

# Servidor Web com foco em VPS (Apache, PHP, MySQL, iRedMail, Segurança, etc.)



Ribamar FS – <http://ribafs.org>

2014

# **Servidor Web com foco em VPS**

---

## **Ficha Catalográfica**

---

S725c

Servidor Web com foco em VPS / Ribamar  
Ferreira de Sousa. - Fortaleza: Clube de Autores, 2014  
168p.  
1. Servidores Linux. 2. Administração. I.  
Título.

---

## **Normalização Bibliográfica**

Lúcia Maria Piancó Chaves – DNOCS-CGE/MD  
Margarida Lídia de Abreu Vieira – DNOCS-CGE/MD

# Índice

|   |    |
|---|----|
| Prefácio.....   | 6  |
| Introdução.....   | 7  |
| Dados Importantes para a Instalação e Configuração.....             | 9  |
| Agradecimentos.....   | 9  |
| 1.0 - Roteiro de Migração de Site para outra Hospedagem.....        | 11 |
| 1.1 - Backup Completo.....  | 11 |
| 1.2 - Redirecionar Tudo.....  | 11 |
| 1.3 - Migração.....   | 12 |
| 2.0 - Ajustes Iniciais.....   | 15 |
| 2.1 - Em caso de migração veja o capítulo 1.....                    | 15 |
| 2.2 - Criar novo usuário para administrar o servidor.....           | 15 |
| 2.3 - Criando Chave do SSH para acessar sem senha.....              | 16 |
| 2.4 - Mudar o fuso horário.....                                     | 17 |
| 2.5 - Criar uma partição de swap no Ubuntu.....                     | 17 |
| 2.6 - Configurar locales.....                                       | 17 |
| 2.7 - Configurar hostname e hosts.....                              | 17 |
| 2.8 - Instalar servidores de horário.....                           | 18 |
| 2.9 - DNS.....  | 19 |
| Migração do Domínio.....  | 19 |
| Exemplo de DNS no DigitalOcean.....                                 | 21 |
| Zone File.....  | 22 |
| Exemplo de DNS no registro.br.....                                  | 27 |
| Exemplo de DNS no Amazon AWS.....                                   | 30 |
| 3.0 - Instalação do iRedMail.....                                   | 37 |
| Desinstalação.....  | 44 |
| Dicas sobre o iRedMail.....   | 44 |
| Configurações Extras no iRedMail.....                               | 47 |
| 3.1 - Antispam no RoundCube.....                                    | 47 |
| 3.2 - Configurando o registro dkim para outros domínios.....        | 49 |
| 3.3 - Configurando o registro SPF do iRedMail no DNS.....           | 50 |
| 3.4 - Configuração do fail2ban.....                                 | 50 |
| 3.5 – Mais Algumas configurações do iRedMail.....                   | 53 |
| 3.6 - Customizar Título do Navegador e do Roundcube.....            | 55 |
| 3.7 - Como mudar o tamanho dos anexos dos e-mails no RoundCube..... | 55 |
| 3.8 - Adicionar identidades ao Roundcube.....                       | 56 |
| 3.9 - Instalar Plugins no Roundcube.....                            | 56 |
| 3.10 - Adicionar novo domínio ao iRedMail.....                      | 56 |
| 4.0 - Melhorando a Segurança do Servidor.....                       | 59 |
| 4.1 - SSH hardening.....  | 59 |
| 4.2 - Monitorando login do root.....                                | 60 |
| 4.3 - Sanitizar Joomla.....   | 60 |
| 4.4 - Instalar e usar o W3AF.....                                   | 61 |
| 4.5 - Atualizações automáticas de segurança.....                    | 62 |
| 4.6 - Protegendo administrators com SSL.....                        | 62 |
| 4.7- Configurando e usando fail2ban.....                            | 63 |
| 4.8 - Sanitizar MySQL.....  | 65 |
| 4.9 - Sanitizar o Apache.....                                       | 65 |
| 4.10 - Sanitizar o PHP.....   | 65 |
| 4.11 - Sanitizar IPTables.....                                      | 67 |

|  |     |
|--|-----|
| 4.12 - Sanitizar Registros do DNS para e-mail.....                     | 67  |
| 4.13 - Instalando o IDS psad.....                                      | 68  |
| 4.14 - Melhorando a segurança do SSH com Denyhosts.....                | 69  |
| 4.15 - Monitorando rootkits com RKHunter.....                          | 70  |
| 4.16 - Testando vulnerabilidades web com Nikto.....                    | 71  |
| 4.17 - Monitorando a rede com ngrep.....                               | 72  |
| 4.18 - Melhorando a segurança com o pacote harden.....                 | 72  |
| 4.19 - Proteger su limitando o acesso somente para o grupo admin.....  | 72  |
| 4.20 - Prevenir IP Spoofing.....                                       | 72  |
| 4.21 - Sanitizar a memória compartilhada.....                          | 73  |
| 4.22 - Atualizando para a versão mais recente.....                     | 74  |
| 4.23 - Scannear portas abertas.....                                    | 74  |
| 4.24 - Monitorar arquivos modificados.....                             | 74  |
| 4.25 - Melhorar a segurança em partições.....                          | 74  |
| 4.26 - Sanitizar seu Desktop.....                                      | 75  |
| 4.27 - phpsecinfo.....   | 75  |
| 4.28 - Monitorar logs com o logcheck.....                              | 75  |
| 4.29 - Ajustando as Permissões do /var/www.....                        | 76  |
| 4.30 - Upgrade do Ubuntu Server Entre as versões.....                  | 78  |
| 4.31 - Terminal Web.....   | 79  |
| 4.32 - Usando Senhas Fortes no Servidor.....                           | 79  |
| 4.33 - Instalação e Configuração do mod_security e do mod_evasive..... | 80  |
| 4.33.1 - Instalação do mod_security e do mod_evasive.....              | 80  |
| 4.33.2 - Liberando sites no mod_security.....                          | 82  |
| 4.33.3 - Testando segurança de sites.....                              | 84  |
| 5.0 - Configurar Apache e PHP.....                                     | 87  |
| 5.1 - Dar suporte aos arquivos .htaccess.....                          | 87  |
| 5.2 - Adicionar extensões ao PHP.....                                  | 87  |
| 5.3 - Adicionar um Subdomínio.....                                     | 88  |
| 5.4 - Adicionar um Domínio.....  | 88  |
| 5.5 - Proteger alguns diretórios com senha pelo Apache.....            | 89  |
| 5.6 - Proteger seções administrador de sites Joomla forçando SSL.....  | 90  |
| 6.0 - Criação dos Bancos.....  | 93  |
| 6.1 - MySQL.....   | 93  |
| 6.2 - PostgreSQL.....  | 94  |
| 7.0 - Instalar sites e aplicativos, descompactando no /var/www.....    | 97  |
| 8.0 - Monitorando o servidor.....                                      | 99  |
| 8.1 - Monitorando manualmente.....                                     | 99  |
| 8.2 - Adicionar Serviços ao Boot num Debian.....                       | 101 |
| 8.3 - Remover serviços do boot.....                                    | 101 |
| 8.4 - Desabilitar bluetooth.....                                       | 101 |
| 8.5 - Ferramentas para gerenciar serviços no boot.....                 | 101 |
| 8.6 - Monitorando logs com o Logcheck.....                             | 102 |
| 8.7 - Analisar arquivos de log com o logwatch.....                     | 102 |
| 8.8 - Instalar Nagios para Monitorar Servidores.....                   | 103 |
| 8.9 - Melhor visualização dos acessos do Apache com o goaccess.....    | 105 |
| 8.10 - Deixando a saída dos logs colorida.....                         | 105 |
| 8.11 - Desabilitando o login via SSH de todas as contas.....           | 106 |
| 8.12 - Monitorando ações dos usuários.....                             | 106 |
| 8.13 - Dividindo a tela em duas.....                                   | 106 |
| 8.14 - Usando htop.....  | 107 |
| 8.15 - Que programas estão usando a banda.....                         | 107 |

|  |     |
|--|-----|
| 8.16 - Monitorando a rede.....   | 107 |
| 8.17 - Gerenciamento de Arquivos.....  | 108 |
| 8.18 - Usando o cron para executar comandos agendados.....                         | 108 |
| 8.19 - Verificando BlackLists.....   | 110 |
| 9.0 – Alguns Comandos Úteis no Linux.....  | 111 |
| 10.0 - Testando o Servidor.....  | 121 |
| 10.1 - Testando com nmap.....  | 121 |
| 10.2 - Outros testes.....  | 133 |
| 11.0 - Ferramentas Úteis.....  | 137 |
| 11.1 - Testando desempenho de grandes servidores.....                              | 137 |
| 11.2 - Varrendo uma rede com Wireshark.....  | 137 |
| 11.3 - Instalar o webmin.....  | 137 |
| 11.4 - Logrotate.....  | 138 |
| 12.0 - Dicas Extras.....   | 141 |
| 12.1 - Exportar livro de endereços do Gamaail para ser importado no RoundCube..... | 141 |
| 12.2 - Firewall Básico com UFW.....  | 141 |
| 12.3 - Dicas para promover seu site.....   | 145 |
| 12.4 - Codificação de Caracteres.....  | 148 |
| 12.6 - Tunning do Apache.....  | 149 |
| 12.7 - DNS Free.....   | 156 |
| 12.8 - Erro comum no SSH.....  | 157 |
| 12.9 - Script para redirecionamento de página.....                                 | 157 |
| 13.0 - Servidor de Testes de Segurança.....  | 159 |
| 14.0 - Referências.....  | 161 |
| Posfácio.....  | 164 |

## Prefácio

***“Cada vez que presenciamos uma injustiça e não agimos, nós treinamos nosso caráter para ser passivo na presença dessa injustiça e assim eventualmente perdemos toda a habilidade de nos defender e defender aqueles que amamos.”***

***Julian Assange***

Parece que a primeira participação de Edward Snowden em um fórum do site Ars Technica, em 2001, foi perguntando como poderia montar seu próprio servidor. Na época, Snowden que se identificava como TheTrueHOOHA, pedia para serem delicados e que dessem dicas de como hospedar seu próprio servidor.

Todos nós hoje sabemos a importância de Snowden não só para o pessoal da área de Tecnologia da Informação (TI), mas para todas as pessoas que usam meios eletrônicos para se comunicar. Se em seu primeiro contato em busca de dicas para montar e hospedar seu servidor, TheTrueHOOHA não tivesse sido bem sucedido e tido boa acolhida, quem sabe se teríamos o Snowden de hoje?

Início este prefácio assim por duas razões. A primeira é chamar a atenção de todos para a necessidade de cuidados com segurança e privacidade de nossas aplicações, redes e servidores. As denúncias de Snowden, precedidas por aquelas feitas por integrantes do Wikileaks, mostram que vivemos em um verdadeiro panóptico virtual, vigiados por governos, agências secretas, corporações e sabe-se lá por quem mais.

A segunda é destacar a importância do conhecimento na área dos servidores para todos os profissionais de TI. Afinal é neles que rodam nossas aplicações, sites etc. O Ribamar (me orgulho em dizer, meu amigo de longa data), mais uma vez inova ao desmistificar de forma simples e prática uma área bastante nebulosa e que exige bons, senão excelentes, conhecimentos técnicos e muita dedicação.

Como ele mesmo diz, o livro trata do uso de um servidor Linux Ubuntu 12.04 em VPS destinado a abrigar um servidor web com Apache, PHP e MySQL. Mostra a instalação de uma boa solução de e-mail com webmail e outros bons recursos. O grande foco do livro fica na segurança do servidor, que acabou ganhando, merecidamente, a maior atenção.

Autor de vários outros livros, cursos e tutoriais, em grande parte voltados para o software livre, o Riba, como é conhecido, traz mais uma valiosa contribuição para quem trabalha com TI ou para quem é curioso e quer saber mais. E faz isto de forma livre e gratuita. Pela natureza técnica do trabalho, eu mesmo o aconselhei a publicar por uma editora e a vender o livro. Ele preferiu simplesmente disponibilizá-lo da forma atual (edição virtual gratuita), garantindo também que quem queira uma edição em papel possa tê-la. Algumas ideias não tem preço. Algumas atitudes também não. Parabéns ao Riba e boa leitura e excelente aprendizado para todos nós.

[Haroldo Barbosa](#)

Jornalista e desenvolvedor web

(<http://bitautonomo.blogspot.com/>)

# Introdução

## Objetivo principal deste livro

O objetivo é instalar um servidor que abrigue alguns sites, aplicativos e também ofereça uma solução de e-mail simples com webmail juntamente com a configuração do DNS através do painel de administração da hospedagem. Também aborda como criar subdomínios, proteger pastas com senha e adicionar outros domínios ao mesmo servidor.

O objetivo inicial era apenas o de compartilhar como se gerencia um servidor tipo VPS, que era meu novo brinquedinho. Acontece que comecei a perceber que agora estava sozinho e que a segurança era mais importante do que eu havia percebido. Foi então que eu sai procurando ajuda sobre como deixar meu servidor mais seguro, melhor, menos inseguro.

Aqui não tratarei de teoria sobre administração de servidores, mas apenas de passos práticos de como instalar, configurar e como melhorar a segurança. Não que a teoria não seja importante, é sim, mas para isso precisará procurar em outro lugar bons tutoriais na internet, livros e cursos.

Usei servidores com o sistema operacional Linux Ubuntu. Abordarei a instalação completa de um servidor destinado a abrigar alguns sites, um aplicativo, um diretório protegido, alguns subdomínios, um domínio extra.

É bom lembrar que aqui não faço propaganda da hospedagem, por mais que goste, nem de nenhuma empresa. Não digo que esta é a melhor, nem a única, nem nada do gênero. Encontrei vários pontos positivos, mas sei que podem existir outras empresas que podem ser melhores e isso depende também do que você espera da hospedagem. Este roteiro pode ser aplicado a outras empresas com as devidas adaptações, assim como a outras distribuições Linux também com as devidas adaptações. O grande foco aqui não é na administração do VPS, que geralmente é bem simples, mas foco na administração do servidor, instalação, configurações, otimizações e segurança de um servidor web, servidor de banco de dados e servidor de e-mail.

Servidores Web tem atualmente uma grande gama de funções. Aqui eu me restrinjo praticamente a abrigar alguns sites criados em PHP com MySQL, usando Apache2 como servidor web e tendo como sistema operacional o Linux Ubuntu além de oferecer uma solução de e-mail, com webmail e bons recursos com o iRedMail. Reforcei o foco na segurança, pois no VPS quem cuida da segurança somos nós administradores. Sei que não abordo muito, mas a minha intenção é a de mostrar este servidor proposto funcionando e razoavelmente seguro e, principalmente, despertar e estimular para uma atitude proativa em termos de segurança e eficiência.

## Público Alvo

O sistema operacional aqui abordado é o Linux, especificamente a distribuição Ubuntu, o que requer que você, para aproveitar bem a leitura e colocar em prática, tenha conhecimento de Linux. Chego a resumir muito vários assuntos, o que subentende que você precisa ter pelo menos uma ideia do que estou falando para acompanhar com proveito.

Para que você seja capaz de entender e colocar em prática os conhecimentos deste livro você precisa ter conhecimento de pelo menos administração de sites em hospedagens compartilhadas ou similares em servidores Linux. Caso não tenha este conhecimento e ainda assim queira aprender a administrar seu site em uma hospedagem tipo VPS, precisa ter uma boa motivação para aprender e assimilar os conhecimentos apresentados, tendo em vista que com VPS quase tudo fica a nosso cargo e praticamente não temos suporte da empresa que contratamos. O suporte oferecido é apenas para nos acostumarmos com a estrutura da administração web: criação da máquina virtual, DNS (quando oferece), backup/snapshot, reiniciar/parar servidor, etc. Quanto ao sistema operacional, firewall, ao Apache, PHP, MySQL, extensões, configurações, e-mails fica tudo conosco. Isso tem dois lados: mais trabalho por um lado mas mais controle por outro. Não é uma solução que atende a todos, portanto você precisa refletir se ela vai atender sua necessidade.

### **Servidor de E-mail**

Neste servidor instalo o iRedMail como solução de e-mails, que é a solução de e-mail free para pequenos servidores mais popular atualmente e conta com bons recursos, como antispam, spamassassin, webmail (Roundcube), iredadmin para a criação/gerenciamento de domínios e de e-mails, etc. Por conta do iRedMail, que instalarei com o MySQL, já receberei instalados o MySQL, o Apache e o PHP, entre outros. Apenas precisarei instalar alguns módulos adicionais do apache e algumas extensões do PHP e efetuar algumas configurações.

### **Sobre o Autor**

Ribamar FS – ribafs@gmail.com

Graduou-se em Engenharia civil e logo abandonou para trabalhar com informática em tempo integral: com Linux, programação web, PHP, Joomla, CakePHP, administração do PostgreSQL, administração de servidores Linux, etc.

Veja aqui um resumo sobre o que fiz e ando fazendo:

<http://ribafs.org/sobre-mim>

### **Alguns Pontos Positivos de uma Hospedagem do tipo VPS (Virtual Private Server)**

- Liberdade de instalar o que bem entender: php, ruby on rails, java, python, etc.
- Instalar e configurar módulos para o Apache.
- Instalar qualquer extensão para o PHP.
- Instalar o SGBD PostgreSQL.
- Instalar o que quiser para melhorar a segurança do servidor.
- Indicado se você gosta de você mesmo fazer e do seu jeito;
- Autonomia e agilidade: você não precisa pedir nada a ninguém, você mesmo resolve;
- Instalar a criptografia SSL e assim protejo melhor meus sites, especialmente o administrador;
- Criar um snapshot/backup e guardar o servidor

### **Alguns Pontos Negativos em uma Hospedagem do tipo VPS**

- Você trabalha mais, pois precisa instalar o servidor, o Apache, MySQL, PHP, configurar tudo e deixar pronto para instalar os sites. Também precisa instalar uma solução para enviar e receber e-mails, caso queira isso no servidor;
- Falta de suporte para assuntos relativos ao servidor em si, como envio e recebimento de e-mails, como apache parado, etc. Em geral só oferecem suporte sobre a estrutura administrativa da hospedagem;



# Dados Importantes para a Instalação e Configuração

## Domínios

ribafs.org e tiagoarts.com - HostGator

ribafs.net.br - Registro.br

ribafs.sub.es - uni.me

## IPs no Servermania

21.129.54.123, 21.129.54.124, 21.129.54.125 e 21.129.54.126

Aqui o IP 21.129.54.123 é o principal, associado ao domínio ribafs.net.br

## IP no DigitalOcean

162.243.89.121 ribafs.sub.es

Usei estes dados nas duas hospedagens, com servidores do tipo VPS.

## Hostnames

servermania – ribafs

digitalocean – ribafs.sub.es

## ***Agradecimentos***

Gostaria de agradecer ao meu camarada Haroldo Barbosa pela elaboração da nova capa deste livro. Muito agradecido meu caro Haroldo.



## 1.0 - Roteiro de Migração de Site para outra Hospedagem

- 1.1 - Backup Completo
- 1.2 - Redirecionar Tudo
- 1.3 - Migração

### 1.1 - Backup Completo

Antes de qualquer ação no novo servidor, efetuar um backup completo do servidor atual:

- copiar todo o /var/www

```
cd /var/www
tar czpvf varwww.tar.gz /var/www
mv *.tar.gz /home/ribafs
```

- Copiar a pasta:

/var/vmail/vmail1

- Executar manualmente para ter o backup de agora, pois já está no cron:

/var/vmail/backup/backup\_mysql.sh (o backup ficará dentro de

/var/vmail/backup/mysql)

Copiar toda a pasta do backup:

```
cp -ra /var/vmail/backup/mysql /home/ribafs
```

MUITO IMPORTANTE: Antes de restaurar os backups de arquivos e bancos fazer uma cópia do original, pois acontece de as novas versões serem incompatíveis com as anteriores

Para restaurar importe os scripts de /var/vmail/backup/mysql e copie

/var/vmail/vmail1

- arquivos de configuração a serem guardados:

apache (sites-available),

php.ini,

mod\_security,

mod\_evasive,

logcheck,

sshd\_config, etc

- e outros que achar por bem

- Guardar tudo em outro servidor (se possível) e uma cópia em seu desktop

- trocar senhas especialmente do usuário do SSH (usar senhas fortes, com 16 ou mais caracteres mais 1 ou 3 para o salt) .

Quando temos um site em uma hospedagem e mudamos para uma outra hospedagem.

É importante tomar cuidados para que quando o seu domínio apontar para a nova hospedagem seu site já estiver na nova e com tudo configurado, de forma a manter seu site no ar sem interrupção.

### 1.2 - Redirecionar Tudo

Muito importante quando vamos remover tudo de um servidor e reinstalar. Evita que o site fique fora por toda a reinstalação e mantenha um aviso de "Manutenção ...".

Providenciar para que no site novo todas as solicitações encontrem o index.php com o aviso.

