- Apresentar ao aluno os conceitos sobre os serviços de internet no Gnu/Linux com foco em segurança.

Apresentação Matéria

Ementa

- Introdução
 - O que é o Gnu/Linux
 - Distribuições
- Hardening
 - Conceitos
 - Procedimentos
 - Pré e Pós Instalação
 - Bastille

Apresentação Matéria

Ementa

- DNS
 - Conceitos
 - O que é
 - DNS primário e secundário
 - DNSsec
 - Bind9
 - Instalação
 - Configuração
 - Servidor Master
 - Servidor Slave com DNSsec

Apresentação Matéria

Ementa

- Web Server
 - Conceitos
 - Apache
 - Instalação
 - Configuração
- Proxy
 - Conceitos
 - Squid
 - Instalação
 - Configuração
 - Complementos

Apresentação Matéria

Ementa

- Mail Server
 - Conceitos
 - Postfix
 - Instalação
 - Configuração
 - Complementos

Bibliografia

Shema, Mike Hack Notes - Segurança na Web
Campus / Elsevier

Dhanjani, Nitesh Hack Notes - Segurança no
Linux e Unix Campus / Elsevier

Anônimo Segurança Máxima para LINUX
Campus / Elsevier

Melo, Domingos, Correia e Maruyama BS7799,
Da Tática à Prática em Servidores Linux Alta
Books

Planejamento das aulas

Aulas expositivas – Abordagem teórica da do assunto.

Laboratório – Atividades práticas dos assuntos abordados

Hardening Linux

Hardening Linux

- É o processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas - com foco na infra-estrutura e objetivo principal de torná-la preparada para enfrentar tentativas de ataque.

Hardening Linux

- Limitar o software instalado àquele que se destina à função desejada do sistema;
- Aplicar e manter os patches atualizados, tanto de sistema operacional quanto de aplicações;
- Revisar e modificar as permissões dos sistemas de arquivos, em especial no que diz respeito a escrita e execução;
- Reforçar a segurança do login, impondo uma política de senhas fortes.

Hardening Linux

Procedimentos

- Pré-instalação:
 - Planejamento de daemons/serviços;
 - Esquemas de particionamento.
- Pós-Instalação:
 - Proteger o GRUB com senha;
 - Atualizações e Patches;
 - Remover serviços desnecessários;
 - Remover SUID/SGID;
 - Uso do sudo;
 - Bloquear o usuário root.

Hardening Linux

Pós-instalação - Prática

- Atualização do sistema:
 - aptitude update && aptitude safe-upgrade
- Protegendo o GRUB
 - grub-md5-crypt
 - Password: **INFORME SENHA <ENTER>**
 - Retype password: **REPITA SENHA <ENTER>**
 - Copie o hash informado
 - vim /boot/grub/menu.lst

Hardening Linux

Pós-instalação - Prática

– vim /boot/grub/menu.lst

```
title                Debian GNU/Linux, kernel 2.6.26-2-686
root                 (hd0,1)
kernel               /boot/vmlinuz-2.6.26-2-686 root=/dev/hda2 ro
                    quiet
initrd               /boot/initrd.img-2.6.26-2-686
password --md5 $1$i/MM1/$cB0VonMnHi9fyOxuGp7JB1
```

Hardening Linux

Pós-instalação - Prática

Habilitar sudo:

- aptitude install sudo
- addgroup admin
- adduser aluno admin
- vim /etc/sudoers

Hardening Linux

Pós-instalação - Prática

- vim /etc/sudoers

Uncomment to allow members of group
sudo to not need a password

(Note that later entries override this, so you
might need to move it further down)

%sudo ALL=NOPASSWD: ALL

%admin ALL=(ALL) ALL

Hardening Linux

Pós-instalação - Prática

- Bloqueando o usuário root:
 - `usermod -L root`
- Para desbloquear:
 - `usermod -U root`

Hardening Linux Bastille

- O Bastille protege o sistema operacional, configurando o sistema de maneira proativa para aumentar sua segurança e reduzir as chances de comprometimento.
- Ele também pode ser usado para acessar no processo de Hardening do sistema, reportando e detalhando cada configuração de segurança usada pelo programa.