Instalar o apache:  
apt-get install apache2

Habilitar o mod\_rewrite  
a2enmod rewrite  
service apache2 restart

Criar o aviso:

```
nano /var/www/index.php
```

Contendo:  
<h2>Em manutencao. Volta em breve!</h2>

Criar o  
nano /var/www/.htaccess

Contendo:  
# Redireciona tudo para o index.php do raiz recursivamente  
# Útil para criar página que captura erro 404, no lugar de index.php seria erro404.php  
RewriteEngine on  
RewriteCond %{REQUEST\_FILENAME} !-d  
RewriteCond %{REQUEST\_FILENAME} !-f  
RewriteCond %{REQUEST\_URI} !=/index.php  
RewriteRule ^ /index.php [L,R]

### **1.3 - Migração**

Primeiro devemos instalar o sistema operacional no novo servidor

- Criar o rebuild do servidor
- Conectar via SSH
- apt-get update; apt-get upgrade; reboot
- Configurar hostname e /etc/hosts
- Efetuar configurações básicas:
  - criar partição de swap,
  - adicionar novo usuário
  - efetuar algumas otimizações
- Instalar pacotes úteis como unzip, mc, etc
- Instalar iredMail
- Instalar webmin e liberar a porta 10000
- Instalar extensões de PHP
- Configurar apache: mod\_rewrite, .htaccess
- Configurar permissões do /var/www
- Criar bancos para os sites e aplicações
- Efetuar upload de sites e apps:
  - Ajustar os scripts de configuração de cada um para o novo banco, user e senha
  - Ajustar alguns links se necessário no novo servidor
- Criar e-mails
- Instalar sites extras/lojas virtuais
- Ao final ajustar o firewall e a segurança em geral (aliás, deveria ser feito no início)
- Configurar o DNS no novo servidor, juntamente com os devidos registros

- Adicionar SPF e DKIM para combate a spams
- Depois de tudo pronto mudar o domínio para o novo DNS
- Aguardar a propagação, que agora quando acontecer não deve ter surpresas
- Após tudo pronto e o domínio propagado vale a pena criar um Snapshot para guardar como backup

Veja o capítulo 2.0 (Ajustes iniciais).



## 2.0 - Ajustes Iniciais

- 2.1 - Backup completo do servidor atual
- 2.2 - Criar novo usuário para administrar o servidor, acessar via SSH, admin e sudoers
- 2.3 - Criando Chave do SSH para acessar sem senha
- 2.4 - Mudar o fuso horário
- 2.5 - Criar partição swap para VPS com pouca RAM, como 512MB
- 2.6 - Configurar locales
- 2.7 - Configurar hostname e hosts
- 2.8 - Instalar servidores de horário
- 2.9 - DNS

```
apt-get update
apt-get install nano unzip aptitude dnsutils mc rconf sysv-rc-conf splitvt
apt-get remove sendmail
```

- Trocar a senha de root, caso tenha recebido uma senha da hospedagem e exclua o e-mail com a mesma, se usando um e-mail público.

### 2.1 - Em caso de migração veja o capítulo 1

Caso seja um novo servidor, ao invés do backup faça um projeto detalhado de como quer o VPS

### 2.2 - Criar novo usuário para administrar o servidor

```
adduser ribafs
addgroup admin
adduser ribafs admin
nano /etc/sudoers
ribafs ALL=(ALL) NOPASSWD:ALL
```

```
su - ribafs
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_ribafs -t dsa (Enter 2 vezes)
cat ~/.ssh/id_ribafs*.pub > ~/.ssh/authorized_keys
chmod 600 ~/.ssh/*
exit
```

Agora já podemos sanear o SSH:

```
nano /etc/ssh/sshd_config
Port 65522
PasswordAuthentication yes
Protocol 2
LoginGraceTime 30 # reduzir tempo do timeout
AllowUsers ribafs root
```

```
service ssh restart  
exit
```

Volta para o micro local

Este será o usuário com o qual administrará o servidor, acessando via SSH. Remova o acesso do root, o qual é muito visado pelos crackers, pois é o único usuário que eles conhecem.

## **2.3 - Criando Chave do SSH para acessar sem senha**

Chaves do SSH fornecem uma maneira mais segura de fazer login em um servidor com SSH do que usando uma senha apenas. Enquanto uma senha pode eventualmente ser quebrada com um ataque de força bruta, chaves SSH são quase impossíveis de decifrar pela força bruta sozinha. Gerando um par de chaves cria-se duas longas sequências de caracteres: uma pública e uma privada. Você pode colocar a chave pública em qualquer servidor, e depois desbloqueá-lo conectando-se a ele com um cliente que já tem a chave privada. Quando os dois correspondem, o sistema abre, sem a necessidade de uma contra-senha. Você pode aumentar ainda mais a segurança, protegendo a chave privada com uma senha.

Criar o par de chaves no cliente (seu desktop)

```
cd  
ssh-keygen -t rsa  
Apenas tecele Enter 3 vezes.
```

Copiar a sua chave pública para o servidor.  
Temos duas alternativas:

```
ssh-copy-id "ribafs@21.129.54.123 -p 65522"
```

Agora tente logar normalmente do seu desktop para o servidor  
Acessará sem senha

```
ssh -p 65522 ribafs@21.129.54.123
```

Original:

<https://www.digitalocean.com/community/articles/how-to-set-up-ssh-keys--2>

Obs.:

Ao mudar a porta do SSH lembre de liberar no /etc/default/iptables e restartar o iptables.



## **2.4 - Mudar o fuso horário**

para um mais adequado para você.

Ex: America/Fortaleza.

```
dpkg-reconfigure tzdata
```

## **2.5 - Criar uma partição de swap no Ubuntu**

Especialmente para quem tem pouca memória RAM, como 512MB ou menos, o swap torna-se ainda mais importante. Ao ponto de alguns softwares nem chegarem a instalar/rodar. O swap não é a solução ideal para suprir RAM, mas ajuda com alguns softwares leves, como é o caso do iRedMail. Se for instalar algo mais pesado como o Zimbra o ideal é ter um servidor com pelo menos 3GB de RAM, idealmente com 4GB.

O iRedMail roda bem até com os 512MB mas com uma partição de swap.

```
dd if=/dev/zero of=/swapfile bs=1M count=2048
mkswap /swapfile
swapon /swapfile
```

Adicionar ao fstab  
sudo nano /etc/fstab

```
/swapfile swap swap defaults 0 0
```

Testar  
free -m

## **2.6 - Configurar locais**

```
locale-gen --no-purge --lang en_US.UTF-8 pt_BR.UTF-8 pt_BR
dpkg-reconfigure locales
update-locale
```

## **2.7 - Configurar hostname e hosts**

```
hostname - ribafs
nano /etc/hostname
```

```
/etc/hosts
```

O /etc/hosts precisa ter o formato:

```
IP      FQDN hostname (opcional)
```

FQDN = host.dominio. Exemplo: web.ribafs.net.br

IP principal: 21.129.54.123

Nele devo instalar o iRedMail, pois é onde fica o DNS reverso

```
21.129.54.124 ribafs.org ribafs
21.129.54.125 ssh.ribafs.net.br ribafs
21.129.54.126 tiagoarts.com ribafs
127.0.0.1 localhost.localdomain localhost
# Auto-generated hostname. Please do not remove this comment.
21.129.54.123 ribafs.net.br ribafs
::1          localhost ip6-localhost ip6-loopback
```

As 4 primeiras linhas e a última, por mais que mude, após o boot elas são refeitas.  
(os detalhes acima são para o serviço servermania)

## **2.8 - Instalar servidores de horário**

```
apt-get upgrade
```

```
apt-get install ntp ntpdate
```

```
#ntpdate -q ntp.ubuntu.com
```

```
mv /etc/ntp.conf /etc/ntp.confORIG
```

```
nano /etc/ntp.conf
```

Adicione o conteúdo abaixo:

```
# "memoria" para o escorregamento de frequencia do micro
# pode ser necessario criar esse arquivo manualmente com
# o comando touch ntp.drift
driftfile /etc/ntp.drift
```

```
# estatísticas do ntp que permitem verificar o histórico
# de funcionamento e gerar gráficos
statsdir /var/log/ntpstats/
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable
```

```
# servidores públicos do projeto ntp.br
server a.st1.ntp.br iburst
server b.st1.ntp.br iburst
server c.st1.ntp.br iburst
server d.st1.ntp.br iburst
server gps.ntp.br iburst
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
```

```
# outros servidores
# server outro-servidor.dominio.br iburst

# configurações de restrição de acesso
restrict default kod notrap nomodify nopeer
restrict -6 default kod notrap nomodify nopeer
```

Reinicie:

```
service ntp restart
```

Detalhes: <http://www.ntp.br/NTP/MenuNTPLinuxBSD>

## 2.9 - DNS

Configuração do DNS no painel administrativo da Hospedagem

Precisamos ir até a hospedagem e anotar os nameservers.

Com os nameservers ir até à administração do domínio e mudar os nameservers.

Voltando à hospedagem adicionar os registros no DNS (A, MX, CNAME, etc). Após uns 5 minutos poderemos ver os efeitos no intoDNS

<http://www.intodns.com/>

Caso a hospedagem não ofereça nameservers e opção para adicionar registros ao DNS, precisaremos usar este recurso na administração do domínio. Algumas empresas, como o Registro.br oferecem esta opção na interface web. Algumas não oferecem então precisamos contatar o suporte e enviar para eles o IP do nosso servidor e solicitar que criem os respectivos registros no DNS. Aqui também precisamos acompanhar com o intoDNS.

Se ele mostrar algum problema em algum registro, faça os ajustes ou peça ajuda ao suporte do domínio.

Quando o intoDNS mostrar tudo verdinho ou azul e no máximo algo amarelo, então devemos

testar bem com ferramentas como o dig e host:

```
dig dominio.com mx
dig dominio.com any
host dominio.com
```

## ***Migração do Domínio***

Sempre que mudar a administração de um domínio de uma empresa para outra ou mesmo quando alterar qualquer registro no DNS monitore a propagação do domínio que pode acontecer em minutos e pode demorar até 72 horas.

Quando ele me mostra todos os dados sem erro não significa que já propagou. Então eu começo a testar com o whois, dig, rout e nslookup pelo terminal:

```
whois ribafs.net.br
```

```
dig ribafs.net.br mx
```

```
dig +trace ribafs.net.br
```

```
dig ribafs.net.br any
```

```
host ribafs.net.br
```

```
host -t soa ribafs.net.br
```

Para saber o DNS reverso use:

```
nslookup 162.243.89.121
```

```
dig -t ptr 121.89.243.162.id-addr.arpadig -t ptr 121.89.243.162.id-addr.arpa
```

Testar um DNS server específico:

```
nslookup redhat.com ns1.redhat.com
```

Mudar o número da porta

```
nslookup -port 56 redhat.com
```

```
nslookup -debug redhat.com
```

**Cuidado:** estes testes devem ser feitos no seu desktop.

Caso faça no terminal do servidor o /etc/hosts irá mostrar tudo propagado, pois ele assume.

## DNS Reverso

Este DNS é muito importante para quem usa um servidor de e-mails, pois ele configurado corretamente passa confiança para o servidor que recebe seus e-mails.

O pessoal do DigitalOcean cria automaticamente um DNS reverso para cada droplet. Para que seu DNS reverso fique correto você precisa colocar o nome do seu domínio no nome da droplet, como hostname.

Assim, veja o meu:

```
ribafs.org
```

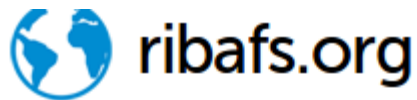


Create Droplet

| Image   | Name       | IP Address     | Status | Memory | Disk | Region |
|---|------------|----------------|--------|--------|------|--------|
|  | ribafs.org | 162.243.89.121 | Active | 512MB  | 20GB | nyc2   |

## Exemplo de DNS no DigitalOcean

Lembrar que este DNS que configuramos no Ocean é o DNS externo, apenas para conversar com a internet e não o interno, visto que não uso rede interna no VPS.

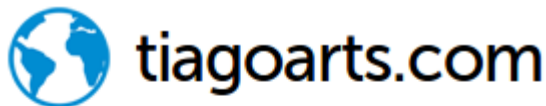


|       |                        |                    |
|-------|------------------------|--------------------|
| A     | @                      | 162.243.89.121     |
| A     | mail.ribafs.org.       | 162.243.89.121     |
| CNAME | www                    | ribafs.org.        |
| CNAME | refletindo.ribafs.org. | ribafs.org.        |
| CNAME | familia.ribafs.org.    | ribafs.org.        |
| MX    | 10 mail.ribafs.org.    |                    |
| TXT   | @                      | "v=spf1 a mx -all" |
| NS    | NS1.DIGITALOCEAN.COM.  |                    |
| NS    | NS2.DIGITALOCEAN.COM.  |                    |
| NS    | NS3.DIGITALOCEAN.COM.  |                    |

## Zone File

```
$TTL      1800
@         IN      SOA     NS1.DIGITALOCEAN.COM.  hostmaster.ribafs.org. (
        1385854267 ; last update: 2013-11-30 23:31:07 UTC
        3600 ; refresh
        900 ; retry
        1209600 ; expire
        1800 ; ttl
        )
         IN      NS      NS1.DIGITALOCEAN.COM.
         IN      NS      NS2.DIGITALOCEAN.COM.
         IN      NS      NS3.DIGITALOCEAN.COM.
         IN      MX      10      mail.ribafs.org.
@         IN      A      162.243.89.121
mail.ribafs.org.  IN      A      162.243.89.121
www       CNAME   ribafs.org.
@         TXT     "v=spf1 a mx -all"
refletindo.ribafs.org. CNAME  ribafs.org.
familia.ribafs.org.   CNAME  ribafs.org.
```

## Segundo Domínio Adicionado



|       |                        |                    |
|-------|------------------------|--------------------|
| A     | @                      | 162.243.89.121     |
| A     | mail.tiagoarts.com.    | 162.243.89.121     |
| CNAME | *                      | @                  |
| MX    | 10 mail.tiagoarts.com. |                    |
| TXT   | @                      | "v=spf1 a mx -all" |
| NS    | NS1.DIGITALOCEAN.COM.  |                    |
| NS    | NS2.DIGITALOCEAN.COM.  |                    |
| NS    | NS3.DIGITALOCEAN.COM.  |                    |

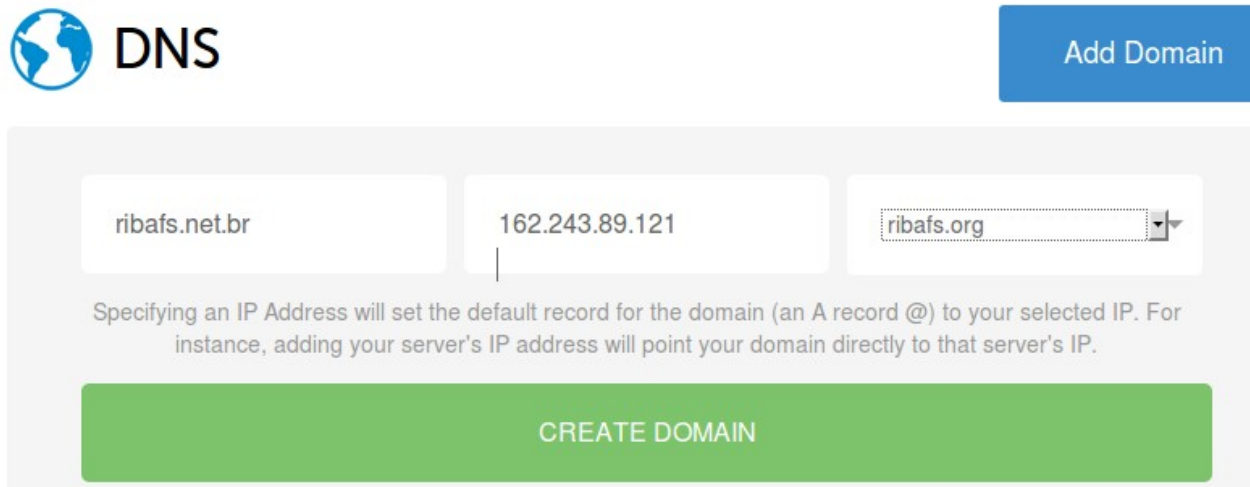
## Adicionando um Terceiro Domínio à mesma droplet


Efetuar login no painel

Clicar em DNS

Clicar em Add Domain acima

Preencher assim:



 **DNS** [Add Domain](#)

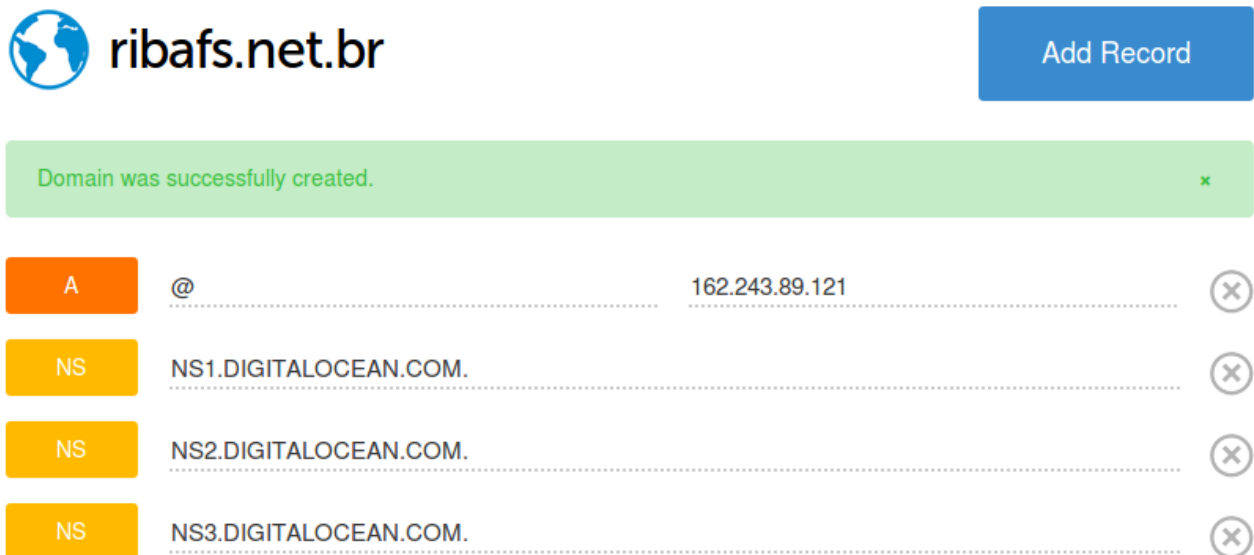
ribafs.net.br | 162.243.89.121 | ribafs.org


Specifying an IP Address will set the default record for the domain (an A record @) to your selected IP. For instance, adding your server's IP address will point your domain directly to that server's IP.

[CREATE DOMAIN](#)





Clicar abaixo em CREATE DOMAIN

Veja que ele já cria estes registros abaixo:



 **ribafs.net.br** [Add Record](#)

Domain was successfully created.

|    |                       |                |   |
|----|-----------------------|----------------|---|
| A  | @                     | 162.243.89.121 |  |
| NS | NS1.DIGITALOCEAN.COM. |                |  |
| NS | NS2.DIGITALOCEAN.COM. |                |  |
| NS | NS3.DIGITALOCEAN.COM. |                |  |

Zone File - DNS is propagating.