Hardening Linux Bastille

- Para instalar o Bastille execute:
 - `aptitude install bastille`
- Para executá-lo em modo gráfico:
 - `bastille -x`
- Para executá-lo em modo texto (ncurses):
 - `bastille`

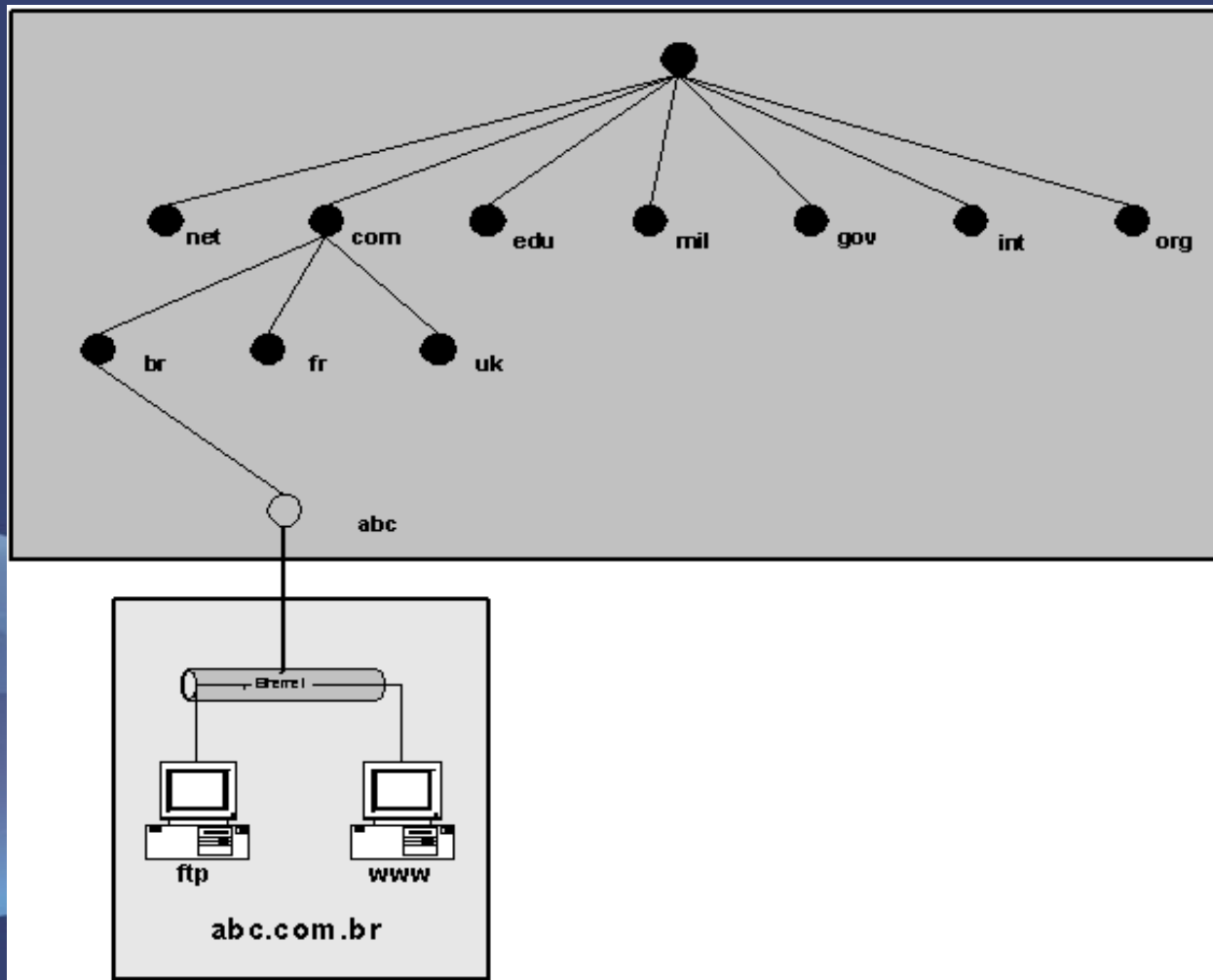
Domain Name System (Bind DNS)

DNS

Conceitos básicos

- O sistema de distribuição de nomes de domínio foi introduzido em 1984 e com ele os nomes de hosts residentes em um banco de dados pode ser distribuído entre servidores múltiplos, diminuindo assim a carga em qualquer servidor que provê administração no sistema de nomeação de domínios.

DNS Hierarquia



DNS

Conceitos

- Os dados associados com os nomes de domínio estão contidos em Resource Records ou RR (Registro de Recursos)
 - Tipos comuns de Records
 - SOA – Indica onde começa a autoridade a zona
 - NS – Indica um servidor de nomes para a zona
 - A – Mapeamento de nome a endereço (Ipv4)
 - AAAA – Mapeamento de nome a endereço (Ipv6)
 - MX – Indica um mail exchanger para um nome
 - CNAME – Mapeia um nome alternativo (apelido)

DNS

Conceitos

- Arquivo de zona – Possui os RRs referentes a um determinado domínio, sendo que cada domínio possui um arquivo de zona.
- Tipos de servidores:
 - Servidor Recursivo – Ao receber requisições de nomes, faz requisições para os servidores autoritativos e conforme a resposta recebida dos mesmos continua a realizar requisições para os outros servidores autoritativos até obter a resposta satisfatória.

DNS

Vulnerabilidades

- Poluição de cache
- Impersonificação do recursivo
- Impersonificação do master
- Updates não autorizados
- Dados corrompidos

DNS

Reverso

- O DNS Reverso resolve o endereço IP, buscando o nome de domínio associado ao host. Ou seja, quando temos disponível o endereço IP de um host e não sabemos o endereço do domínio, tentamos resolver o endereço IP através do DNS reverso que procura qual nome de domínio está associado aquele endereço.

DNS

Reverso

- Os servidores que utilizam o DNS Reverso conseguem verificar a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS, isto evita spams por exemplo.

DNS

DNSsec

- O DNSSEC adiciona é um sistema de resolução de nomes mais seguro, reduzindo o risco de manipulação de dados e domínios forjados. O mecanismo utilizado é baseado na tecnologia de criptografia que emprega assinaturas.
- Ele utiliza um sistema de chaves assimétricas. Isso significa que alguém com um domínio compatível com DNSSEC possui um par de chaves eletrônicas que consistem em uma chave privada e uma chave pública.
- Atualmente o domínio que utiliza esta tecnologia é o jus.br

DNS

DNSsec

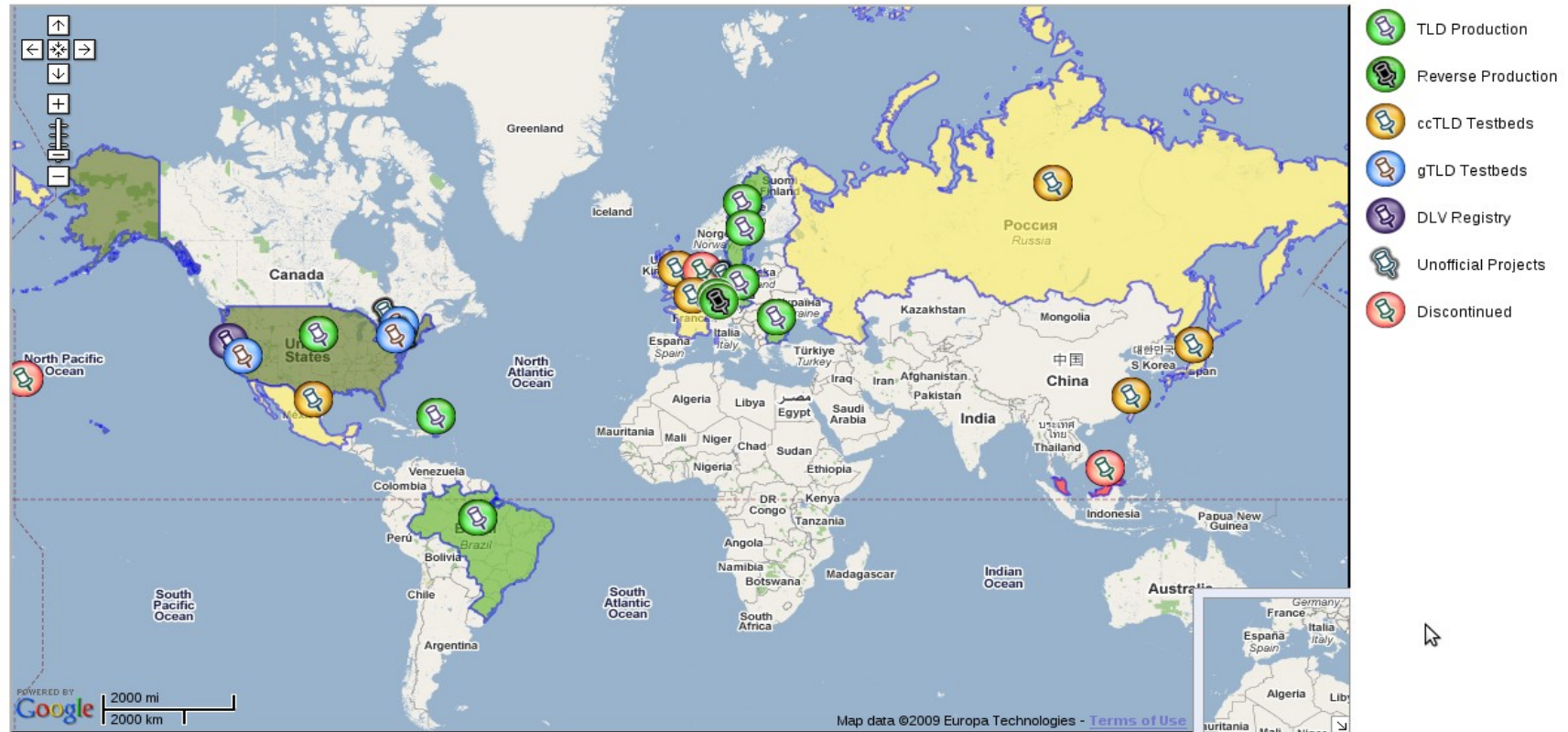
- O que garante?
 - Origem (Autenticidade)
 - Integridade
 - A não existência de um nome ou tipo
- O que não garante?
 - Confidencialidade
 - Proteção contra ataques de negação de serviço (DOS)