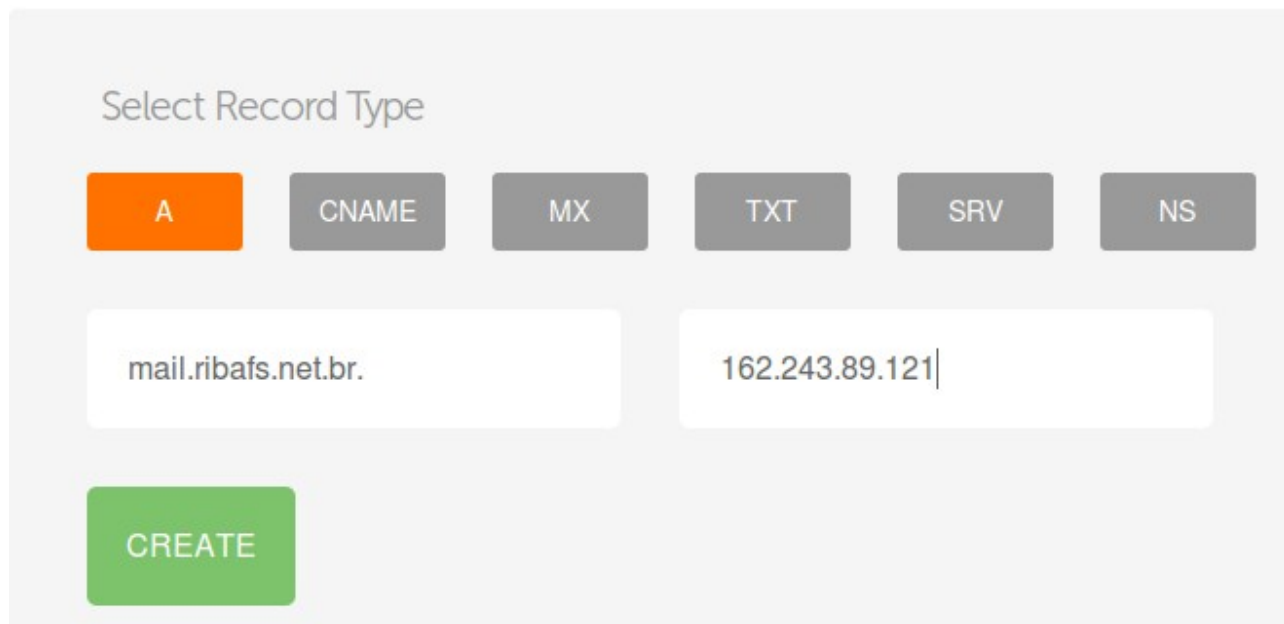
Precisaremos adicionar os demais que precisarmos:

Adicionaremos os registros A, CNAME, MX e um TXT

Adicionar um registro A para o e-mail:

Clique em Add Record

Agora clique no A e preencha como abaixo:



Select Record Type

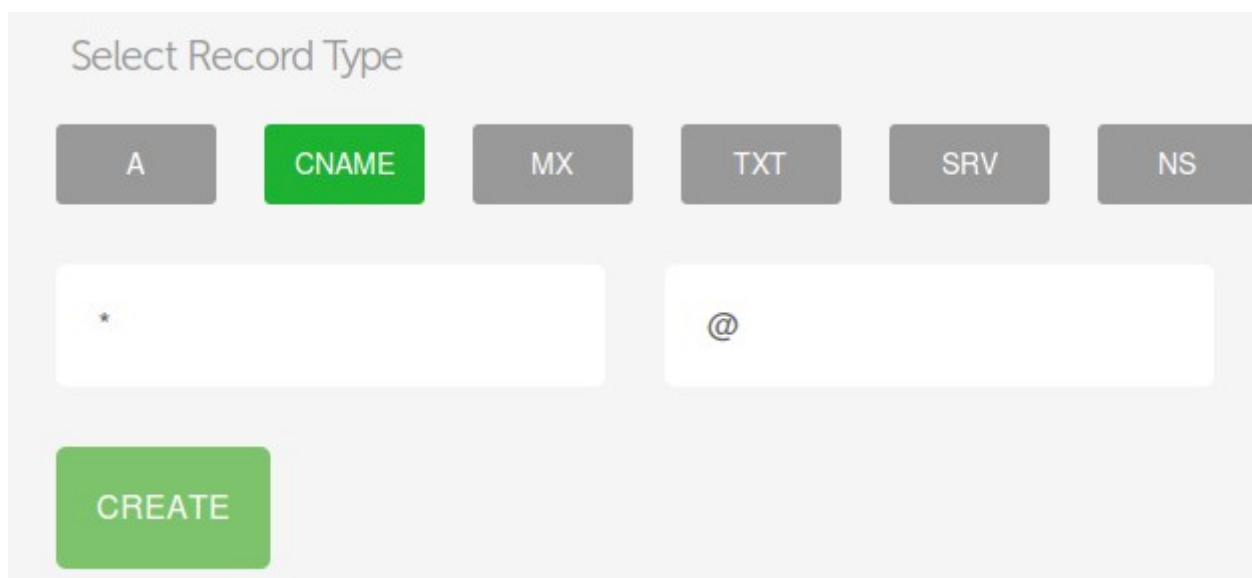
**A** CNAME MX TXT SRV NS

mail.ribafs.net.br. 162.243.89.121|

CREATE

Então clique em CREATE

Agora vamos criar o registro CNAME de forma semelhante, para que fique assim:



Select Record Type

A **CNAME** MX TXT SRV NS

\* @

CREATE

No meu domínio principal eu tive alguns problemas que creditei ao CNAME e mudei para:



CNAME www ..... ribafs.org. (X)



Agora vamos adicionar o registro MX assim:

Select Record Type

A CNAME **MX** TXT SRV NS


mail.ribafs.net.br. 10

CREATE ADD GMAIL MX RECORDS

Adicione o TXT assim:

TXT @ "v=spf1 mx mx:mail.ribafs.net.br -all"

Nosso DNS ficará assim:

 **ribafs.net.br** Add Record

|       |                        |  |   |
|-------|------------------------|--|---|
| A     | @                      | 162.243.89.121                         | ⊗ |
| A     | mail.ribafs.net.br.    | 162.243.89.121                         | ⊗ |
| CNAME | *                      | @                                      | ⊗ |
| MX    | 10 mail.ribafs.net.br. |  | ⊗ |
| TXT   | @                      | "v=spf1 mx mx:mail.ribafs.net.br -all" | ⊗ |
| NS    | NS1.DIGITALOCEAN.COM.  |  | ⊗ |
| NS    | NS2.DIGITALOCEAN.COM.  |  | ⊗ |
| NS    | NS3.DIGITALOCEAN.COM.  |  | ⊗ |

Veja que abaixo ele mostra os comandos em modo texto na Zone File.

Após estes ajustes e o registro no registro.br ou em outra administração, uma consulta no intodns já mostra nosso domínio bonitinho, mesmo que o dig ainda não acuse:

<http://www.intodns.com/ribafs.net.br>

## Veja meus DNSs no Servidor



Add Domain



ribafs.net.br




ribafs.org



tiagoarts.com



To update your PTR record please update your Droplet's hostname through the control panel.

| IP Address     | PTR Record  | View  |
|----------------|-------------|---|
| 162.243.89.121 | ribafs.org. |  |

Os 3 estão usando um mesmo servidor, uma mesma droplet no Ocean.

## Exemplo de DNS no registro.br

<http://registro.br>

Faça o login

Clique no domínio abaixo de Administrativo

Clique em Utilizar os servidores DNS do Registro.br

**DNS**  
É obrigatória a delegação dos servidores Master e Slave 1

Utilizar os servidores DNS do Registro.br [Mais informações](#)

**SALVAR & EDITAR DNS**

**SALVAR** **LIMPAR**

Clique em Salvar & Editar DNS

Clicar em Modo Avançado abaixo

**Records da Zona - ribafs.net.br**

Endereço do site:

Endereço do servidor de email:

**SALVAR** **AJUDA** **MODO AVANÇADO**

**Records da Zona - ribafs.net.br**

Nenhum record cadastrado

**+ RECORD** **SALVAR** **AJUDA** **MODO BASICO**

Clique em + RECORD e adicione o primeiro registro, registro A.  
Repita para os demais registros.

E adicione os registro abaixo, alterando o IP.

Veja um exemplo de tela para o registro A, com a Ajuda:




| Records da Zona - ribafs.net.br |  |   |  |
|---------------------------------|--|---|--|
|                                 | Nome   | Tipo                                    | Dados  |
| x                               | <input type="text" value=""/> .ribafs.net.br | A                                       | <input type="text" value="162.243.89.121"/>                                |
|                                 |  | <input type="button" value="+ RECORD"/> | <input type="button" value="SALVAR"/> <input type="button" value="AJUDA"/> |

Os dados associados com o domínio ficam armazenados em resource records (registros de recursos). Os tipo de records suportados pelo sistemas são:

- **A** - Representa um endereço IPv4. Exemplo:  
*meudominio.com.br A 200.160.10.251*
- **AAAA** - Representa um endereço IPv6. Exemplo:  
*meudominio.com.br AAAA 2001:12ff:0:2::3*
- **CNAME** - Indica um nome alternativo. Exemplo:  
*www.meudominio.com.br CNAME meublog.example.com.*
- **MX** - Representa um nome para um servidor de email. Exemplo:  
*meudominio.com.br MX mail-server.example.com.*
- **TXT** - Informações de texto livre

Após preencher os dados clique em SALVAR

Clique novamente em SALVAR & EDITAR DNS  
Proceda de forma semelhante para adicionar os demais registros.  
Adicione outros se achar por bem.

| Records da Zona - ribafs.net.br |                    |   |  |
|---------------------------------|--------------------|---|--|
|                                 | Nome               | Tipo                                    | Dados  |
| x                               | ribafs.net.br      | A                                       | 162.243.89.121  |
| x                               | ribafs.net.br      | MX                                      | 10 mail.ribafs.net.br  |
| x                               | ribafs.net.br      | TXT                                     | "v=spf1 a mx -all"   |
| x                               | mail.ribafs.net.br | A                                       | 162.243.89.121  |
| x                               | www.ribafs.net.br  | CNAME                                   | ribafs.net.br.  |
|                                 |                    | <input type="button" value="+ RECORD"/> | <input type="button" value="SALVAR"/> <input type="button" value="AJUDA"/>                           |

Os dados associados com o domínio ficam armazenados em resource records (registros de recursos). Os tipo de records suportados pelo sistemas são:

- **A** - Representa um endereço IPv4. Exemplo:  
*meudominio.com.br A 200.160.10.251*
- **AAAA** - Representa um endereço IPv6. Exemplo:  
*meudominio.com.br AAAA 2001:12ff:0:2::3*
- **CNAME** - Indica um nome alternativo. Exemplo:  
*www.meudominio.com.br CNAME meublog.example.com.*
- **MX** - Representa um nome para um servidor de email. Exemplo:  
*meudominio.com.br MX mail-server.example.com.*
- **TXT** - Informações de texto livre

Aguardar que o domínio propague.

Para ficar testando, pode abrir um arquivo no /var/www, ou pode executar no terminal:




dig ribafs.net.br mx

host ribafs.net.br

Uma ótima alternativa web:

<http://www.intodns.com/>

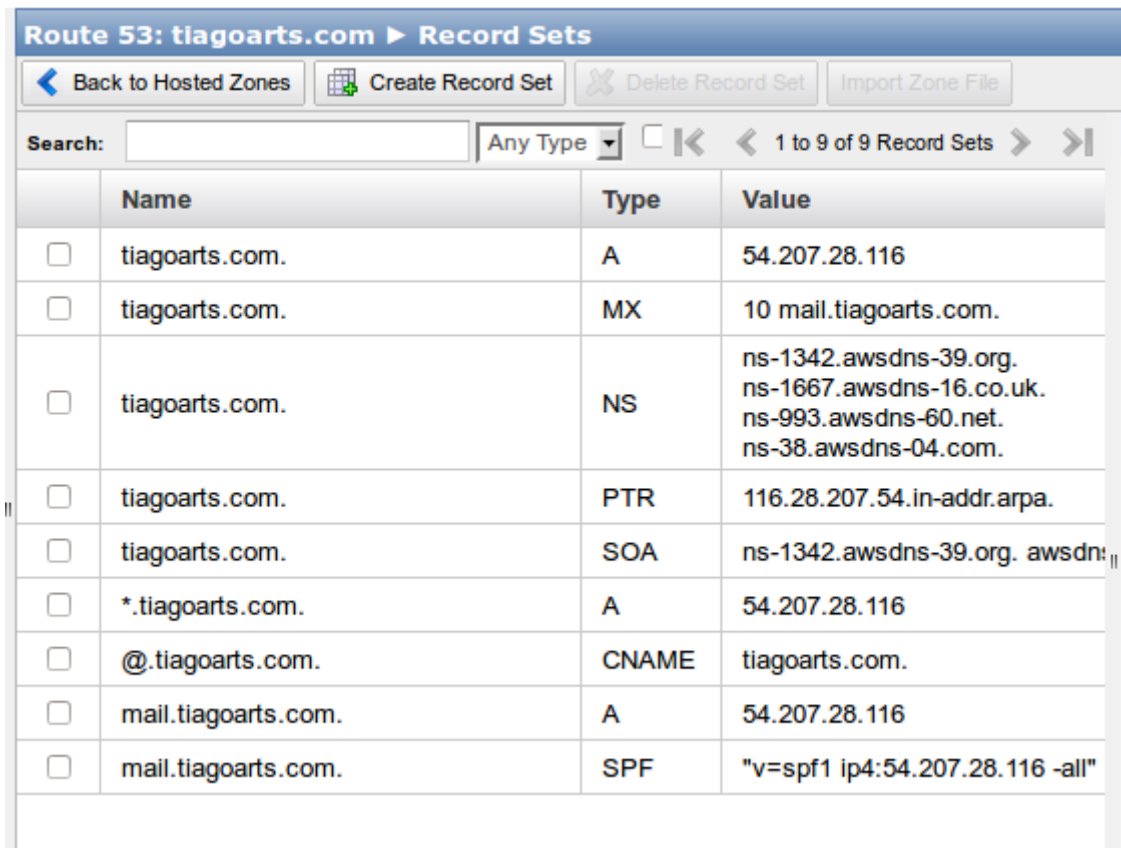
Quando usei outro IP para o e-mail (Servermania)

| Records da Zona - ribafs.net.br |                    |       |   |
|---------------------------------|--------------------|-------|---|
|                                 | Nome               | Tipo  | Dados   |
| ✘                               | ribafs.net.br      | A     | 23.229.54.124  |
| ✘                               | ribafs.net.br      | MX    | 10 mail.ribafs.net.br.  |
| ✘                               | ribafs.net.br      | TXT   | "v=spf1 a mx -all"  |
| ✘                               | mail.ribafs.net.br | A     | 23.229.54.123  |
| ✘                               | www.ribafs.net.br  | CNAME | ribafs.net.br  |

[+ RECORD](#) [SALVAR](#) [AJUDA](#)

## Exemplo de DNS no Amazon AWS

No AWS usamos a ferramenta Route 53 para adicionar um domínio



The screenshot shows the AWS Route 53 console for the domain 'tiagoarts.com'. The interface includes navigation buttons like 'Back to Hosted Zones', 'Create Record Set', 'Delete Record Set', and 'Import Zone File'. A search bar and a dropdown menu for 'Any Type' are visible. Below, a table lists 9 DNS records with columns for Name, Type, and Value.

|                          | Name                | Type  | Value   |
|--------------------------|---------------------|-------|---|
| <input type="checkbox"/> | tiagoarts.com.      | A     | 54.207.28.116   |
| <input type="checkbox"/> | tiagoarts.com.      | MX    | 10 mail.tiagoarts.com.  |
| <input type="checkbox"/> | tiagoarts.com.      | NS    | ns-1342.awsdns-39.org.<br>ns-1667.awsdns-16.co.uk.<br>ns-993.awsdns-60.net.<br>ns-38.awsdns-04.com. |
| <input type="checkbox"/> | tiagoarts.com.      | PTR   | 116.28.207.54.in-addr.arpa.   |
| <input type="checkbox"/> | tiagoarts.com.      | SOA   | ns-1342.awsdns-39.org. awsdns-  |
| <input type="checkbox"/> | *.tiagoarts.com.    | A     | 54.207.28.116   |
| <input type="checkbox"/> | @.tiagoarts.com.    | CNAME | tiagoarts.com.  |
| <input type="checkbox"/> | mail.tiagoarts.com. | A     | 54.207.28.116   |
| <input type="checkbox"/> | mail.tiagoarts.com. | SPF   | "v=spf1 ip4:54.207.28.116 -all"   |

### Configuração DNS para SPF

```
iredmail.org.      3600  IN   TXT   "v=spf1 mx mx:mail.iredmail.org -all"  
ou  
iredmail.org.      3600  IN   TXT   "v=spf1 ip4:202.96.134.133 -all"  
  
TXT               ribafs.org        "v=spf1 ip4:202.96.134.133 ~all"
```

### Implementando DKIM com o opendkim

**LEMBRANDO:** quando usamos o iRedMail não precisamos fazer o seguinte, pois o iRedMail já traz este recurso ativo, veja o item 3.2.

Uma solução para reduzir spams. Criado pela Cisco e Yahoo.

Uma alternativa open é o OpenDKIM.

Instalação

```
apt-get install opendkim
```

Criação das chaves e do registro DKIM no DNS  
Antes de configurar precisamos criar o registro no DNS

```
mkdir /etc/certs-opendkim  
cd /etc/certs-opendkim
```

```
openssl genrsa -out private.key 1024  
chmod 600 private.key
```

```
openssl rsa -in private.key -out public.key -pubout -outform PEM
```

Já temos a chave:

```
cat public.key
```

Com ela vamos atualizar nossa chave no DNS

Configuração:  
nano /etc/opendkim.conf

Descomentar e alterar as linhas:

```
Domain          ribafs.org  
Selector        2013  
ATPSDomains     ribafs.org
```

```
touch /etc/mail/dkim.key  
chmod 600 /etc/mail/dkim.key
```

Gerar chave para assinar

```
opendkim-genkey -D /etc/mail/ -d ribafs.org -s default  
mkdir /etc/mail/ribafs.org  
opendkim-genkey -D /etc/mail/ribafs.org/ -d ribafs.org -s default  
opendkim-genkey -D /etc/mail/ -d ribafs.org -s default
```

```
chown -R opendkim:opendkim /etc/mail/ribafs.org  
mv /etc/mail/ribafs.org/default.private /etc/mail/ribafs.org/default
```

Arquivos de configuração:

- /etc/opendkim.conf – OpenDKIM’s main configuration file
- /etc/opendkim/KeyTable – a list of keys available for signing
- /etc/opendkim/SigningTable - a list of domains and accounts allowed to sign
- /etc/opendkim/TrustedHosts – a list of servers to “trust” when signing or verifying

Criar os 3 arquivos, contendo cada um:

```
nano /etc/mail/KeyTable  
default._domainkey.ribafs.org ribafs.org:default:/etc/mail/ribafs.org/default
```

```
nano /etc/mail/SigningTable  
*@ribafs.org default._domainkey.ribafs.org
```

```
nano /etc/mail/TrustedHosts
127.0.0.1
refletindo.ribafs.org
familia.ribafs.org
ribafs.org
```

```
nano /etc/postfix/main.cf
```

Adicionar ao final:

```
smtpd_milters      = inet:127.0.0.1:8891
non_smtpd_milters  = $smtpd_milters
milter_default_action = accept
```

```
/etc/init.d/openssl stop
/etc/init.d/openssl start
```

```
/etc/init.d/postfix restart
```

Testando

```
tail -f /var/log/mail.log
dig ribafs.org TXT default._domainkey.ribafs.org
```

```
apt-get install openssl
openssl testkey -d ribafs.org -s mail -k /etc/mail/dkim.key
```

Gerar chave

```
openssl genkey -t -s mail -d ribafs.org
```

```
cd /etc/certs-openssl
cat public.key
```

```
cat private.key
```

Criar um registro do tipo TXT, contendo:

```
mail._domainkey.ribafs.org "k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQD1ghVw8YuUGFbjMyTvNHkj3dUK
ng1e2cZFgVY+y03sSxvmVln8snZAa7/mlapwP596gH7DGZcGGNww4SFIY62hP6R0
EqrlYH+f7jbgMigd+KDC7yoOZG814UY+GoCGL3mfjSdRWtNOgrq/dpTkMcFNnW5
SqTgopmRI0ZlagMMNwIDAQAB"
```

Fonte:

<http://www.pedropereira.net/instalar-configurar-openssl-postfix/>

### Informações sobre DNS

Domínio - termo usado somente quando um servidor é dedicado a um número de IP e a um domínio.

Domínio virtual - quando muitos nomes de domínios compartilham o mesmo IP.



terciário (tlt) - www  
secundário (tls) - ribafs.org  
superior (tls) - org  
raiz (.) . (opcional)

tlt.tls.tld.

FQDN - hostname.dominio

Exemplo:  
www.ribafs.org

## **Limpar o cache do DNS**

### ***Limpar cache DNS no Windows***

Abra o terminal(Aperte Ctr+R e em executar digite cmd).

Digite ipconfig /flushdns

Mostrará uma mensagem que o cache foi limpo.

### ***Limpar cache DNS no Linux***

Abra o terminal, nem preciso dar atalho né?

Digite o seguinte comando

sudo aptitude install nscd

/etc/init.d/nscd restart

### ***Limpar cache DNS no Mac OS***

No Mac OS, abra o terminal, procure por ele no Spotlight e digite:

sudo dscacheutil -flushcache

Digite sua senha e o cache será limpo

### ***Limpar o cache do Firefox***

Editar - Preferências - Avançado - Rede - Cache de conteúdo web - Limpar agora

## **Hostname**

O DigitalOcean cria automaticamente um DNS reverso partindo do nosso hostname ao criarmos a droplet.

hostname - é um nome para a máquina, pode ser qualquer um, web, www, mail, joao ou o domínio.

Para que o DNS reverso seja criado corretamente, devemos colocar o nome do domínio no hostname.

Exemplo:  
Hostname - tiagoarts.com

## Registros do DNS

```
A      ribafs.net.br.          162.243.89.121
A      mail.ribafs.net.br.    162.243.89.121
CNAME  www  ribafs.net.br.
MX     0      mail.ribafs.net.br.
TXT    ...
```

Quando temos apenas um domínio de e-mail, usar 0 na prioridade para evitar problemas com o domínio web.

Quando temos vários domínios ou subdomínios para o e-mail, devemos usar números de prioridade diferentes, com as devidas prioridades. Exemplo 10 e 20:

```
MX     10     mail1.ribafs.net.br.
MX     20     mail2.ribafs.net.br.
```

## Registros

MX - identificar o local de entrega de um e-mail para determinado endereço.

Cada host definido em um registro MX deve ter um registro correspondente do tipo A em uma zona válida

A - são os registros centrais do DNS. Vinculam um domínio ou subdomínio a um IP  
Um registro A pode estar ligado a vários IPs.

CNAME - são aliases de registros A. Para cada registro CNAME você pode selecionar um alias e um host

Ele aponta um registro A para um subdomínio

Não é bom utilizar registros CNAME pois conflitam com os registros TXT e SPF.

Temos um host - serv1.abc.com.br

Criamos um CNAME www para o host serv1.abc.com.br, então ao acessar:

www.abc.com.br estamos acessando serv1.abc.com.br

Evite registrar cada subdomínio.

TXT - Refere-se a TeXT, o qual permite incluir um texto curto em um hostname. Técnica usada para implementar o SPF.