DNS

DNSsec no mundo

World Wide DNSSEC Deployment

See also [DNSSEC Theory and World Wide Deployment](#) by Paul Wouters, November 21, 2007, [SecTor](#)



This map was created by Paul Wouters

DNS

Prática – Servidor primário

- Instalação e Configuração
 - aptitude install bind9
 - cd /etc/bind
 - cp named.conf.local named.conf.local.ORIG
 - vim /etc/bind/named.conf.local

DNS

Prática – Servidor primário

– vim /etc/bind/named.conf.local

```
zone "acme.local" {
```

```
type master;
```

```
file "/etc/bind/zones/acme.local.db";
```

```
};
```

```
zone "0.168.192.in-addr.arpa" {
```

```
type master;
```

```
file "/etc/bind/zones/rev.0.168.192.in-addr.arpa";
```

```
};
```

DNS

Prática – Servidor primário

- `cp named.conf.options named.conf.options.ORIG`
- `vim /etc/bind/named.conf.options`

```
forwarders {  
208.67.222.222;  
};
```

DNS

Prática – Servidor primário

- `mkdir /etc/bind/zones`
- `vim /etc/bind/zones/acme.local.db`

– vim /etc/bind/zones/acme.local.db

\$TTL 604800

@ IN SOA acme.local. admin.acme.local. (

2009051301 ; Serial

7200 ; Refresh (2 horas)

120 ; Retry (2 minutos)

2419200 ; Expire (1 mes)

604800) ; Default TTL (1 semana)

;

@ IN NS ns1.acme.local.

acme.local. IN MX 10 mail.acme.local

acme.local. IN A 192.168.0.1

www IN CNAME acme.local.

mail IN A 192.168.0.1

– vim /etc/bind/zones/rev.0.168.192.in-addr.arpa

```
$TTL 1d;
```

```
$ORIGIN 0.168.192.IN-ADDR.ARPA.
```

```
@ IN SOA ns1.acme.local. admin.acme.local. (  
    2009051301  
    7200  
    120  
    2419200  
    604800  
)
```

```
IN NS ns1.acme.local.
```

```
1 IN PTR ns1.acme.local.
```