SPF - ajuda a melhorar a reputação do servidor de e-mail, assim como o DKIM

```
TXT @ "v=spf1 mx a ip4:162.243.89.121 ~all"
```

```
TXT @ "v=spf1 a include:ribafs.net.br ~all"
```

```
"v=spf1 ip4:192.168.0.1/16 -all"
```

```
"v=spf1 include:ribafs.net.br -all"
```

```
"v=spf1 mx mx:ribafs.net.br -all"
```

```
"v=spf1" "ip4:ribafs.net.br" "-all"
```

```
v=spf1 include:ribafs.net.br
```

```
v=spf1 include:_spf.google.com ~all
```

```
v=spf1 a mx ip4:192.0.2.32/27 -all
```

\* define um domínio coringa. qualquercoisa.dominio.com.br irá responder com ip 201.20.45.23!

Curingas do DNS representam um perigo claro e significativo à segurança e estabilidade do Sistema de Nomes de Domínio, portando devemos evitar seu uso.

@ antes do MX significa todos os servidores de e-mail

TXT "v=spf1 ip4:162.243.89.121 -all"  
SPF (Sender Policy Framework)

### **Exemplo na Amazon:**

SPF ribafs.net.br "v=spf1 ip4:54.207.0.57 -all"

Caso queira receber os e-mails em um subdomínio basta apontar o raiz para (@) registro MX para o subdomínio e criar um registro tipo A para o subdomínio do IP

@ IN MX mail.ribafs.net.br  
mail IN A 162.243.95.30

Para instalar o servidor de e-mail adicione um registro A e um MX ao DNS:

mail 162.40.24.30 A 1800  
mail 162.40.24.30 MX 10

bar.example.com. CNAME foo.example.com.  
foo.example.com. A 192.0.2.23

### **DNS Reverso**

Resolve um endereço IP para um nome de serviço e adiciona ".in-addr.arpa" ao final.

O nslookup está desatualizado e ferramentas como host e dig devem ser preferidas.

Exemplo:

ribafs.net.br. 57.0.207.54.in-addr.arpa. PTR

### **Propagação**

Qualquer alteração do DNS precisa aguardar a propagação (atualização).

A propagação depende de vários fatores:

- o registro precisa ser atualizado em cada um dos name servers autoritativos;
  - os resolvers também precisam colocar em cache as perguntas;
  - também precisa esperar o TTL (time to live) da configuração do DNS
- Isso pode levar de 30 minutos até 72 horas.

### **Servidores de DNS Públicos**

Um dos servidores DNS públicos mais utilizados é o Open DNS e apesar de algumas pessoas não gostarem do mesmo por fazer uso de um motor de busca alternativo provavelmente ele é a melhor alternativa.

1. Open DNS: 208.67.222.222 e 208.67.220.220.
2. DNS Resolvers: 205.210.42.205 e 64.68.200.200.
3. DNS Advantage: 156.154.70.1 e 156.154.71.1.
4. Giga DNS (brasileiro): 189.38.95.95 e 189.38.95.96.



## 3.0 - Instalação do iRedMail

O roteiro abaixo indica 0.8.5, mas hoje já existe a versão 0.8.6.

Caso tenha um servidor rodando iRedMail precisa fazer alguns backups exportando os bancos:

vmail

roundcubemail

livro de endereços do Roundcube

Tudo antes de de reinstalar o servidor e guardar no desktop ou noutra servidor.

Exportar livro de endereços do Gmail para ser importado no RoundCube

Quem usa o e-mail do Gmail tem um grande livro de endereços, contendo todos os e-mails de quem enviou para você e dos que você enviou.

Estes e-mails podem ser úteis se for usar o RoundCube, pois ele também completa os e-mails quando vamos criar um e-mail.

Para exportar o Livro no Gmail

-Abra o Gmail

-Acima e à esquerda clique na combo Gmail – Depois clique em Contatos

-Clique acima na combo Mais – Depois em Exportar...

-Selecione o formato vCard e clique em Exportar

Importar no WebMmail RoundCube

-Abra seu webmail no Roundcube

-Clique acima e à direita em Catálogo de Endereços

-Clique em Importar

-Clique em Selecionar arquivo e Selecione o arquivo exportado do Gmail

-Clique em Importar e aguarde

Agora quando criar um novo e-mail, ao iniciar a digitação no campo Para, ele irá auto-completando para você.

```
apt-get update
```

```
apt-get upgrade
```

```
apt-get install mc nmap unzip
```

```
reboot
```

```
cd /root/
```

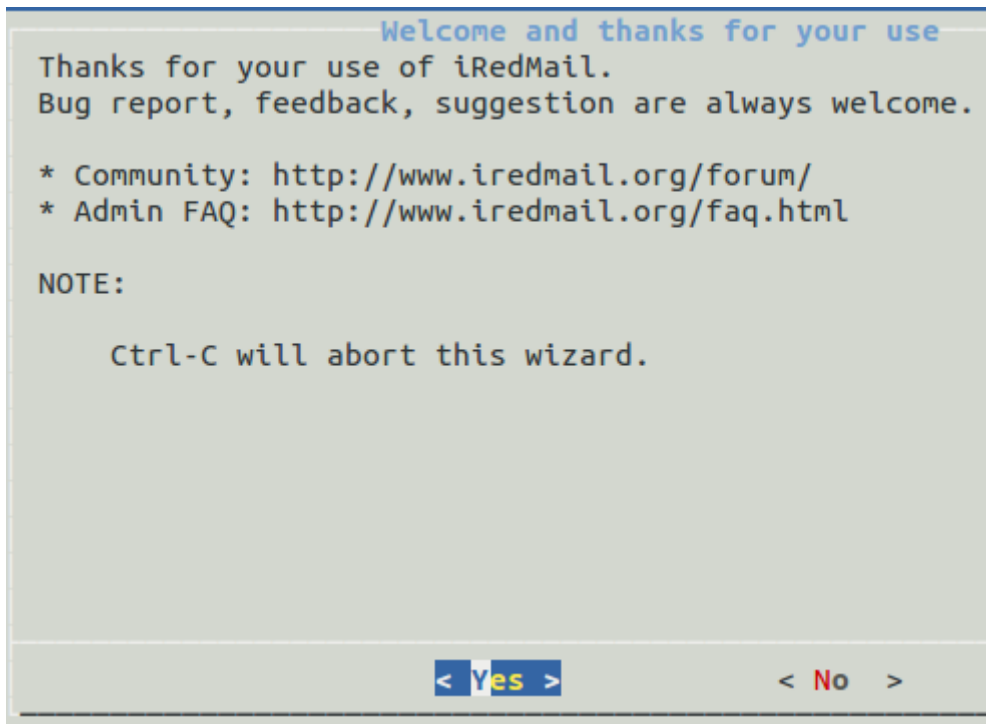
```
wget https://bitbucket.org/zhb/iredmail/downloads/iRedMail-0.8.6.tar.bz2
```

```
tar xjf iRedMail-0.8.6.tar.bz2
```

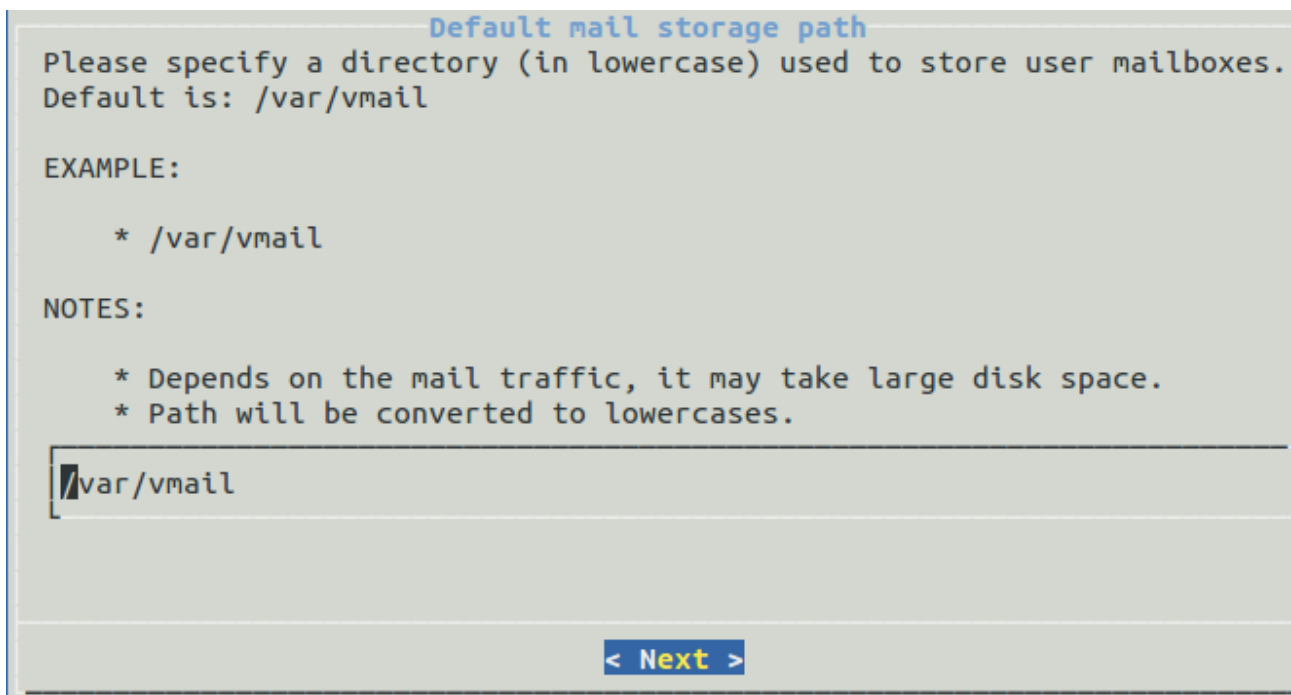
```
cd iRedMail-0.8.6
```

```
bash iRedMail.sh
```

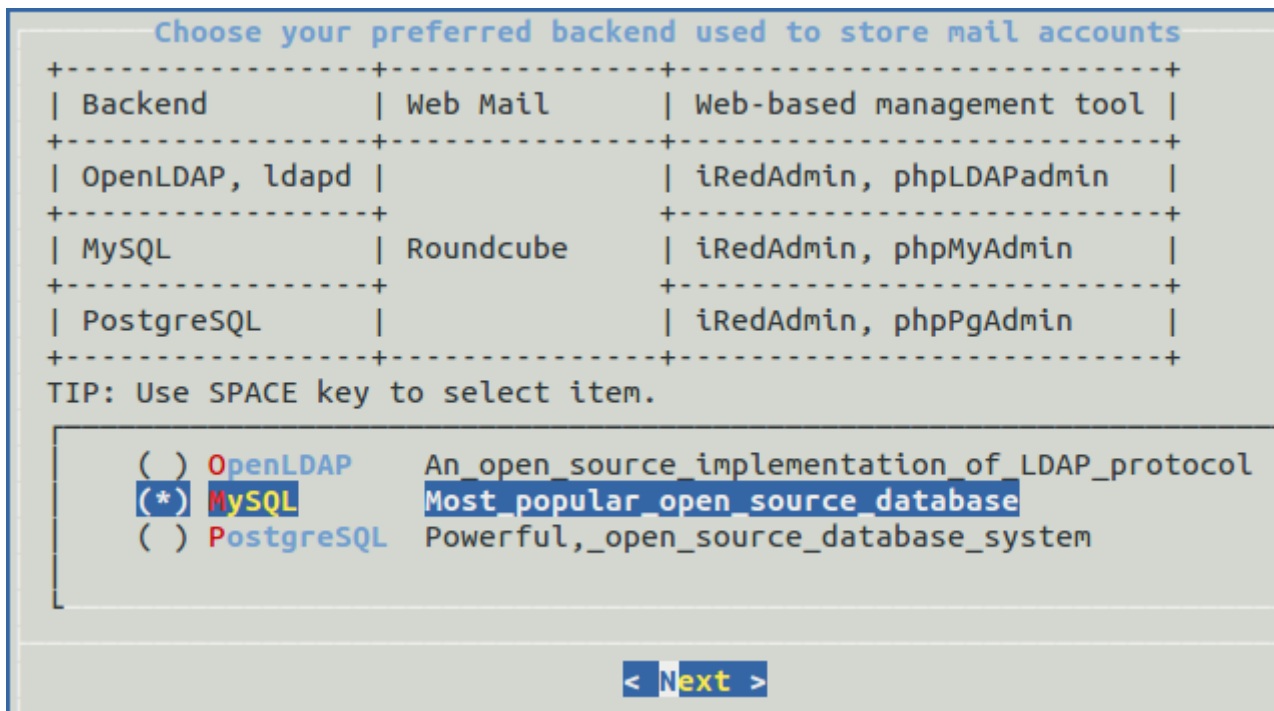
Aguarde...



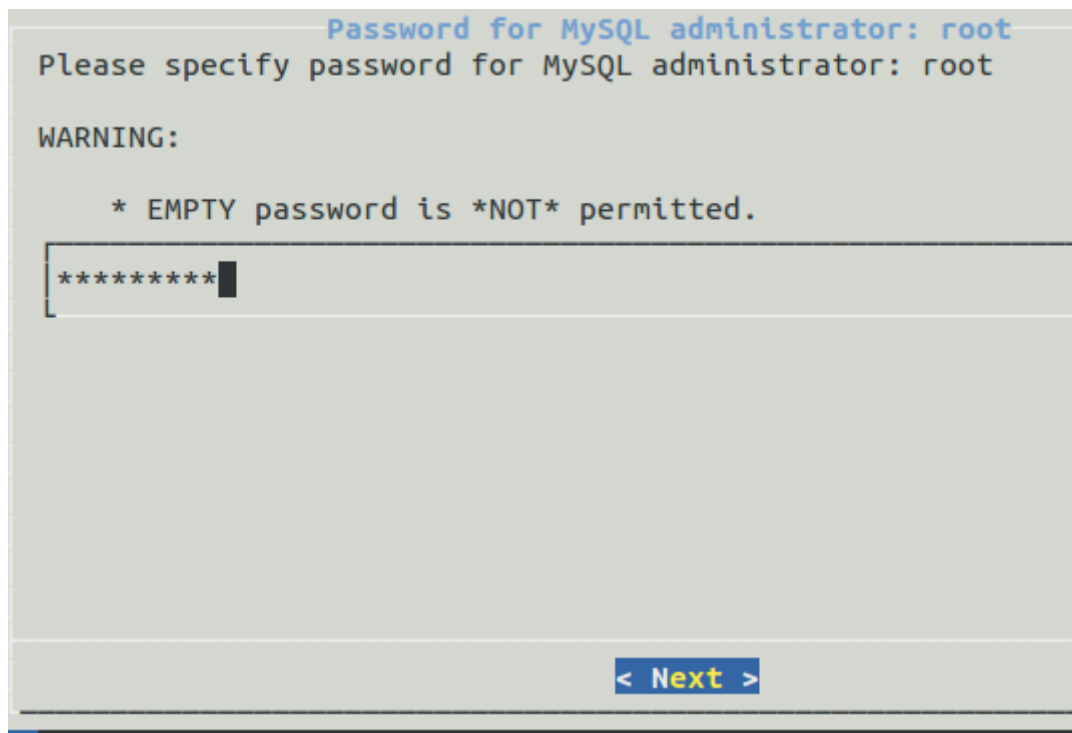
Apenas tecle Enter para confirmar a continuação



Apenas enter novamente



Mova com as setas para cima e para baixo para selecionar o SGBD e tecle enter para continuar.



Entre com a senha para o root do MySQL e enter.

**Your first virtual domain name**

Please specify your first virtual domain name.

EXAMPLE:

- \* example.com

WARNING:

- \* It cannot be the same as server hostname: webriba.ribafs.local.

[< Next >](#)

Digite o nome do domínio e tecle enter.

No meu caso no servidor, apareceu mail.ribafs.org e eu digitei na caixa:  
ribafs.org

E enter.

**Password for the administrator of your domain**

Please specify password for the administrator user:

- \* postmaster@ribafs.local

Note:

- \* You can login to both webmail and iRedAdmin with this account.
- \* Please reset password immediately after installation completed.

WARNING:

- \* EMPTY password is \*NOT\* permitted.

[< Next >](#)

Entre com a senha para o usuário [postmaster@ribafs.local](mailto:postmaster@ribafs.local), que será o administrador do iredadmin e tecle Enter.



```
Optional components

Note:
* DKIM is recommended.
* SPF validation (Sender Policy Framework) is enabled by default.
* DNS records (TXT type) are required for both SPF and DKIM.
* Refer to file for more detail after installation:
  /home/ribafs/iRedMail-0.8.5/iRedMail.tips

[*] DKIM signing/verification   DomainKeys Identified Mail
[*] iRedAdmin                   Official web-based Admin Panel
[*] Roundcubemail               WebMail program (PHP, AJAX)
[*] phpMyAdmin                  Web-based MySQL management tool
[*] Awstats                     Advanced web and mail log analyzer
[*] Fail2ban                    Ban IP with too many password failures

< Next >
```

Veja os bons recursos opcionais e adicionais.

Tecele enter.

```
Configuration completed.
*****
***** WARNING *****
*****
*
* Below file contains sensitive infomation (username/password), please
* do remember to *MOVE* it to a safe place after installation.
*
*   * /home/ribafs/iRedMail-0.8.5/config
*
*****
< Question > Continue? [y|N]
```

y  
E Enter  
Aguarde...

Se aparecer esta mensagem

```
< Question > Would you like to *REMOVE* sendmail now? [Y|n]
```

Apenas tecele Enter para confirmar.

### Firewall

```
< Question > Would you like to use firewall rules provided by iRedMail now?
< Question > File: /etc/default/iptables, with SSHD port: 22. [Y|n]
```

É importante usar o firewall que acompanha o iRedMail, caso contrário teremos que configurar manualmente, liberando portas e redirecionando.  
Apenas tecele enter para confirmar as duas perguntas.

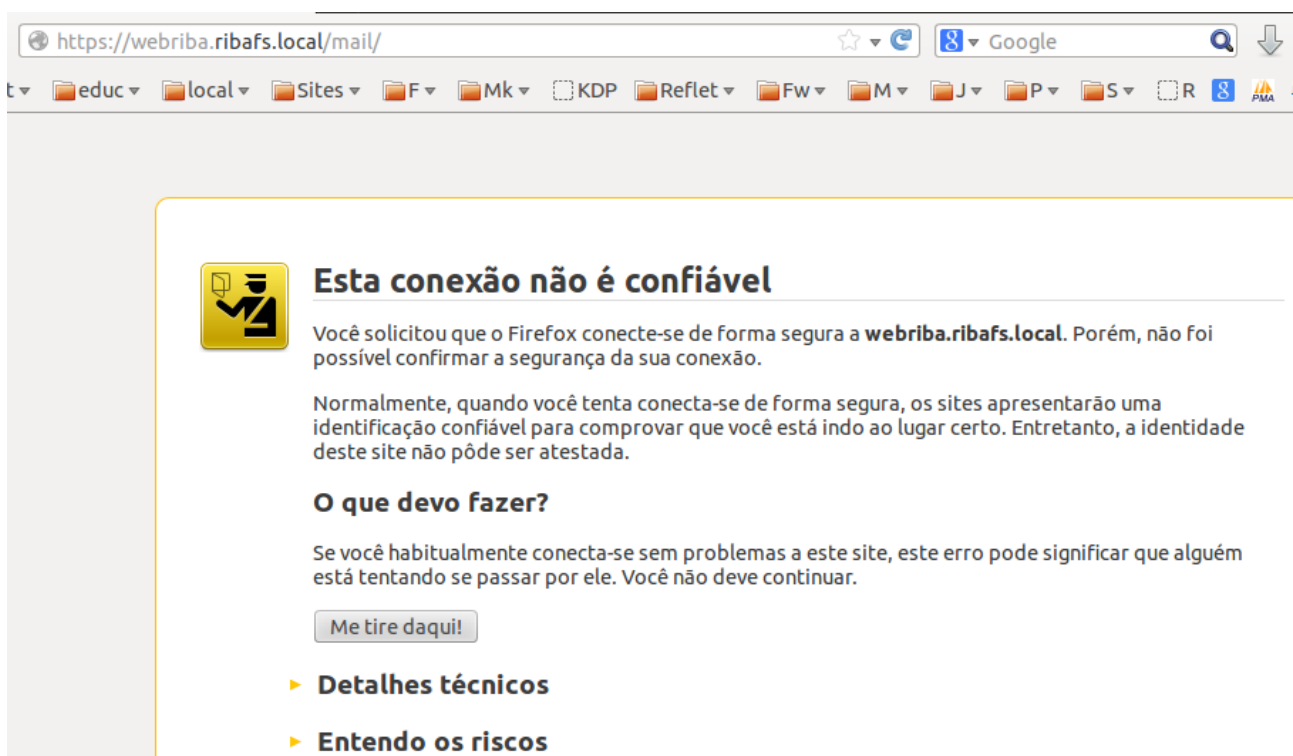
## Conclusão.

```
*****
* URLs of installed web applications:
*
* - Webmail: https://webriba.ribafs.local/mail/
* - Admin Panel (iRedAdmin): https://webriba.ribafs.local/iredadmin/
*   + Username: postmaster@ribafs.local, Password: zmxn1029r
*
*****
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
* - /home/ribafs/iRedMail-0.8.5/iRedMail.tips
*
* And it's sent to your mail account postmaster@ribafs.local.
*
* Please reboot your system to enable mail services.
*
*****
ribafs@webriba:~/iRedMail-0.8.5$
```

Veja acima o link do webmail e do iredadmin, assim como usuário e senha.  
Execute um reboot  
reboot