DNS

Prática – Servidor primário

– `/etc/init.d/bind9 restart`

– `vim /etc/resolv.conf`

search acme.local

nameserver 192.168.0.1

– `dig acme.local`

DNS

Prática – Servidor secundário com DNSsec

- `mkdir /etc/bind/zones`
- No master e no slave
 - `vim /etc/bind/named.conf.options`
dnssec-enable yes;
- No slave
 - `dnssec-keygen -a hmac-md5 -b 128 -n host acme.local`

DNS

Prática – Servidor secundário com DNSsec

- No master e no slave
 - /etc/bind/named.conf

```
key "TRANSFER" {  
    algorithm hmac-md5;  
    secret "INFORME AQUI A CHAVE";  
};
```

DNS

Prática – Servidor secundário com DNSsec

- No master
 - /etc/bind/named.conf
- ```
server 192.168.0.2 {
 keys {
 TRANSFER;
 };
};
```

# DNS

## Prática – Servidor secundário

- No slave com DNSsec

– vim /etc/bind/named.conf

```
server 192.168.0.1 {
```

```
 keys {
```

```
 TRANSFER;
```

```
 };
```

```
};
```

# DNS

## Prática – Servidor secundário

- No slave com DNSsec

– vim /etc/bind/named.conf.local

```
zone "acme.local" {
 type slave;
 file "/etc/bind/zones/slave_acme.local";
 masters { 192.168.0.1; };
 allow-notify { 192.168.0.1; };
};
```

# DNS

## Prática – Servidor secundário com DNSsec

- No master e no slave
    - vim /etc/bind/named.conf
- ```
include "/etc/bind/rndc.key";
```

DNS

Prática – Servidor secundário com DNSsec

- No master
 - aptitude aptitude install ntp ntpdate
 - ntpdate ntp.pop-ba.rnp.br
 - /etc/init.d/bind9 restart
- No slave
 - ntpdate 192.168.0.1
 - /etc/init.d/bind9 restart

Web Server (Apache)

Apache Web Server

Histórico

- O servidor Apache surgiu no National Center of Supercomputing Applications (NCSA) através do trabalho de Rob McCool.
- Ao sair da NCSA, McCool parou de trabalhar no software (que nessa época recebia justamente a denominação NCSA) e então várias pessoas e grupos passaram a adaptar o servidor Web às suas necessidades.

Apache Web Server

Prática

- `aptitude install apache2 openssl ssl-cert`
- `a2enmod ssl`
- `sudo openssl req @$@ -new -x509 -days 365 -nodes -out /etc/apache2/apache.pem -keyout /etc/apache2/apache.pem`
- `sudo chmod 600 /etc/apache2/apache.pem`
- `cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl`
- `ln -s /etc/apache2/sites-available/ssl /etc/apache2/sites-enabled/`

Apache Web Server

Prática

– `vim /etc/apache2/sites-available/ssl`

NameVirtualHost *:443

<VirtualHost *:443 >

ServerAdmin webmaster@localhost

...

CustomLog /var/log/apache2/access.log combined

SSLEngine on

ServerSignature On

SSLCertificateFile /etc/apache2/apache.pem

Apache Web Server

Prática

– `sudo apache2ctl restart`

– `a2enmod rewrite`

– `vim /etc/apache2/sites-available/default`

...

`CustomLog /var/log/apache2/access.log combined`

`ServerSignature On`

`RewriteEngine on`

`RewriteRule ^(.*)$ https://%{SERVER_NAME}$1 [L,R]`

`RewriteLog "/var/log/apache2/rewrite.log"`

`RewriteLogLevel 2`

...