## Acessando o Roundcube Webmail

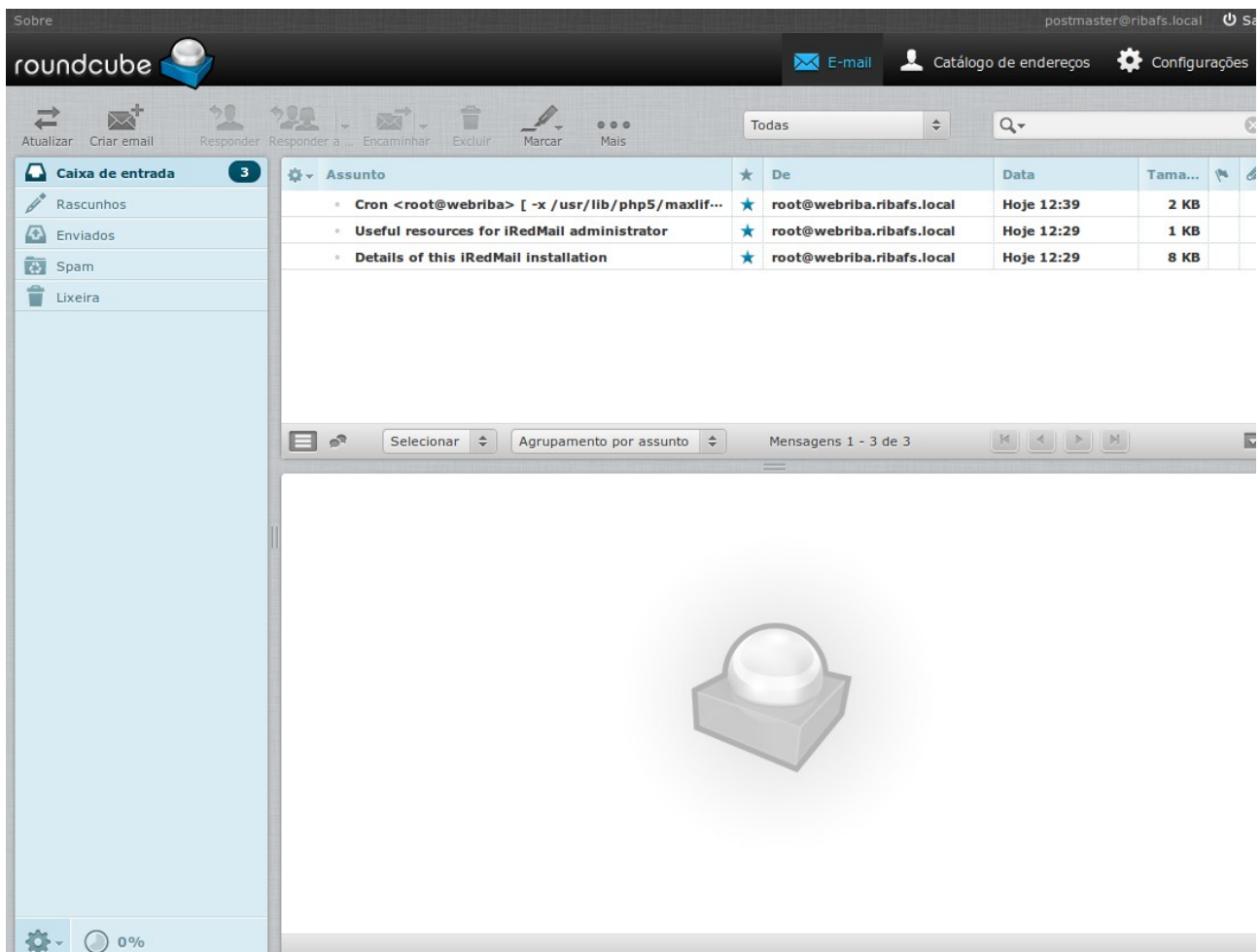
No servidor meu endereço ficou assim: <https://ribafs.org/mail>



Aceite o registro clicando em Entendo os Riscos  
Então clique em Adicionar Exceção  
Confirmar Exceção de Segurança



Veja o Roundcube:



Abra a primeira mensagem do root com Subject Cron...

Veja o conteúdo:

```
PHP Deprecated: Comments starting with '#' are deprecated in
/etc/php5/cli/conf.d/ming.ini on line 1 in Unknown on line 0
```

O que indica que precisamos resolver isso para evitar estas mensagens.

Edite o arquivo:

```
nano /etc/php5/cli/conf.d/ming.ini
```

Na linha 1 mude o # por // e salve.

Pronto. Agora não mais esta mensagem será enviada pelo cron.

## **Desinstalação**

Nunca fui bem sucedido na desinstalação do iRedMail, sempre precisei instalar tudo novamente, desde o sistema operacional. Por isso também é importante instalar logo no início, para não perder muito tempo em caso de instalar tudo novamente.

Caso siga com cuidado os cuidados iniciais na criação do swap, na configuração do hostname e do /etc/hosts geralmente instala e funciona bonitinho.

Mas se quiser experimentar o script de desinstalação:

<http://www.iredmail.org/forum/topic333-iredmail-support-faq-how-to-uninstall-iredmail.html>

## **Dicas sobre o iRedMail**

Veja detalhes sobre a versão 0.8.5:

<http://www.iredmail.org/forum/topic5167-news-announcements-bug-fixes-iredmail085-has-been-released.html>

Ele já vem com dois filtros interessantes: Vacation e Move Spam to Junk Folder. Ambos vem por padrão desativados.

Para ativar o do Spam abra o Roundcube

Configurações

Filtros

Em Filtros clique em Move Spam to Junk Folder

Apenas desmarque Filtro desativado e Salve

Pronto o plugin está ativo.

Configurar uma conta de e-mail para receber todos os e-mails

```
mysql -u root -p
use vmail;
INSERT INTO alias (address, goto) VALUES ('@ribafs.net.br','contato@ribafs.net.br');
```

### **Aumentando o tempo de sessão**

```
nano /usr/share/apache2/roundcubemail-0.8.5/config/main.inc.php
```

Mudar o tempo de 10 para 60 ou 4320:  
\$rcmail\_config['session\_lifetime'] = 4320;

### **Clamav**

```
/etc/init.d/clamav-freshclam restart
/etc/init.d/clamav-daemon restart
/etc/init.d/dovecot restart
```

### **Adicionar novo domínio ao iRedMail:**

<https://ribafs.org/iredadmin>

Adicionar - Domínio

Os domínios ficam armazenados na tabela domain do banco vmail.

Apache:

<http://httpd.apache.org/docs/2.2/logs.html>

O AWStats vem com o iRedMail e é uma boa ferramenta também para analisar logs.

### **Ver lista de e-mails do servidor:**

```
mailq
```

### **Testar:**

```
telnet localhost 25
telnet localhost 110
```

### **Portas Utilizadas pelo iRedMail**

Do site do iRedMail:

iRedMail Requer as seguintes portas abertas:

O Servidor de e-mail é um servidor complexo e requer várias portas abertas na rede. Por default o iRedMail precisa das portas:

Apache (Web server)  
80: porta normal do web service  
443: HTTPS (http over SSL)

## Postfix

25: normal SMTP  
587: Submission, SMTP over SSL.

## MySQL

3306: default listen port. (Recusa conexões da rede externa no iptables por default)

## OpenLDAP

389: normal LDAP port. (Recusa conexões da rede externa no iptables por default)  
636: LDAP over SSL. (Recusa conexões da rede externa no iptables por default)

## Dovecot

110: POP3 service  
995: POP3S (Secure POP3 over SSL)  
143: IMAP service  
993: IMAPS (Secure IMAP over SSL)  
2000: managesieve service. (Recusa conexões da rede externa no iptables por default)

## Policyd (Postfix policy server)

10031: default listen port. (Recusa conexões da rede externa no iptables por default)

## Amavisd-new

127.0.0.1:10024  
127.0.0.1:10025

Como habilitar na rede as portas desejadas?

Editar /etc/default/iptables (RHEL/CentOS) ou /etc/default/iptables (Debian/Ubuntu), e adicionar as portas que deseja abrir, assim:

```
#!/A INPUT -p tcp -m multiport --dport 80,443,25,465,110,995,143,993,587,465,22 -j ACCEPT  
-A INPUT -p tcp -m multiport --dport 80,443,25,465,110,995,143,993,587,465,22,10000 -j  
ACCEPT
```

E então restartar o serviço iptables para surtir efeito

```
: /etc/init.d/iptables restart
```

## Address Book

O Address Book (Livro de Endereços) do Roundcube fica localizado no banco roundcubemail, tabela contacts e configurado no arquivo config/main.inc.php.

## Migrar iRedMail para um Novo Servidor

MySQL: Migrar mail accounts

Todas as contas de e-mail estão armazenadas por padrão no banco vmail.

Basta exportar este banco no atual servidor e importar no novo.

Migrar mailboxes no formato maildir

Simplesmente copie todas as mailboxes no formato maildir para o novo servidor com iRedMail.

```
/var/vmail/vmail1
```

Ajuste o correto dono do arquivo de mailboxes. Por default o dono é o user vmail, group vmail.

Ajuste as permissões do arquivo mailboxes. Default é 0700.

Veja isso

[http://trac.roundcube.net/wiki/Howto\\_Upgrade](http://trac.roundcube.net/wiki/Howto_Upgrade)

Migrate Policyd database

O banco Policyd armazena as blacklist/whitelist, estrangulamento, etc. Para migrar seus dados, simplesmente exporte no atual e importe no novo servidor.

O script `/var/vmail/backup/backup_mysql.sh`

Cria um backup de todos os bancos do iRedMail.

**Upgrade para novas versões**

[http://www.iredmail.org/wiki/index.php?title=Main\\_Page#Upgrade\\_Tutorials](http://www.iredmail.org/wiki/index.php?title=Main_Page#Upgrade_Tutorials)

## **Configurações Extras no iRedMail**

3.1 - Antispam no RoundCube

3.2 - Configurando dkim para outros domínios

3.3 - Configurando o registro SPF do iRedMail no DNS

3.4 - Configuração do fail2ban

3.5 - Algumas configurações do iRedMail

3.6 - Customizar Título do Navegador e do Roundcube

3.7 - Como mudar o tamanho dos anexos dos e-mails no RoundCube

3.8 - Adicionar identidades ao Roundcube

3.9 - Instalar Plugins no Roundcube

3.10 - Adicionar novo domínio ao iRedMail:

**Atualização do clamav:**

```
freshclam
```

### **3.1 - Antispam no RoundCube**

spamassassin "treine" automaticamente as mensagens após os usuários marcarem como "Spam" ou "Não Spam".

Download

<http://www.tehinterweb.co.uk/roundcube/#pimarkasjunk2>

```
wget http://www.tehinterweb.co.uk/roundcube/plugins/markasjunk2.tar.gz
```

```
tar xzpvf markasjunk2.tar.gz -C /usr/share/apache2/roundcubemail-0.9.5/plugins
```

```
cp /usr/share/apache2/roundcubemail-0.9.5/plugins/markasjunk2/config.inc.php.dist
```

```
/usr/share/apache2/roundcubemail-0.9.5/plugins/markasjunk2/config.inc.php
```

```
nano /usr/share/apache2/roundcubemail-0.9.5/plugins/markasjunk2/config.inc.php
```

Mude as seguintes linhas:

```
$rcmail_config['markasjunk2_learning_driver'] = 'cmd_learn';
```

```
$rcmail_config['markasjunk2_spam_cmd'] = 'sa-learn --no-sync --spam --username=amavis %f';
```

Agora adicionar o plugin ao main.inc.php

```
nano /usr/share/apache2/roundcubemail-0.9.5/config/main.inc.php
```

Adicionar na linha:

```
$rcmail_config['plugins'] = array("password", "managesieve", "markasjunk2",);
```

Agora ao acessar o webmail verá um botão Spam que poderá ser clicado quando considerar uma mensagem spam.

Quando acessar a pasta Spam e selecionar uma mensagem verá o botão Not Junk (Não Spam), quando poderá ensinar ao spamassassin que esta mensagem não é spam.

## **Melhorando a eficiência do anti-spam**

No Debian por padrão a atualização diária das regras do Spamassassin vem desativada, para ativar basta editar o arquivo /etc/default/spamassassin e mudar a variável CRON para 1:

```
nano /etc/default/spamassassin  
CRON=1
```

Isso fará com que o script spamassassin, que está no diretório /etc/cron.daily seja executado diariamente.

## **Bloqueando SPAM com o próprio domínio**

Combater SPAMs que forjam o remetente sendo do próprio domínio.

```
nano /etc/postfix/main.cf
```

F6 para procurar smtpd\_sender\_restrictions

Alterar para isso:

```
smtpd_sender_restrictions = permit_mynetworks, reject_sender_login_mismatch,  
permit_sasl_authenticated, check_sender_access  
hash:/etc/postfix/controles/sender_restrictions,reject_unknown_sender_domain
```

Adicionamos a parte final.

```
mkdir /etc/postfix/controles
```



Crie o arquivo:  
nano /etc/postfix/controles/sender\_restrictions

Contendo:  
ribafs.org DISCARD Uso nao autorizado do ribafs.org  
ribafs.net.br DISCARD Uso nao autorizado do ribafs.net.br  
tiagoarts.com DISCARD Uso nao autorizado do tiagoarts.com

postmap /etc/postfix/main.cf  
postmap /etc/postfix/controles/sender\_restrictions

service postfix restart

Fonte: <http://respirandolinux.wordpress.com/>

### **3.2 - Configurando o registro dkim para outros domínios**

Adicionando outros domínios ao DKIM

```
cd /var/lib/dkim  
amavisd-new genrsa tiagoarts.com.pem  
amavisd-new genrsa ribafs.org.pem
```

```
chmod 0644 tiagoarts.com.pem  
chmod 0644 ribafs.org.pem
```

```
nano /etc/amavis/conf.d/50-user
```

Adicionar aqui:  
# Add dkim\_key here.  
dkim\_key("ribafs.net.br", "dkim", "/var/lib/dkim/ribafs.net.br.pem");  
dkim\_key("ribafs.org", "dkim", "/var/lib/dkim/ribafs.org.pem");  
dkim\_key("tiagoarts.com", "dkim", "/var/lib/dkim/tiagoarts.com.pem");

Alterar a linha, adicionando os domínios:

```
@local_domains_maps = ['ribafs.net.br', 'mail.ribafs.net.br', 'ribafs.org', 'tiagoarts.com'];
```

```
/etc/init.d/amavis restart
```

Testando:

```
amavisd-new showkeys tiagoarts.com  
amavisd-new showkeys ribafs.org  
http://www.iredmail.org/wiki/index.php?  
title=IRedMail/FAQ/Enable.DKIM.Signing.For.New.Mail.Domain/Debian.Ubuntu
```

### **3.3 - Configurando o registro SPF do iRedMail no DNS**

Exemplos simples:

```
TXT @ "v=spf1 a mx -all"
```

ou

```
TXT @ "v=spf1 mx mx:mail.ribafs.net.br -all"
```

Recomendações da FAQ do iRedMail

Please refer <http://www.openspf.org/> to setup SPF record.

This is a simply example:

```
iredmail.org.      3600  IN   TXT   "v=spf1 mx mx:mail.iredmail.org -all"
```

or:

```
iredmail.org.      3600  IN   TXT   "v=spf1 ip4:202.96.133.133 -all"
```

Exemplo:

```
yourdomain.com. 3600 IN TXT "v=spf1 mx a:mail.yourdomain.com -all"
```

### **3.4 - Configuração do fail2ban**

Logo após instalar o iRedMail altere o script:

```
nano /etc/fail2ban/jail.conf
```

```
#Altere o bantime para 3600. Para evitar erro.
```

```
#bantime = 600
```

```
bantime = 3600
```

```
#Adicione o findtime
```

```
findtime = 300
```

#### **Configurando o fail2ban para proteger 4 serviços: ssh, smtp, pop3/imap e webmail.**

fail2ban vem com filtro para o serviço sshd, então só precisamos criar 3 novos filtros. O arquivo de filtro define as expressões regulares para encontrar quais endereços IP devemos proibir.

```
nano /etc/fail2ban/filter.d/roundcube.iredmail.conf
```

```
[Definition]
```

```
failregex = roundcube: (.*) Error: Login failed for (.*) from <HOST>\.
```

```
ignoreregex =
```

```
nano /etc/fail2ban/filter.d/dovecot.iredmail.conf
```

```
[Definition]
```

```
failregex = (? : pop3-login|imap-login) : .* (? : Authentication failure|Aborted login \ (auth failed|Aborted login \ (tried to use disabled|Disconnected \ (auth failed) .* rip=(?P<host>\S*) , .*  
ignoreregex =
```

```
nano /etc/fail2ban/filter.d/postfix.iredmail.conf
```

```
[Definition]
```

```
failregex = \[<HOST>\]: SASL (PLAIN|LOGIN) authentication failed  
    reject: RCPT from (.*)\[<HOST>\]: 550 5.1.1  
    reject: RCPT from (.*)\[<HOST>\]: 450 3.7.1  
    reject: RCPT from (.*)\[<HOST>\]: 554 5.7.1  
ignoreregex =
```

Temos agora três novos arquivos de filtros. É hora de deixar fail2ban usá-los. Desde que o filtro do ssh é ativado por padrão, não precisa tocar todos os arquivos de configuração, por isso só precisa criar

"/etc/fail2ban/jail.local" para permitir esses três novos filtros.

No Debian/Ubuntu, fica em "/var/log/mail.log".

```
nano /etc/fail2ban/jail.local
```

```
[roundcube-iredmail]
```

```
enabled    = true  
filter     = roundcube.iredmail  
action     = iptables-multiport[name=roundcube,  
port="ssh,http,https,smtp,smtps,pop3,pop3s,imap,imaps,sieve", protocol=tcp]  
logpath    = /var/log/maillog  
findtime   = 3600  
maxretry   = 5  
# attention: time is in seconds - the value of 3600 means ONE hour  
# maybe you want to change it to 60 for testing  
bantime    = 3600  
ignoreip   = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
```

```
[dovecot-iredmail]
```

```
enabled    = true  
filter     = dovecot.iredmail  
action     = iptables-multiport[name=dovecot,  
port="ssh,http,https,smtp,smtps,pop3,pop3s,imap,imaps,sieve", protocol=tcp]  
logpath    = /var/log/dovecot.log  
maxretry   = 5  
findtime   = 300  
# attention: time is in seconds - the value of 3600 means ONE hour  
# maybe you want to change it to 60 for testing  
bantime    = 3600  
ignoreip   = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
```

```
# Adicionar seu e-mail abaixo em dest=  
[postfix-iredmail]  
enabled = true  
filter = postfix.iredmail  
action = iptables-multiport[name=postfix,  
port="ssh,http,https,smtp,smtps,pop3,pop3s,imap,imaps,sieve", protocol=tcp]  
#      sendmail[name=Postfix, dest=ribamar@ribafs.org]  
  
# You may need to change "logpath" of roundcube and postfix filter on different Linux/BSD.  
# On RHEL/CentOS, it's "/var/log/maillog".  
# On Debian/Ubuntu, it's "/var/log/mail.log".  
# On openSUSE, it's "/var/log/mail".  
# On FreeBSD, it's "/var/log/maillog".  
logpath = /var/log/maillog  
# attention: time is in seconds - the value of 3600 means ONE hour  
# maybe you want to change it to 60 for testing  
bantime = 3600  
maxretry = 5  
ignoreip = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
```

Restartar o fail2ban para que funcione:

```
/etc/init.d/fail2ban restart
```

Testando

Pode usar o comando "fail2ban-regex" para verificar o filtro

```
fail2ban-regex /var/log/maillog /etc/fail2ban/filter.d/roundcube.iredmail.conf
```

```
[...]  
Success, the total number of match is 3  
[...]
```

Depois:

```
fail2ban-regex /var/log/dovecot.log /etc/fail2ban/filter.d/dovecot.iredmail.conf
```

```
[...]  
Success, the total number of match is 3  
[...]
```

Depois:

```
fail2ban-regex /var/log/maillog /etc/fail2ban/filter.d/postfix.iredmail.conf
```

```
[...]  
Success, the total number of match is 3  
[...]
```

### 3.5 – Mais Algumas configurações do iRedMail

Mail Storage:

- Root directory: /var/vmail
- Mailboxes: /var/vmail/vmail1
- Backup scripts and copies: /var/vmail/backup

Funções que desabilitou no php.ini:

Disabled functions: show\_source,system,shell\_exec,passthru,exec,phpinfo,proc\_open

Policyd (cluebringer):

- \* Web UI:
  - URL: <https://www.ribafs.net.br/cluebringer/>
  - Username: postmaster@ribafs.net.br
  - Password: senharfs
- \* Configuration files:
  - /etc/cluebringer/cluebringer.conf
  - /etc/cluebringer/cluebringer-webui.conf
- \* RC script:
  - /etc/init.d/postfix-cluebringer
- \* Database:
  - Database name: cluebringer
  - Database user: cluebringer
  - Database password: oVhp6BW5I8HAPbLv50cIoALon00geW

Arquivos de log

- \* Log files:
  - /var/log/dovecot.log
  - /var/log/sieve.log
- \* See also:
  - /var/vmail/sieve/dovecot.sieve
  - Logrotate config file: /etc/logrotate.d/dovecot
  
- \* Log files:
  - /var/log/clamav/clamd.log
  - /var/log/clamav/freshclam.log

iRedAdmin

Bancos

iredadmin

- \* Settings:
  - /usr/share/apache2/iRedAdmin-0.3/settings.py
- \* See also:
  - /etc/apache2/conf.d/iredadmin.conf

Awstats:

- \* Configuration files:
  - /etc/apache2/conf.d/awstats.conf
- \* Login account:
  - Username: postmaster@ribafs.net.br, password: senharfs

- \* URL:
  - <https://www.ribafs.net.br/awstats/awstats.pl>
  - <https://www.ribafs.net.br/awstats/awstats.pl?config=web>
  - <https://www.ribafs.net.br/awstats/awstats.pl?config=smtp>
- \* Crontab job:  
shell> crontab -l root

#### Roundcube webmail:

- \* Configuration files:
  - /usr/share/apache2/roundcubemail-0.9.5/
  - /usr/share/apache2/roundcubemail-0.9.5/config/
- \* URL:
  - <http://www.ribafs.net.br/mail/>
  - <https://www.ribafs.net.br/mail/> (Over SSL/TLS)
  - <http://www.ribafs.net.br/webmail/>
  - <https://www.ribafs.net.br/webmail/> (Over SSL/TLS)
- \* Login account:
  - Username: postmaster@ribafs.net.br, password: senharfs
- \* See also:
  - /etc/apache2/conf.d/roundcubemail.conf

#### phpMyAdmin:

- /usr/share/phpmyadmin/config.inc.php
- <https://www.ribafs.net.br/phpmyadmin>
- /etc/apache2/conf.d/phpmyadmin.conf

#### Backup MySQL database:

- \* Script: /var/vmail/backup/backup\_mysql.sh
- \* See also:
  - # crontab -l -u root

#### iRedMail resumo

#### SSL

postfix  
dovecot  
clamav  
spamassassin  
amavis  
policyd  
mysql  
apache  
php  
phpmyadmin  
awstats

#### Web:

login - postmaster@ribafs.net.br  
senha -

https://www.ribafs.net.br/phpmyadmin  
https://www.ribafs.net.br/cluebringer/  
https://www.ribafs.net.br/awstats/awstats.pl  
https://www.ribafs.net.br/iredadmin  
https://www.ribafs.net.br/mail

Mail Storage:

- Root directory: /var/vmail
- Mailboxes: /var/vmail/vmail1
- Backup scripts and copies: /var/vmail/backup

Backup dos bancos do iRedMail, que está no cron (crontab -l):  
/var/vmail/backup/backup\_mysql.sh

### **3.6 - Customizar Título do Navegador e do Roundcube**

```
nano /usr/share/apache2/roundcubemail-0.9.5/config/main.inc.php
```

Alterar as duas linhas abaixo:

```
// add this user-agent to message headers when sending  
$rcmail_config['useragent'] = "RibaFS WebMail";
```

```
// use this name to compose page titles  
$rcmail_config['product_name'] = 'RibaFS Webmail';
```

### **3.7 - Como mudar o tamanho dos anexos dos e-mails no RoundCube**

Mudar o tamanho dos e-mails no Postfix (para 100MB)  
Executar (Observe: 104857600 = 100MB x 1024 KB x 1024 Bit):  
postconf -e message\_size\_limit='104857600'  
/etc/init.d/postfix restart

Mudar php para permitir upload deste tamanho  
nano /etc/php5/apache2/php.ini

```
memory_limit = 200M;  
upload_max_filesize = 100M;  
post_max_size = 100M;
```

Mudar o webmail Roundcube para permitir este upload  
nano /usr/share/apache2/roundcubemail/.htaccess

```
php_value upload_max_filesize 100M  
php_value post_max_size 100M
```

```
/etc/init.d/apache2 restart
```

<http://www.iredmail.org/forum/topic464-iredmail-support-faq-how-to-change-mail-attachment-size.html>

### **3.8 - Adicionar identidades ao Roundcube**

Para adicionar outros e-mails que serão gerenciados pelo Roundcube. Estes e-mails precisam ter o recurso de redirecionamento, como o Gmail.

```
nano /usr/share/apache2/roundcubemail-0.9.5/config/main.inc.php
```

Mudar a linha abaixo para:  
`$rcmail_config['identities_level'] = 0`

Vá novamente em Configurações – Identidades, que já aparece o botão +.

Configurações - Identidades  
Clicar em + e adicionar

### **3.9 - Instalar Plugins no Roundcube**

<http://plugins.roundcube.net/>  
[http://trac.roundcube.net/wiki/Plugin\\_Repository](http://trac.roundcube.net/wiki/Plugin_Repository)

Para instalar um plugin descompacte na pasta:  
`/usr/share/apache2/roundcubemail-0.9.2/plugins/`

Editar  
`nano config.inc.php`

Efetue configurações sugeridas e edite:  
`nano /usr/share/apache2/roundcubemail-0.9.2/config/main.inc.php`

Tecele F6 e Shift+Insert e cole:  
`$rcmail_config['plugins']`

Adicionar nosso plugin à linha:  
`$rcmail_config['plugins'] = array("password", "managesieve", "nomenovoplugin",);`

Salvar e fechar

Para desabilitar o plugin basta remover da linha acima.

### **3.10 - Adicionar novo domínio ao iRedMail**

Adicionar novos domínios através da interface web iredadmin



<https://ribafs.org/iredadmin>

Adicionar - Domínio

Os domínios ficam armazenados na tabela domain do banco vmail.



## 4.0 - Melhorando a Segurança do Servidor

- 4.1 - Sanitizar o SSH
- 4.2 - Monitorando login do root
- 4.3 - Sanitizar Joomla
- 4.4 - Instalar w3af
- 4.5 - Atualizações automáticas de segurança
- 4.6 - Protegendo administrators com SSL
- 4.7 - Configurando e usando fail2ban
- 4.8 - Sanitizar MySQL
- 4.9 - Sanitizar o Apache
- 4.10 - Sanitizar o PHP
- 4.11 - Sanitizar IPTables
- 4.12 - Sanitizar Registros do DNS para e-mail
- 4.13 - Instalando o IDS psad
- 4.14 - Melhorando a segurança do SSH com Denyhosts
- 4.15 - Monitorando rootkits com RKHunter
- 4.16 - Testando vulnerabilidades web com Nikto
- 4.17 - Monitorando a rede com ngrep
- 4.18 - Melhorando a segurança com o pacote harden
- 4.19 - Protegendo su
- 4.20 - Prevenir IP Spoofing
- 4.21 - Sanitizar a memória compartilhada
- 4.22 - Atualizando para a versão mais recente
- 4.23 - Scannear portas abertas
- 4.24 - Monitorar arquivos modificados
- 4.25 - Melhorar a segurança em partições
- 4.26 - Sanitizar seu Desktop
- 4.27 - phpsecinfo
- 4.28 - Monitorar logs com o logcheck
- 4.29 - Ajustando as Permissões do /var/www
- 4.30 - Upgrade do Ubuntu Server Entre as versões
- 4.31 - Terminal Web
- 4.32 - Usando Senhas Fortes no Servidor

### 4.1 - SSH hardening

Antes criar o usuário ribafs, com acesso ao sudoers e ssh

```
nano /etc/ssh/sshd_config
```

```
Port 65522  
PermitRootLogin no  
AllowUsers ribafs  
LoginGraceTime 30  
AllowUsers ribafs
```

```
service ssh restart
```

Adicionar ao /etc/default/iptables para somente acessar do IP  
iptables -A INPUT -p tcp -s 72.232.194.162 --dport 22 -j ACCEPT

Caso não possa usar um IP, adicione isso para prevenir ataques de brute-force por logging e bloqueando repetidas tentativas de login do mesmo IP:

```
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name ssh --rsource  
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent ! --rcheck --seconds 60  
--hitcount 4 --name ssh --rsource -j ACCEPT
```

```
service iptables restart
```

## 4.2 - Monitorando login do root

Adicione ao início do script .bashrc do root:

```
nano /root/.bashrc  
echo -e "Acesso ao shell do Root em `tty` \n `w`" | mail -s "Alerta: Acesso do root"  
ribamar@ribafs.org
```

## 4.3 - Sanitizar Joomla

- Joomla:

- Adotar SSL no administrator
- Reforçar com proteção do diretório administrator pelo Apache
- Esconder termo "Joomla" dos metatags:

- Alterar metatags em Configuração Global - Configurações de Meta Dados (Trocar Joomla por outra palavra)

- Adicionar a tag <head> do template (para ocultar na origem do código HTML):

```
<?php $this->setGenerator('Ribafs - Desenvolvimento Web'); ?>
```

- Renomear diretório do template allrounder para "modelo" (testar antes localmente)
- Usar mod\_rewrite
- Habilitar o plugin reCaptcha em todos os formulários
- Ajustar donos de todos os arquivos root:www-data e permissões:

arquivos - 644

diretórios - 755

index.php - 444

administrator/index.php - 444

templates/modelo/index.php - 444

configuration.php

- copiar configuration.php para o /var

- Remover todo o conteúdo do /portal/configuration.php e deixar apenas estas duas

linhas:

```
<?php
```

```
require_once( dirname( __FILE__ ) . '/../configuration.php' );
```

- Fazer o mesmo com o refletindo e o família

- Desabilitar execução de scripts em imagens

Criar um .htaccess no diretório ou adicionar ao existente as duas linhas abaixo:

```
AddHandler cgi-script .php .pl .py .jsp .asp .htm .shtml .sh .cgi  
Options -ExecCGI
```

[http://docs.joomla.org/Security\\_Checklist/You\\_have\\_been\\_hacked\\_or\\_defaced](http://docs.joomla.org/Security_Checklist/You_have_been_hacked_or_defaced)

Consultar a lista de vulnerabilidade de extensões antes de instalar é algo prudente:

[http://docs.joomla.org/Vulnerable\\_Extensions\\_List](http://docs.joomla.org/Vulnerable_Extensions_List)

Instale somente o que for usar e remova o que não precisa;

Atualize também todas as extensões de terceiros com frequência;

Não use o usuário "admin". Mude para algo customizado;

Nunca use permissões do tipo 666 ou 777 para arquivos e diretórios;

Use URLs amigáveis e use um mapa do site;

Mais detalhes:

<http://ribafs.org/portal/joomla/seguranca>

<http://ribafs.org/portal/cake/seguranca>

Sites e Aplicativos em Geral

<http://ribafs.org/portal/programacao-web/seguranca>

Veja no Extensions outras opções, especificamente aqui:

<http://extensions.joomla.org/extensions/access-a-security/site-security>

#### **4.4 - Instalar e usar o W3AF**

Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.

```
apt-get install w3af
```

Traz uma interface para a console e uma gráfica

## 4.5 - Atualizações automáticas de segurança

aptitude install unattended-upgrades

```
nano /etc/apt/apt.conf.d/10periodic
```

Excluir tudo e adicionar:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

Isso somente atualiza pacotes de segurança

Atualização completa, de todos os pacotes:

```
apt-get update
apt-get upgrade
```

## 4.6 - Protegendo administrators com SSL

Proteger seções administrator de sites Joomla forçando SSL

Forçar acesso somente com SSL (porta 443):

Adicionar a função ForceHTTPS() logo no início do administrator/index.php:

```
<?php
/**
 * @package Joomla.Administrator
 * @copyright Copyright (C) 2005 - 2013 Open Source Matters, Inc. All rights reserved.
 * @license GNU General Public License version 2 or later; see LICENSE.txt
 */

// Set flag that this is a parent file
define('_JEXEC', 1);
define('DS', DIRECTORY_SEPARATOR);

function ForceHTTPS() {
    if ($_SERVER['HTTPS'] != "on") {

        $url = $_SERVER['SERVER_NAME'];

        $new_url = "https://" . $url . $_SERVER['REQUEST_URI'];
        header("Location: $new_url");
        exit;
    }
}
```

```
ForceHTTPS();
```

```
...
```

### **ALERTA**

Para subdomínios entre o caminho completo na linha do \$new\_url.

Cuidado quando implementa SSL somente em uma seção do site, pois pode gerar problema de acesso quando acessa o administrador com SSL e depois vai acessar o site com SSL. Vale a pena implementar somente no administrador mas fique atento. O site deve ser acessado sem https, somente com http.

## **4.7- Configurando e usando fail2ban**

```
nano /etc/fail2ban/jail.conf
```

Entre com o e-mail do administrador, que receberá avisos de segurança

```
#mta = sendmail
```

```
mta = mail
```

```
destemail = ribamar@ribafs.org
```

Checar status:

```
fail2ban-client status
```

Restartar

```
/etc/init.d/fail2ban restart
```

### **Desbloquear um certo IP bloqueado por engano**

```
iptables -L -n
```

Após rodar o comando acima e percebermos o IP bloqueado, por exemplo 201.14.45.23, rode:

```
iptables -D fail2ban-SSH -s 201.14.45.23 -j DROP
```

Assim este IP` poderá acessar novamente.

Comando mais específico:

```
fail2ban-client set ssh-iptables unbanip IpaRemover
```

Whitelisting

Whitelisting is setup in the jail.conf file using a space separated list.

```
[DEFAULT]
```

```
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
```

```
# ban a host which matches an address in this list. Several addresses can be
```

```
# defined using space separator.
```

```
ignoreip = 127.0.0.1 192.168.1.0/24 8.8.8.8
```

```
# This will ignore connection coming from common private networks.
```

```
# Note that local connections can come from other than just 127.0.0.1, so
```

```
# this needs CIDR range too.
```

```
ignoreip = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
```

## Blacklist

First, check the banaction currently used (you need that, to modify the correct actionfile afterwards)  
/etc/fail2ban/jail.local

```
#
# ACTIONS
#
...
banaction = iptables-multiport
...

/etc/fail2ban/action.d/iptables-multiport.conf

...
actionstart = iptables -N fail2ban-<name>
               iptables -A fail2ban-<name> -j RETURN
               iptables -I INPUT -p <protocol> -m multiport --dports <port> -j fail2ban-<name>
               # Persistent banning of IPs
               cat /etc/fail2ban/ip.blacklist | while read IP; do iptables -I fail2ban-<name> 1 -s $IP -j
DROP; done
...
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
            # Persistent banning of IPs
            echo '<ip>' >> /etc/fail2ban/ip.blacklist
...

```

Your blacklist should look something like this (one IP per line, of course you can add IPs manually)  
/etc/fail2ban/ip.blacklist

```
...
10.0.0.242
192.168.1.39
...

```

Restart fail2ban to make the changes active



## 4.8 - Sanitizar MySQL

mysql\_secure\_installation

Responda yes para todas as perguntas, exceto a inicial da senha

Algum tempo depois, verifique com paciência os logs recebidos do logcheck e se aparecer algum usuário sem senha pela seguinte mensagem:

```
"WARNING: mysql.user contains 3 root accounts without password!"
```

Execute novamente:

mysql\_secure\_installation

Depois acesse

```
mysql -u root -p
```

Verifique as contas do root:

```
SELECT User, Host, Password FROM mysql.user;
```

Veja as que estão sem senha e execute para cada uma:

```
SET PASSWORD FOR 'root'@'127.0.0.1' = PASSWORD('suasenha');
```

```
SET PASSWORD FOR 'root'@'::1' = PASSWORD('suasenha');
```

Teste novamente:

```
SELECT User, Host, Password FROM mysql.user;
```

## 4.9 - Sanitizar o Apache

Esconder informações do Apache:

```
nano /etc/apache2/conf.d/security
```

mudando as duas linhas abaixo:

```
ServerTokens Prod  
ServerSignature Off  
#Adicionar  
FileETag None
```

```
/etc/init.d/apache2 restart
```

## 4.10 - Sanitizar o PHP

Tomar cuidado para usar boas práticas de segurança na programação de forma a manter o servidor seguro.

Esconder a extensão do php

Adicionar ao final do .htaccess

```
<IfModule mod_rewrite.c>
Options +FollowSymLinks
Options +Indexes
RewriteEngine On
RewriteCond %{SCRIPT_FILENAME} !-d
RewriteRule ^([\^\.]*)$ $1.php [NC,L]
</IfModule>
```

Original em inglês: [http://www.ehow.com/how\\_12037234\\_hide-php-extension-apache.html](http://www.ehow.com/how_12037234_hide-php-extension-apache.html)

Checar módulos

```
php -m
Remover os não usados
```

Ajustes no php.ini  
nano /etc/php5/apache2/php.ini

Com a ajuda do PHPsecinfo:

```
allow_url_fopen = Off
file_uploads = On
session.save_path = "/var/www/phptmp"
memory_limit = 32M;
open_basedir = /var/www
post_max_size = 256K
upload_max_filesize = 256K
upload_tmp_dir = /var/www/phptmp
```

```
chown www-data /var/www/phptmp
chmod 700 /var/www/phptmp
```

```
expose_php=Off (default na versão 5.3)
```

```
display_errors=Off (default na versão 5.3)
log_errors=On
error_log=/var/log/apache2/php_scripts_error.log
```

```
disable_functions
=eval,show_source,system,shell_exec,passthru,exec,phpinfo,proc_open,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,
```

```
/etc/init.d/apache2 restart
```

Manter o PHP, os softwares e o SO atualizados

Proteger arquivos de configuração do apache, php e mysql contra escrita:  
/etc/php5/apache2/php.ini

/etc/apache2/sites-available/default e demais  
/etc/mysql/my.ini

Busca por backdoors

```
grep -iR 'c99' /var/www/  
grep -iR 'r57' /var/www/  
find /var/www/ -name \*.php -type f -print0 | xargs -0 grep c99  
grep -RPn "(passthru|shell_exec|system|base64_decode|fopen|fclose|eval)" /var/www/
```

Detalhes no documento

Linux: 25 PHP Security Best Practices For Sys Admins

<http://www.cyberciti.biz/tips/php-security-best-practices-tutorial.html>

## **4.11 - Sanitizar IPTables**

Caso tenha instalado o iRedMail ele já instala um firewall com o IPTables e cuida bem da segurança.

Tanto que se quiser usar qualquer outra porta extra terá que abri manualmente.

Evite abrir novas portas, mas se precisar edite o arquivo:

```
nano /etc/default/iptables
```

Exemplo: adicionei para o webmin:

```
-A INPUT -p tcp --dport 10000 -j ACCEPT
```

Visualizar uso:

```
iptables -L
```

## **4.12 - Sanitizar Registros do DNS para e-mail**

Use SPF e DKIM para evitar que seu servidor seja visto como spammer.

Algumas interfaces oferecem o registro SPF, em outras precisamos usar o registro TXT

Ver detalhes no item 2.8.

## 4.13 - Instalando o IDS psad

IDS (Intrusion Detection System) - Detectar Tentativas de Intrusão

aptitude install psad

Checar status atual:

```
psad -S
```

Após executar guarda o resultado em:

```
/var/log/psad/status.out
```

Podemos configurar para envio de e-mail em detecção de intrusão:Reforçando a

```
nano /etc/psad/psad.conf
```

```
EMAIL_ADDRESSES      ribamar@ribafs.org,admin@ribafs.org;
HOSTNAME              web.ribafs.org;      (mudar para o FQDN)
ENABLE_AUTO_IDS      Y;
```

Restartar:

```
service psad restart
```

Reload e update:

```
psad -R
```

```
psad --sig-update
```

```
psad -H
```

Status:

```
psad --Status
```

```
psad --debug
```

```
nano /etc/php5/conf.d/suhosin.ini
```

Mude a linha abaixo:

```
suhosin.session.encrypt = off
```

```
service apache2 restart
```

Após instalar e configurar recebi um e-mail sugerindo adicionar ao

```
nano /etc/default/iptables
```

```
# Log, Adicionei pelo psad
```

```
-A INPUT -j LOG
```

```
-A FORWARD -j LOG
```

```
/etc/init.d/iptables restart
```

Logs:

```
/var/log/psad
```

Para receber o syslog por e-mail:

```
sudo apt-get install logcheck syslog-summary
```

Setar seu e-mail em:  
nano /etc/logcheck/logcheck.conf

#### **4.14 - Melhorando a segurança do SSH com Denyhosts**

O denyhosts destina-se a ajudar a impedir ataques a servidores SSH (também conhecido como ataques baseados em dicionário e ataques de força bruta).

```
/etc/hosts.allow - permitidos  
/etc/hosts.deny - negados
```

Negar todos:  
/etc/hosts.deny  
sshd: ALL

Permitir conexão somente de um certo IP:  
/etc/hosts.allow  
sshd: 24.229.54.125 (IP de casa, que muda) ou sshd: 177.0.0.0/255.0.0.0  
sshd: 201.18.141.126

Usando um IP exclusivo para os sites

Outro exclusivo para acesso por SSH e aplicativos internos, arquivos em diretórios protegidos  
nano /etc/ssh/sshd\_config

```
ListenAddress 24.229.54.125      (somente para quem acessa de uma intranet e  
                                não externo. Não dá para VPS, que acessa eternamente)
```

```
apt-get install denyhosts  
service denyhosts start
```

```
nano /etc/denyhosts.conf
```

```
ADMIN_EMAIL = ribamar@ribafs.org  
SYSLOG_REPORT=YES
```

Adicione seu IP ou qualquer outro que queira permitir acesso ao arquivo:  
nano /etc/hosts.allow

Assim:  
sshd: 177.130.202.171

Fica complicado se você administra de um micro usado ADSL, que muda de IP a cada ligação da sua internet. Caso seja assim, precisará adicionar seu novo IP ao hosts.allow sempre que seu IP mudar. Também precisa adicionar os IPs de todos os micros que usa para administrar o servidor. Mas é bom manter a ferramenta (denyhosts), visto que é realmente eficiente.