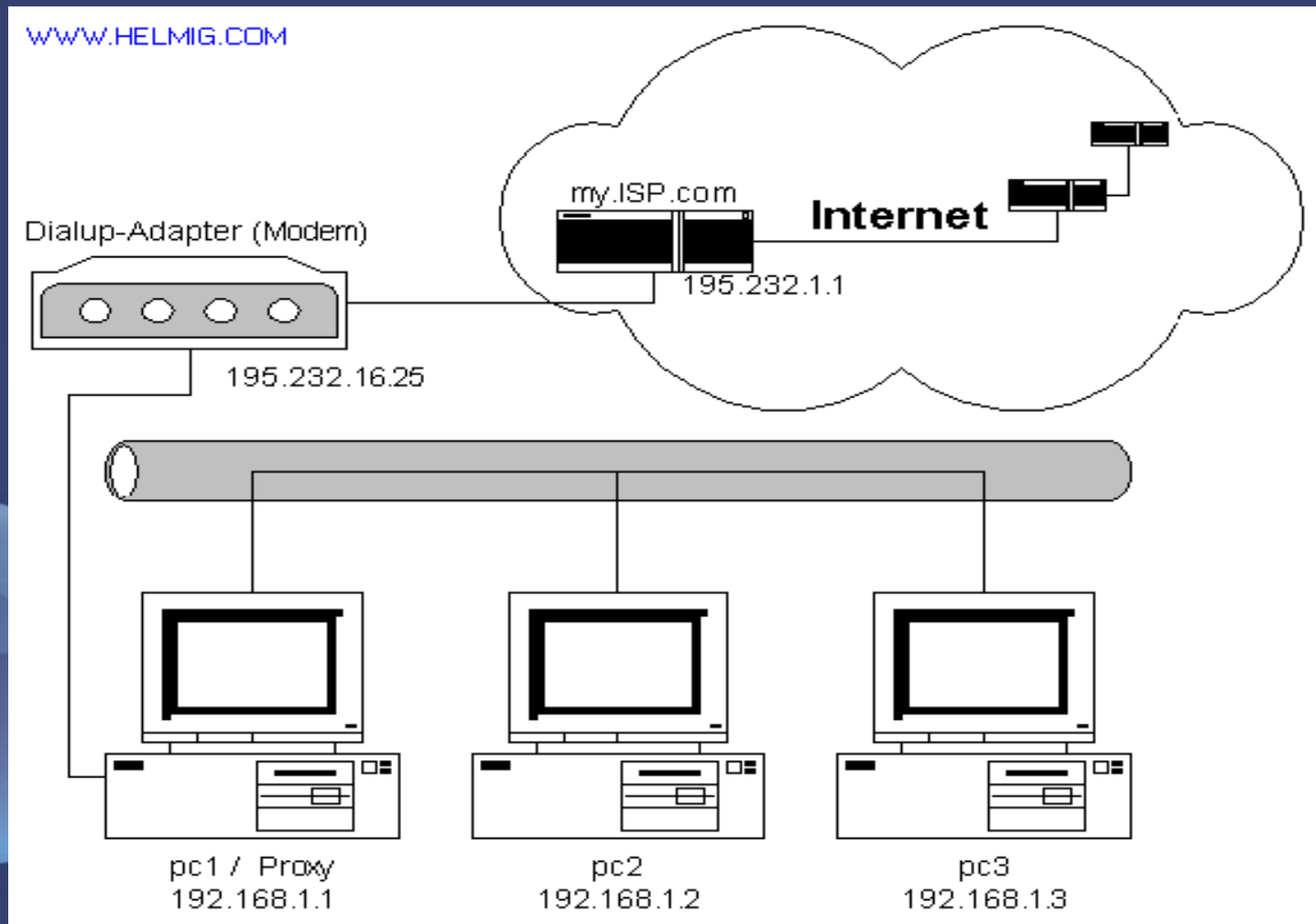
Proxy Server (Squid)

Squid Proxy Server

Histórico

- Proxy é um servidor que atende a requisições repassando os dados a outros servidores. Um usuário conecta-se a um servidor proxy, requisitando algum serviço, como um arquivo, conexão, website, ou outro recurso disponível em outro servidor.
- Podemos dividi-los em:
 - Web Proxy
 - Proxy Transparente
 - Proxy anônimo

Squid Proxy Server



Squid Proxy Server

Prática

- aptitude install squid dansguardian sarg
- cd /etc/squid
- cp squid.conf squid.conf.orig
- vim /etc/squid/squid.conf

...

```
acl CONNECT method PURGE  
acl redelocal src 192.168.0.0/24
```

...

```
http_access allow redelocal
```

Squid Proxy Server

Prática

– vim /etc/squid/bloqueio

www.gmail.com

www.google.com

– vim /etc/squid/squid.conf

...

acl redelocal src 192.168.0.0/24

**acl BLOQUEIO url_regex -i
"/etc/squid/bloqueio"**

...

http_access allow redelocal !BLOQUEIO

Squid Proxy Server

- Tuning do squid
 - <http://linuxadm.blogspot.com/2008/06/squid-tuning-mais-dicas-aumentando.html>

Squid Proxy Server

Complementos

- Dansguardian
 - O DansGuardian é outra opção de filtro de conteúdo desenvolvido para trabalhar em conjunto com o Squid, filtrando conteúdo indesejado.
 - A grande diferença entre ele e o SquidGuard é que o SquidGuard se limita a bloquear páginas contidas nas listas, enquanto o DansGuardian utiliza um filtro adaptativo, que avalia o conteúdo da página e decide se ela é uma página imprópria com base no conteúdo.