Se achar trabalhoso pode editar o script de configuração e mudar o parâmetro  
HOSTNAME\_LOOKUP  
para NO  
E restartar o denyhosts.

Monitorando  
less /etc/hosts.deny

Impressiona ver o conteúdo do arquivo acima com vários IPs bloqueados, enquanto nem percebemos nada e isso reforça a necessidade de cuidar bem da segurança. O logwatch me mostra a mensagem:

“Um total de nove sites sondado o servidor”.

service denyhosts restart

#### **4.15 - Monitorando rootkits com RKHunter**

O RKHunter efetua varreduras por rootkits, backdoors e possíveis explorações locais. Ele faz isso comparando hashes SHA-1 de arquivos importantes com conhecidos bons em bancos de dados on-line, em busca de diretórios padrão (de rootkits), permissões erradas, arquivos ocultos, strings suspeitos em módulos do kernel, e testes especiais para Linux e FreeBSD.

apt-get install rkhunter

Executar e atualizar rkhunter:

```
rkhunter --update  
rkhunter --propupd  
rkhunter --check
```

Observe os Warning em vermelho

Ver report:

```
less /var/log/rkhunter.log
```

```
logwatch | less
```

## 4.16 - Testando vulnerabilidades web com Nikto

O Nikto é web server scanner escrito em perl usado para detectar vulnerabilidades em servidores web. Ele é muito simples de ser usado e atualizado gerando relatórios em txt, html e csv. Requer repositório multiverse no /etc/apt/sources.list

```
apt-get install nikto
```

Atualizando os plugins:  
nikto -update

Usando o Nikto

```
nikto -h HOST -p PORT
```

```
nikto -h HOST -p PORT -ssl
```

```
nikto -h ribafs.org  
nikto -C all -host 200.128.X.X -o vitima.txt (mude X.X pelos números desejados)
```

- C all - Força a checagem de todos os diretórios em busca de cgi
- host - Ip da vitima
- o - Gera um arquivo de relatório

Varrendo uma porta de um host:  
nikto -h google.com -p 443

Help  
nikto -H | less

Esta ferramenta tanto ajuda a defender o seu site quanto ajuda para quem quer perceber vulnerabilidades em outros sites ou atacar.

Documentação oficial:  
<http://cirt.net/nikto2-docs/>

Exemplos de uso:  
<http://cirt.net/nikto2-docs/usage.html>

Usando ubuntu, onde tem perl nikto.pl usamos somente nikto.

Opções de comando:  
<http://cirt.net/nikto2-docs/options.html>

Tutorial:  
<http://www.binarytides.com/nikto-hacking-tutorial-beginners/>

## **4.17 - Monitorando a rede com ngrep**

apt-get install ngrep

ngrep -h (help)

Usando:

ngrep -d any port 25

Monitorar todas as atividades cruzando origem e destino da porta 25 (SMTP)

Execute o comando acima. Observe que o terminal fica parado a espera de ações na porta 25. Envie um e-mail do seu servidor para qualquer e-mail e veja o que acontece.

ngrep -d any 'error' port syslog

Monitorar qualquer tráfego na rede baseado no syslog procurando a ocorrência da palavra ``error''.

ngrep -wi -d any 'user|pass' port 21

Monitorar qualquer tráfego cruzando origem e destino na porta 21

Origem: <http://ngrep.sourceforge.net/usage.html>

## **4.18 - Melhorando a segurança com o pacote harden**

Este pacote é destinado a ajudar o administrador a melhorar a segurança do sistema e instala diversos pacotes com essa finalidade.

Contendo: checksecurity harden-environment harden-servers harden-tools libipc-signal-perl libmime-types-perl libproc-waitstat-perl logcheck logcheck-database logtail mime-construct sash

apt-get install harden

## **4.19 - Proteger su limitando o acesso somente para o grupo admin**

usermod -a -G admin ribafs

dpkg-statoverride --update --add root admin 4750 /bin/su

## **4.20 - Prevenir IP Spoofing**

nano /etc/host.conf

Adicione ou edite:

order bind,hosts

nospoof on

Desativar modo promiscuo em interfaces

ifconfig venet0:0 -promisc

ifconfig venet0:1 -promisc



```
ifconfig venet0:2 -promisc
ifconfig venet0:3 -promisc
```

```
nano /etc/sysctl.conf
```

Descomente ou adicione as linhas seguintes:

```
# IP Spoofing protection
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Disable source packet routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0

# Ignore send redirects
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Log Martians
net.ipv4.conf.all.log_martians = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1
```

## **4.21 - Sanitizar a memória compartilhada**

Sanitizar a memória compartilhada para somente leitura  
nano /etc/fstab

Adicionar a linha:

```
tmpfs /dev/shm tmpfs defaults,noexec,nosuid 0 0
```

## 4.22 - Atualizando para a versão mais recente

Quando quiser atualizar da versão 12.04 para a 12.10, por exemplo.

```
sudo apt-get install update-manager-core (caso ainda não esteja instalado)
```

Executar a ferramenta de atualização com o comando:  
do-release-upgrade -d

## 4.23 - Scannear portas abertas

```
apt-get install nmap
```

```
nmap -v -sT localhost
```

```
nmap -v -A dominio.com (mostra muitas informações importantes e dicas para fechar)
```

Scannear SYN:  
nmap -v -sS localhost

```
netstat -tulp  
nmap -sTU 10.40.100.123  
sudo lsof -i -n | egrep 'COMMAND|LISTEN|UDP'
```

## 4.24 - Monitorar arquivos modificados

```
find /var/www -type f -ctime -1 -exec ls -ls {} \;
```

Podemos colocar no cron para que seja executado a cada madrugada e nos envie um e-mail.

Procurar arquivos com 666

```
find /var/www -xdev -perm +o=w ! \( -type d -perm +o=t \) ! -type l -print
```

Procurar diretórios com 777

```
find /var/www -type d -perm -o+w -exec ls -ld {} \;
```

Procurar contas sem senha

```
awk -F: '($2 == "") {print}' /etc/shadow
```

## 4.25 - Melhorar a segurança em partições

Melhorar a segurança na partição /tmp e na /home

Caso tenha a possibilidade de criar estas partições...

```
nano /etc/fstab
```

```
/dev/hda5    /tmp    ext4    defaults,noexec    0    2  
/dev/hda6    /home  ext4    defaults,nosuid    0    2
```

## **4.26 - Sanitizar seu Desktop**

Instalar John the ripper numa estação desktop para testar as senhas do servidor

aptitude install john

Dicionário - /usr/share/john /password.lst

Utilizar para validar as senhas  
john /etc/shadow

As senhas descobertas por ele ficam em:  
/usr/share/john /john.pot

## **4.27 - phpsecinfo**

Uma ferramenta auxiliar de segurança.  
Oferece uma interface parecida com a da função phpinfo() mas mostrando um relatório de segurança sobre o ambiente do PHP e oferece sugestões de como corrigir as falhas.

Download  
wget <http://phpsec.org/projects/phpsecinfo/phpsecinfo.zip>

Instalar - Testar - Corrigir - Mover para fora do www

## **4.28 - Monitorar logs com o logcheck**

Lê todo os logs do sistema e de aplicações e envia um e-mail com relatório de anomalias.

aptitude install logcheck

Configurar (e-mail e outras):  
nano /etc/logcheck/logcheck.conf

Frequência em que roda  
nano /etc/cron.d/logcheck

Roda a cada reboot e a cada 2 minutos e envia e-mail para o root:  
MAILTO=root

```
@reboot    logcheck  if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck -R; fi  
2 * * * *  logcheck  if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi
```

Mudar o e-mail, e de 2 minutos para todo dia 1 da manhã:

0 1 \* \* \* ...

Roda com o próprio usuário:  
sudo -u logcheck logcheck

## **4.29 - Ajustando as Permissões do /var/www**

### **Permissões para quem faz tudo como root**

```
chown -R www-data:www-data /var/www  
find /var/www -type d -exec chmod 2755 {} \  
find /var/www -type f -exec chmod 0644 {} \  
;
```

Adicionar ao final do arquivo

```
nano /etc/skel/.bashrc  
umask u=rwx,g=rx,o=rx
```

Sempre que descompactar um pacote no /var/www

Executar novamente:

```
chown -R root:www-data /var/www  
find /var/www -type d -exec chmod 2755 {} \  
find /var/www -type f -exec chmod 0644 {} \  
;
```

Criar script para facilitar:

```
nano /root/p.sh
```

Contendo:

```
#!/bin/bash  
echo "SINTAXE: /root/p diretorio"  
chown -R root:www-data /var/www/$1  
find /var/www/$1 -type d -exec chmod 2755 {} \  
find /var/www/$1 -type f -exec chmod 0644 {} \  
;  
  
chmod u+x /root/p.sh
```

### **Quem trabalha com uma equipe**

De forma a agilizar as permissões web

Uma forma confortável de ter uma equipe de programadores editando os scripts PHP no /var/www é configurando donos e permissões como a seguir. Assim quando um programador cria ou muda um script todos os demais terão acesso de escrita ao mesmo.

```
addgroup webdevel  
adduser ribafs webdevel
```

```
adduser www-data webdevel
```

```
chown -R root:webdevel /var/www  
find /var/www -type d -exec chmod 2775 {} \  
find /var/www -type f -exec chmod 0664 {} \  
;
```

Adicionar ao final do arquivo

```
nano /etc/skel/.bashrc  
umask u=rwx,g=rwx,o=rx
```

Para os usuários que já tenham sido criados antes devemos adicionar também

```
su - ribafs  
nano /home/ribafs/.bashrc  
umask u=rwx,g=rwx,o=rx
```

Para ter efeito imediato requer:

```
reboot
```

Meu usuário é o ribafs, mude para o seu e adicione outros se precisar.

Sempre que baixar um pacote compactado deve precisar repetir os passos de permissões, pois os arquivos internos geralmente tem permissões inviáveis e até perigosas, como 777:

```
chown -R root:webdevel /var/www  
find /var/www -type d -exec chmod 2775 {} \  
find /var/www -type f -exec chmod 0664 {} \  
;
```

Assim quando instalamos o Joomla e copiamos o arquivo compactado como root, para o /var/www. Descompactamos e renomeamos para "portal".

Quando vamos instalar pelo navegador, chega o momento de excluir o diretório "installation" e se tivermos adotado o esquema acima teremos permissão de remover apenas clicando. Isso não significa que as permissões estão totalmente "abertas", com 777, mas sim que o usuário www-data tem a devida permissão de excluir.

### **Criar Script para Facilitar o Trabalho**

Vamos criar um script que sem parâmetro execute no /var/www

Podemos passar um subdiretório para que execute em /var/www/site2, por exemplo, se chamarmos assim “/home/ribafs/p site2”

```
nano /home/ribafs/p
```

Contendo:

```
chown -R root:webdevel /var/www/$1  
find /var/www/$1 -type d -exec chmod 2775 {} \  
find /var/www/$1 -type f -exec chmod 0664 {} \  
;
```

Dar permissão apenas ao dono

```
chmod u+x /home/ribafs/p
```

Quando descompactar algo no /var/www/site2, executar:  
/home/ribafs/p site2

Para varrer todo o /var/www, execute apenas:  
/home/ribafs/p

## **Segurança**

Você poderia copiar este script para uma pasta no path como /usr/local/bin o que facilitaria para você, pois bastaria digitar “p” em qualquer lugar. Como também poderia dar as permissões assim:

```
chmod +x /home/ribafs/p
```

Mas ambos os procedimentos seriam menos seguros. Este último permite que qualquer usuário execute e a solução anterior permite apenas o dono.

## **Atitude Segura**

Veja que para que você torne seu servidor mais seguro precisa ter uma atitude de vigilância e zelo por ele. Não é uma questão de seguir algumas dicas ou técnicas, mas uma questão de atitude, atitude segura e de cuidado.

## **4.30 - Upgrade do Ubuntu Server Entre as versões**

12.04 - 04/2012 (Precise Pangolin)

14.04 - 04/2014 (Trusty Tahr)

Efetuar antes um backup completo do servidor atual

```
sudo apt-get update && sudo apt-get upgrade
```

```
sudo apt-get install update-manager-core
```

```
nano /etc/update-manager/release-upgrades
```

Altere

```
[DEFAULT] Prompt=its
```

```
sudo do-release-upgrade -d
```

Fonte:

<http://www.estagio.online.pt/upgrade-ubuntu-10-04-server-12-04-lts/>

## **4.31 - Terminal Web**

Alguns serviços como o DigitalOcean e o Servermania oferecem um terminal em sua interface web para emergências. Para o caso de ficarmos impedidos de acessar via SSH.

Se acontecer de você ser impedido de acessar o servidor via SSH, acesse o site do DigitalOcean, faça login, vá em Droplets

-Selecione a sua droplet clicando no nome dela

-Então clique em Console Access e faça login

-Após o login edite o arquivo:

```
nano /etc/hosts.deny
```

Remova o seu IP.

Caso seu IP não seja fixo você pode saber qual está usando acessando: <http://abusar.org.br>

Veja logo acima.

Basta comentar a linha com o seu IP ou remover.

Agora já poderá acessar via SSH.

Caso não tenha feito nada por merecer este bloqueio, edite o arquivo:

```
nano /etc/hosts.allow
```

 e adicione seu IP como sugerido acima na configuração do denyhosts.

O fail2ban faz isso quando tentamos 3 vezes acessar via SSH e erramos a senha nas 3 tentativas, sendo que bloqueia no IPTables.

## **4.32 - Usando Senhas Fortes no Servidor**

Senhas para alta segurança - 24 caracteres

Segurança média - 16 caracteres

Como os hackers usam computadores para quebrar senhas, quanto maior mais forte.

Como reforçar uma senha:

- aumentar o tamanho da senha
- misturar letras com números
- inserir símbolos/espços
- usar maiúsculas
- caso use frase conhecida, troque os espaços por algum símbolo como o \* ou outro

O que não usar:

- palavras simples
- frases conhecidas
- data de nascimento
- número de documento
- não criar senhas que não lembrar
- evite ter muitas senhas
- evite ficar mudando as senhas. Só mude se suspeitar de algo
- não use senhas simples e lógicas, mas procure criar palavras/frases sem sentido ou aleatórias

Original em inglês:

How to Choose a Good Password

[http://www.kryptel.com/articles/encryption\\_passwords.php](http://www.kryptel.com/articles/encryption_passwords.php)

## **4.33 - Instalação e Configuração do mod\_security e do mod\_evasive**

4.33.1 - Instalação do mod\_security e do mod\_evasive

4.33.2 - Liberando sites

4.33.3 - Testando a segurança do site

### **4.33.1 - Instalação do mod\_security e do mod\_evasive**

ModSecurity é um software open source, um módulo de firewall de aplicação web livre (WAF) do Apache. Com mais de 70% de todos os ataques agora realizados sobre o nível de aplicação web, as organizações precisam de toda a ajuda que podem obter para tornar os seus sistemas seguros. WAFs são implantados para estabelecer uma camada de segurança externa, para aumentar a segurança, detectar e prevenir ataques antes que eles atinjam as aplicações web. Ele fornece proteção contra uma série de ataques contra aplicações web e permite a monitorização do tráfego HTTP e análise em tempo real, com pouca ou nenhuma mudança na infra-estrutura existente (<http://www.jangestre.com/2012/04/ubuntu-1204-lts-64bit-apache2-mod.html>).

Instalando o firewall de aplicações ModSecurity e o ModEvasive para prevenir ataques de DDOS

Instalação dos módulos mod\_security com OWASP e mod\_evasive no Apache2 do Ubuntu 12.04 Server

O apache já deve estar instalado.

```
apt-get install libxml2 libxml2-dev libxml2-utils libaprutil1 libaprutil1-dev libapache-mod-security
```

```
Somente para sistema 64 bit: ln -s /usr/lib/x86_64-linux-gnu/libxml2.so.2 /usr/lib/libxml2.so.2
```

```
apt-get install libapache-mod-security
```

```
mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

```
nano /etc/modsecurity/modsecurity.conf
```

```
SecRuleEngine On
```

```
SecRequestBodyLimit 16384000
```

```
SecRequestBodyInMemoryLimit 16384000
```

```
cd /tmp
```

```
wget https://github.com/SpiderLabs/owasp-modsecurity-crs/tarball/v2.2.5
```

```
mv v2.2.5 modsecurity-crs_2.2.5.tar.gz
```

```
tar -zxvf modsecurity-crs_2.2.5.tar.gz
```



```
cp -R SpiderLabs-owasp-modsecurity-crs-5c28b52/* /etc/modsecurity/
```

```
mv /etc/modsecurity/modsecurity_crs_10_setup.conf.example  
/etc/modsecurity/modsecurity_crs_10_setup.conf
```

```
cd /etc/modsecurity/base_rules  
for f in * ; do sudo ln -s /etc/modsecurity/base_rules/$f /etc/modsecurity/activated_rules/$f ; done  
cd /etc/modsecurity/optional_rules  
for f in * ; do sudo ln -s /etc/modsecurity/optional_rules/$f /etc/modsecurity/activated_rules/$f ;  
done
```

```
nano /etc/apache2/mods-available/mod-security.conf
```

Add:

```
Include "/etc/modsecurity/activated_rules/*.conf"
```

```
a2enmod headers  
a2enmod mod-security
```

```
service apache2 restart  
Caso acuse erro edite  
nano -c /etc/modsecurity/modsecurity.conf
```

E comente a linha do erro, aqui foi a 212

Mod Evasive

```
apt-get install libapache2-mod-evasive
```

```
mkdir /var/log/mod_evasive
```

```
chown www-data:www-data /var/log/mod_evasive/
```

```
nano /etc/apache2/mods-available/mod-evasive.conf
```

Add:

```
<ifmodule mod_evasive20.c>  
  DOSHashTableSize 3097  
  DOSPageCount 2  
  DOSSiteCount 50  
  DOSPageInterval 1  
  DOSSiteInterval 1  
  DOSBlockingPeriod 10  
  DOSLogDir /var/log/mod_evasive  
  DOSEmailNotify ribamar@ribafs.org  
  DOSWhitelist 127.0.0.1  
  DOSWhitelist 177.130.202.171  
</ifmodule>
```

```
a2enmod mod-evasive
```

service apache2 restart

Logs

tail /var/log/apache2/modsec\_audit.log

Para adicionar um IP na white list adicione uma linha no arquivo acima:

```
DOSWhitelist 162.13.23.127
```

Devemos adicionar o IP de cada computador que usamos para administrar o servidor.

É bom lembrar que softwares como o mod\_evasive e o denyhosts precisam ter em sua whitelist nossos IP de acesso, caso contrário teremos problema. Ainda bem que o Ocean tem uma console via web.

Com isso quando ele considerar algo que mereça mandará para a blacklist e te enviará um e-mail

Para não mais receber os e-mails mude para DOSSystemCommand ao invés de DOSEmailNotify, assim:

```
nano /etc/apache2/mods-available/mod-evasive.conf
```

```
DOSSystemCommand "echo 'mod_evasive HTTP Blacklisted %s more info here:
```

```
www.projecthoneypot.org/ip_%s' | mail -s 'Blocked IP by mod_evasive' root@localhost"
```

Lista de discussão

[http://sourceforge.net/mailarchive/forum.php?forum\\_name=mod-security-users](http://sourceforge.net/mailarchive/forum.php?forum_name=mod-security-users)

Lisra do owasp

[https://www.owasp.org/index.php/Category:OWASP\\_ModSecurity\\_Core\\_Rule\\_Set\\_Project](https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project)

<http://www.modsecurity.org/>

<http://sourceforge.net/projects/mod-security/files/modsecurity-apache/>

### **4.33.2 - Liberando sites no mod\_security**

Após instalar o mod\_security e configurar acontece de barrar o acesso a alguns sites.

Observar os logs

```
tail /var/log/apache2/error.log
```

Criar o arquivo:

```
nano /etc/modsecurity/activated_rules/whitelist.conf
```

Contendo:

```
<LocationMatch "/mail/">  
  SecRuleRemoveById 981059  
  SecRuleRemoveById 981060  
  SecRuleRemoveById 981143
```

```
</LocationMatch>
```

```
<LocationMatch "/familia/administrator">  
    SecRuleRemoveById 981059  
    SecRuleRemoveById 981143  
    SecRuleRemoveById 981060  
</LocationMatch>
```

```
<LocationMatch "/refletindo/administrator">  
    SecRuleRemoveById 981059  
    SecRuleRemoveById 981143  
    SecRuleRemoveById 981060  
</LocationMatch>
```

```
<LocationMatch "/portal/administrator">  
    SecRuleRemoveById 981059  
    SecRuleRemoveById 981143  
    SecRuleRemoveById 981060  
</LocationMatch>
```

Monitorar os logs

```
tail /var/log/apache2/error.log
```

```
tail /var/log/apache2/modsec_audit.log --lines 60 | less
```

```
service apache2 restart
```

Abrir um site por vez e anotar o ID de cada site bloqueado com falso positivo (indevidamente).

# Copiados do howtoforge

```
SecRuleRemoveById 910006 # Google robot activity - Useful in someways but noisy for sites  
where you want them crawled
```

```
SecRuleRemoveById 960015 # Request Missing an Accept Header - Allow for Google Reader
```

Veja que todos do activated\_rules/\*.conf já são incluídos por padrão.