Squid Proxy Server Complementos

- SARG
 - O SARG (Squid Analysis Report Generator) é uma ferramenta desenvolvida por um brasileiro que permite à você ver para onde seus usuários estão indo na Internet através da análise do arquivo de log do Squid/Dansguardian.

Squid Proxy Server

Prática -

Dansguardian

- `aptitude install dansguardian`
- `cd /etc/dansguardian/`
- `cp dansguardian.conf dansguardian.conf.ORIG`
- `vim /etc/dansguardian/dansguardian.conf`
- Comente a linha:
 - `UNCONFIGURED` – Please remove this line after configuration

Squid Proxy Server

Prática - SARG

- `aptitude install sarg`
- `sarg -c /etc/squid/sarg.conf`

Mail Server (Postfix)

Mail Server Postfix

- O Postfix é um agente de transferência de emails (MTA), um software livre para envio e entrega de emails. Rápido e fácil de administrar, é uma alternativa segura ao Sendmail.
- Ele é o MTA padrão da maioria das distribuições Linux.

Postfix Mail Server

Prática

- `vim /etc/apt/sources.list`
- Adicione a seguinte linha:
`deb http://www.backports.org/debian lenny-backports main contrib non-free`
- `aptitude update`
- `aptitude install postfix mailscanner
spamassassin pyzor razor`
- `/etc/init.d/postfix stop`

Postfix Mail Server

Prática

- `cd /etc/postfix/`
- `cp main.cf main.cf.ORIG`
- `vim main.cf`
- Adicione a linha
 - `header_checks = regexp:/etc/postfix/header_checks`
- Crie o arquivo `header_checks`
 - `vim /etc/postfix/header_checks`
- Adicione a seguinte linha:
 - `/^Received:/ HOLD`

Postfix Mail Server

Prática

- Digite *freshclam* para atualizar o clamav
- Digite *pyzor discover* para atualizar o pyzor
- Digite:
 - `mkdir /var/spool/MailScanner/spamassassin`
 - `chown postfix:postfix \`
`/var/spool/MailScanner/spamassassin`
 - `cd /etc/Mailscanner`
 - `cp Mailscanner.conf Mailscanner.conf.ORIG`

Postfix Mail Server

Prática

- vim Mailscanner.conf
 - %org-name% = matrix
 - %org-long-name% = Matrix Corp
 - %web-site% = www.matrix.local
 - Run As User = postfix
 - Run As Group = postfix
 - Incoming Queue Dir = /var/spool/postfix/hold
 - Outgoing Queue Dir = /var/spool/postfix/incoming
 - MTA = postfix
 - Virus Scanners = clamav

Postfix Mail Server

Prática

- Spam Subject Text = [Spam]
- Rebuild Bayes Every = 86400
- Wait During Bayes Rebuild = yes
- SpamAssassin User State Dir =
/var/spool/MailScanner/spamassassin
- vim /etc/default/mailscanner
 - Descomente a linha run_mailscanner=1
- /etc/init.d/mailscanner start
- /etc/init.d/postfix start

Postfix Mail Server

Prática – Dovecot

- O Dovecot é atualmente o mais seguro servidor de IMAP e POP3. Ele suporta mbox, Maildir e seu próprio formato nativo de alta performance Dbox.
- Ele é 100% compatível com os servidores UW-IMAP, Courier IMAP, e clientes de emails acessando as caixas de correio diretamente.

Postfix Mail Server

Prática – Dovecot

- `aptitude install dovecot`

Fontes

- Fórum Debian
<http://wiki.forumdebian.com.br>
- Wikipedia - <http://www.wikipedia.org>
- Penguin's Place -
<http://penguin.wordpress.com>