```
<IfModule security2_module>  
    # Default Debian dir for modsecurity's persistent data  
    SecDataDir /var/cache/modsecurity  
  
    # Include all the *.conf files in /etc/modsecurity.  
    # Keeping your local configuration in that directory  
    # will allow for an easy upgrade of THIS file and  
    # make your life easier  
    Include "/etc/modsecurity/*.conf"  
  
    Include "/etc/modsecurity/owasp-crs/activated_rules/*.conf"  
</IfModule>
```

Observar os logs novamente e tentar acessar cada um dos sites.

Cada site bloqueado anote o ID e adicione ao ignorados e então reinicie o Apache.

Assim se vai liberando cada site.

Restartei apache:  
service apache2 restart

### **4.33.3 - Testando segurança de sites**

Chame:

[http://ribafs.org/index.php?secret\\_file=/etc/passwd](http://ribafs.org/index.php?secret_file=/etc/passwd)

Será barrado com o aviso:

Forbidden  
You don't have permission to access / on this server.

-----

Simulação básica de ataque de SQL Injection

<http://ribafs.org/?id=23' or '1'=1>

-----

Criar arquivo:

nano /var/www/teste.php

Contendo:

```
<?php
$arquivo=$_GET['arquivo'];
include($arquivo);
?>
```

Chame pelo navegador assim:

<http://ribafs.org/t.php?arquivo=/etc/passwd>

Aparecerá:

Forbidden

You don't have permission to access /t.php on this server.

----

Variação

Arquivos maliciosos/perigosos

Se a função system estiver liberada e existir o arquivo no servidor.  
teste.php:

```
<?php
// Mostrar somente a linha da senha
system('grep password /var/www/configuration.php');
```

?>

-----

## Testando SQL Injection

Antes de configurar as rules, nós criaremos um script em PHP que é vulnerável por SQL injection e testar.

Note que é apenas um script de login básico. Altere as configurações para a conexão com o banco:

```
nano /var/www/login.php
```

```
<html>
<body>
<?php
    if(isset($_POST['login'])){
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','usuario','senha929292','bancoex');
        $result = mysqli_query($con, "SELECT * FROM `usuarios` WHERE username='$username'
AND password='$password'");
        if(mysqli_num_rows($result) == 0)
            echo 'Invalid username or password';
        else
            echo '<h1>Logged in</h1><p>A Secret for you....</p>';
    }else{
?>
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />
            <input type="submit" name="login" value="Login"/>
        </form>
<?php
    }
?>
</body>
</html>
```

Mostrará um form de login.

Ao entrar as credenciais corretas aparecerá a mensagem "A Secret for you."

Precisamos das credenciais no banco. Crie o banco no MySQL e uma tabela "usuarios" e então insira usuários e senhas.

```
mysql -u root -p
create database bancoex;
use bancoex;
create table usuarios(username VARCHAR(100),password VARCHAR(100));
insert into usuarios values('jesin','pwd');
insert into usuarios values('alice','secret');
quit;
```

Acesse

<http://yourwebsite.com/login.php>

E entre com login e senha.

Username: jesin

Password: pwd

Verá a mensagem indicando sucesso. Agora volte e entre com dados errados -- verá a mensagem de "Invalid username or password".

O script está funcionando corretamente.

Agora vamos tentar pular a página de login com SQL injection. Entre o seguinte no campo username:

```
' or true --
```

Note que existe um espaço após -- não funcionará sem o espaço.

Deixe o campo senha vazio e clique no botão Login.

De forma "inesperada" recebemos a mensagem para usuários autenticados.

## 5.0 - Configurar Apache e PHP

S5.1 - Dar suporte aos arquivos .htaccess

5.2 - Adicionar extensões ao PHP

5.3 - Adicionar um Subdomínio

5.4 - Adicionar um Domínio

5.5 - Proteger alguns diretórios com senha pelo Apache

5.6 - Proteger seções administrador de sites Joomla forçando SSL

### 5.1 - Dar suporte aos arquivos .htaccess

Instalar:

```
apt-get install apache2 apache2-suexec openssl-blacklist apache2-mpm-worker
```

```
nano /etc/apache2/sites-available/default
```

Mudar as duas ocorrências de

AllowOverride None para AllowOverride All

Habilitar o mod\_rewrite

```
a2enmod rewrite
```

```
service apache2 restart
```

No Apache 2.4 precisamos editar o arquivo:

```
nano /etc/apache2/apache.conf
```

### 5.2 - Adicionar extensões ao PHP

```
apt-get install libapache2-mod-php5 php5-gd php5-mysql php5-imap php-pear php-auth php5-ming  
php5-snmp php5-xmldrpc php5-xsl php5-suhosin php5-mcrypt php5-memcache php5-tidy  
php5-xmldrpc php5-xsl php5-xcache php5-curl
```

```
service apache2 restart
```

Criar os domínios no DNS e no Apache (VirtualHost)

domínios e respectivos e-mails - tiagoarts.com com contato e ribafs.org com ribamar e fatima

### **5.3 - Adicionar um Subdomínio**

Criar o Virtual Host no Apache

```
mkdir /var/www/refletindo
```

```
cp /etc/apache2/sites-available/default /etc/apache2/sites-available/refletindo
```

```
nano /etc/apache2/sites-available/refletindo
```

Adicione logo abaixo da linha com ServerAdmin:

```
DocumentRoot /var/www/refletindo
```

```
ServerName refletindo.ribafs.net.br
```

Adicionar /var/www/refletindo nas duas ocorrências

```
a2ensite refletindo
```

```
service apache2 restart
```

Criar arquivo para teste:

```
nano /var/www/refletindo/index.html
```

```
<h1>Refletindo</h1>
```

O site deve ficar na pasta /var/www/refletindo

Adicionar o registro CNAME no DNS:

```
refletindo.ribafs.org CNAME ribafs.org.
```

### **5.4 - Adicionar um Domínio**

Adicionar um Novo Domínio ao mesmo Servidor/droplet

Vou adicionar o domínio tiagoarts.com ao meu servidor. Já tenho o ribafs.org.

Criar o Virtual Host no Apache

Para abrigar mais um domínio: tiagoarts.com

```
mkdir /var/www/tiagoarts.com
```

```
cp /etc/apache2/sites-available/default /etc/apache2/sites-available/tiagoarts.com
```

```
nano /etc/apache2/sites-available/tiagoarts.com
```



Altere o início do arquivo para que fique assim:

```
ServerAdmin ribafs@gmail.com
ServerName tiagoarts.com
ServerAlias tiagoarts.com *.tiagoarts.com
```

```
DocumentRoot /var/www/tiagoarts.com
<Directory />
    Options FollowSymLinks
    AllowOverride All
</Directory>
<Directory /var/www/tiagoarts.com/>
```

...

Troque as ocorrências tiagoarts.com pelo seu domínio.

As demais linhas deixe como estão.

Criar um arquivo provisório para testar:

```
nano /var/www/tiagoarts.com/index.html
</h1>Tiago Arts</h1>
```

```
a2ensite tiagoarts.com
service apache2 restart
```

Envie todo o conteúdo do site para /var/www/tiagoarts.com

DNS

Em sendo um domínio secundário...

No caso do DigitalOcean podemos adicionar este novo domínio usando o painel administrativo.

Caso use um domínio no Registro.br, configure com o DNS deles e adicione os registros.

Caso tenha uma administração de domínio sem opção para adicionar os registros, contate o suporte e peça que façam isso.

## **5.5 - Proteger alguns diretórios com senha pelo Apache**

Proteger diretório com login e senha

Quero proteger o diretório:  
/var/www/livros/cursodejoomla/

Configurar o Apache:  
nano /etc/apache2/sites-available/default

```
AllowOverride All
(All ou AuthConfig )
```

```
cd /var/www/livros/cursodejoomla/  
htpasswd -c .htpasswd loginusuario
```

Criar o /var/www/livros/cursodejoomla/.htaccess

```
AuthType Basic  
AuthName "Restrito"  
AuthUserFile "/var/www/livros/cursodejoomla/.htpasswd"  
Require valid-user  
Order deny,allow  
Deny from all  
<Limit GET HEAD POST>  
Allow from all  
</Limit>
```

Caso precise proteger apenas uma página

```
AuthUserFile /var/www/diretorio2/.htpasswd  
AuthType Basic  
AuthName "Página Protegida por senha"  
<Files "mypage.html">  
  Require valid-user  
</Files>
```

Alterar senha

```
htpasswd -nbm tibafs senha diretorio
```

## **5.6 - Proteger seções administrator de sites Joomla forçando SSL**

Forçar acesso somente com SSL (porta 443):

Adicionar a função ForceHTTPS() logo no início do administrator/index.php:

```
<?php  
/**  
 * @package      Joomla.Administrator  
 * @copyright    Copyright (C) 2005 - 2013 Open Source Matters, Inc. All rights reserved.  
 * @license      GNU General Public License version 2 or later; see LICENSE.txt  
 */  
  
// Set flag that this is a parent file  
define('_JEXEC', 1);  
define('DS', DIRECTORY_SEPARATOR);  
  
function ForceHTTPS() {  
    if ($_SERVER['HTTPS'] != "on") {  
  
        $url = $_SERVER['SERVER_NAME'];
```

```
$new_url = "https://" . $url . $_SERVER['REQUEST_URI'];  
header("Location: $new_url");  
exit;  
}  
}  
ForceHTTPS();  
...
```

Quando não funcionar com \$new\_url = "https://" . \$url . \$\_SERVER['REQUEST\_URI'];  
Usar a URL completa:  
\$new\_url = "https://ribafs.org/portal/administrator";

#### ALERTA

Cuidado quando implementa SSL somente em uma seção do site, pois pode gerar problema de acesso quando acessa o administrator com SSL e depois vai acessar o site com SSL. Vale a pena implementar somente no administrator mas fique atento. O site deve ser acessado sem https, somente com http.

Para acessar o site:

<http://ribafs.org>

<http://familia.ribafs.org>

<http://refletindo.ribafs.org>

Para acessar o administrator

<https://ribafs.org/portal/administrator>

<https://refletindo.ribafs.org/refletindo/administrator/>

<https://familia.ribafs.org/familia/administrator/>



## 6.0 - Criação dos Bancos

6.1 - MySQL

6.2 - PostgreSQL

### 6.1 - MySQL

Caso não tenha instalado o iRedMail, instalar:

```
apt-get install mysql-server mysql-client
```

```
mysql -u root -p  
create database portal;  
create database tfshirts;  
create database admin_demo;  
create database familia;  
create database refletindo;  
FLUSH PRIVILEGES;
```

```
GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'suasenhap' WITH  
GRANT OPTION;
```

```
GRANT ALL PRIVILEGES ON tfshirts.* TO tfshirts@localhost IDENTIFIED BY 'suasenhaf'  
WITH GRANT OPTION;
```

```
GRANT ALL PRIVILEGES ON admin_demo.* TO admin_demo@localhost IDENTIFIED BY  
'suasenhaa' WITH GRANT OPTION;
```

```
GRANT ALL PRIVILEGES ON familia.* TO familia@localhost IDENTIFIED BY 'suasenhaf'  
WITH GRANT OPTION;
```

```
GRANT ALL PRIVILEGES ON refletindo.* TO refletindo@localhost IDENTIFIED BY  
'suasenhaf' WITH GRANT OPTION;
```

```
\q
```

Importar Script:

```
mysql -u root -p banco < banco.sql
```

Exportar banco para script:

```
mysqldump -u root -p banco > banco.sql
```

Abrir o RoundCube e importar o livro de visitas (caso tenha)

## 6.2 - PostgreSQL

apt-get install postgresql

su - postgres

Atribuir senha ao postgres

```
psql
```

```
alter role postgres password 'senhapg3212';
```

```
\q
```

```
exit
```

Exemplo prático de criação de banco, com usuário exclusivo e com acesso via web

Banco - show

Usuário - show, com permissão de conectar (LOGIN)

Senha - show senha

Logar como postgres

```
su - postgres
```

Acessar a console

```
psql
```

Criar usuário show com senha show e permissão de conectar (LOGIN)

```
CREATE ROLE show WITH PASSWORD 'showsenha' LOGIN;
```

Criar banco show tendo como dono o usuário show

```
CREATE DATABASE show OWNER show;
```

ou

```
ALTER DATABASE show OWNER TO show;
```

Conectar ao banco show

```
\c show
```

Criar a tabela perguntas

```
create table perguntas(
```

```
    id serial primary key,
```

```
    grau char(15) not null,
```

```
    materia char(15) not null,
```

```
    ano char(1) not null,
```

```
    assunto char(15) not null,
```

```
    pergunta char(100) not null,
```

```
    alternativa1 char(100) not null,
```

```
    alternativa2 char(100) not null,
```

```
    alternativa3 char(100) not null,
```

```
    alternativa4 char(100) not null,
```

```
    escolhida int not null, -- Alternativa escolhida pelo jogador
```

```
    correta int not null, -- Alternativa correta: 1 a 4
```

```
    nivel char(1) not null, -- A, B, C ou D
```

```
    ajuda text
```

);

Criar a tabela recordes:

```
create table recordes(  
    id serial primary key,  
    nome char(30) not null,  
    pontos int,  
    data timestamp without time zone  
);
```

Alterar as tabelas para terem como dono o usuário show

```
ALTER TABLE perguntas OWNER TO show;  
ALTER TABLE recordes OWNER TO show;
```

Pronto, com isso pode usar este banco com as configurações acima em qualquer aplicativo ou site.

Exportar todos os bancos como script

```
su - postgres  
pg_dumpall > bancos.sql
```

Exportar um único banco

```
pg_dump banco > banco.sql
```

Importar todos os bancos para o banco postgres

```
psql -d postgres -f bancos.sql
```

Importando um único banco

```
psql -d banco -f banco.sql
```

Importando de dentro da console psql

```
\COPY tabela FROM 'script.csv'  
\COPY paises FROM 'paises.csv';
```

Exportando do psql:

```
CREATE TEMP TABLE paises AS SELECT * FROM teste WHERE nome LIKE '%tina%';  
\COPY paises TO '/usr/teste.copy';
```





## 7.0 - Instalar sites e aplicativos, descompactando no /var/www

Do desktop ou de outro servidor enviar para o novo

```
scp -P site1.tar.gz ribafs@ribafs.org:/home/ribafs
```

No novo servidor

```
cd /home/ribafs
```

```
tar xzpvf site1.tar.gz -C /var/www (lembre de compactar incluindo o diretório)
```

Importar os scripts dos bancos nos referidos bancos:

```
mysql -u root -p banco < banco.sql
```

Testar sites e aplicativos para ver se tá tudo OK

Depois de tudo pronto mudar/apontar domínios e aguardar propagação

- Testar domínios

Inicialmente - <http://www.intodns.com/>

Se tudo OK, então testar com:

```
dig dominio.com any e host dominio.com
```

Depois de tudo funcionando e domínios propagados efetuar backup full e enviar para o desktop:

- scripts customizados

- arquivos de sites e aplicativos

- bancos de dados

- arquivos



## 8.0 - Monitorando o servidor

- 8.1 - Monitorando manualmente
- 8.2 - Adicionar Serviços ao Boot num Debian
- 8.3 - Remover serviços do boot
- 8.4 - Desabilitar bluetooth
- 8.5 - Ferramentas para gerenciar serviços no boot
- 8.6 - Monitorando logs com o Logcheck
- 8.7 - Analizar arquivos de log com o logwatch
- 8.8 - Instalar Nagios para Monitorar Servidores
- 8.9 - Melhor visualização dos acessos do Apache com o goaccess
- 8.10 - Deixando a saída dos logs colorida
- 8.11 - Desabilitando o login via SSH de todas as contas
- 8.12 - Monitorando ações dos usuários
- 8.13 - Dividindo a tela em duas
- 8.14 - Usando htop
- 8.15 - Que programas estão usando a banda
- 8.16 - Monitorando a rede
- 8.17 - Gerenciamento de Arquivos
- 8.18 - Usando o cron para executar comandos agendados
- 8.19 - Verificando BlackLists

### 8.1 - Monitorando manualmente

Terá relatórios do Nagios.

Ficará recebendo diariamente um e-mail do logcheck com o relatório de erros nos logs.

Receberá também e-mail de alguns softwares configurados para isso como o mod\_evasive e outros.

É importante executar manualmente alguns softwares como:

- rkhunter
  - rkhunter --update
  - rkhunter --propupd
  - rkhunter --check
  
- tail /var/log/rkhunter.log
- nikto
  - nikto -h ribafs.org
  - nikto -C all -host 200.128.12.34 -o vitima.txt
- psad
  - psad -S
  - tail /var/log/psad
- denyhosts
  - /etc/hosts.allow - permitidos
  - /etc/hosts.deny - negados

- ngrep

```
ngrep -d any port 25
```

- nmap

```
nmap -v -sT localhost
```

```
nmap -v -A dominio.com
```

```
Scannear SYN: nmap -v -sS localhost
```

```
netstat -tulp
```

```
nmap -sTU 10.40.100.123
```

```
lsof -i -n | egrep 'COMMAND|LISTEN|UDP'
```

- arquivos modificados

```
find /var/www -type f -ctime -1 -exec ls -ls {} \;
```

Procurar arquivos com 666

```
find /var/www -xdev -perm +o=w ! \( -type d -perm +o=t \) ! -type l -print
```

Procurar diretórios com 777

```
find /var/www -type d -perm -o+w -exec ls -ld {} \;
```

Procurar contas sem senha

```
awk -F: '($2 == "") {print}' /etc/shadow
```

- Rodar phpsecinfo e desabilitar logo após

- atualizar permissões do /var/www

```
chown -R www-data:www-data /var/www
```

```
find /var/www -type d -exec chmod 2755 {} \;
```

```
find /var/www -type f -exec chmod 0644 {} \;
```

Ou executar o script

- Logs

Apache /var/log/apache2

access.log

error.log

Mail /var/log/

mail.log

mail.err

mail.info

mail.warn

```
tail -f /var/log/mail.log /var/log/iredapd.log /var/log/cbpolicyd.log
```

Clamav /var/log/clamav

clamav.log

freshclam.log

Mysql /var/log/mysql

error.log

Outros /var/log

auth.log

dovecot.log

fail2ban.log

```
iredapd.log
cbpolicyd.log
kern.log
messages
mysql.err
mysql.log
sieve.log
syslog
user.log
```

## **8.2 - Adicionar Serviços ao Boot num Debian**

```
cd /etc/init.d (exemplo)
update-rc.d firewall defaults
```

## **8.3 - Remover serviços do boot**

```
cd /etc/init.d
update-rc.d -f bluetooth remove
```

## **8.4 - Desabilitar bluetooth**

```
nano /etc/rc/local
Adicione ao final, antes de exit 0, a linha:
```

```
echo disable > /proc/acpi/ibm/bluetooth
```

## **8.5 - Ferramentas para gerenciar serviços no boot**

```
sysv-rc-conf - mostra todos os runlevel
reconf - pode alterar, mas mostra poucos
chkconfig - só mostra, não altera
```

```
apt-get install sysv-rc-conf reconf chkconfig
```

Desativar os serviços não usados

## **8.6 - Monitorando logs com o Logcheck**

Lê todo os logs do sistema e de aplicações e envia um e-mail com relatório de anomalias.

aptitude install logcheck

Configurar (e-mail e outras):

```
nano /etc/logcheck/logcheck.conf
```

Frequência em que roda

```
nano /etc/cron.d/logcheck
```

Roda a cada reboot e a cada 2 minutos e envia e-mail para o root:

```
MAILTO=root
```

```
@reboot    logcheck  if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck -R; fi  
2 * * * *  logcheck  if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi
```

Mudar o e-mail, e de 2 minutos para todo dia 1 da manhã:

```
0 1 * * * ...
```

Roda com o próprio usuário:

```
sudo -u logcheck logcheck
```

## **8.7 - Analizar arquivos de log com o logwatch**

Configurações:

```
nano /usr/share/logwatch/default.conf/logwatch.conf
```

Altere:

Set your parameters with this sequence.

```
Output = mail
```

```
Format = html
```

```
MailTo = ribafs@gmail.com
```

```
MailFrom = ribafs@gmail.com
```

```
logwatch | less
```

Aguarde...

Para receber por e-mail um relatório no logwatch dos últimos 7 dias:

```
logwatch --mailto ribafs@gmail.com --output mail --format html --range 'between -7 dias e hoje'
```

Agendando no cron

Você também pode agendar tudo isso no cron para receber um relatório diário. Digite o comando abaixo e adicione a seguinte entrada:

```
crontab -e
```

```
0 2 * * * root logwatch --mailto ribafs@gmail.com
```

## 8.8 - Instalar Nagios para Monitorar Servidores

Instalar Nagios no servidor principal (server) e nos demais (clients)

No servidor

```
dd if=/dev/zero of=/swap bs=1024 count=2097152
mkswap /swap && chown root. /swap && chmod 0600 /swap && swapon /swap
echo /swap swap swap defaults 0 0 >> /etc/fstab
echo vm.swappiness = 0 >> /etc/sysctl.conf && sysctl -p
```

```
apt-get install -y nagios3 nagios-nrpe-plugin
usermod -a -G nagios www-data
chmod -R g+x /var/lib/nagios3/
sed -i 's/check_external_commands=0/check_external_commands=1/g' /etc/nagios3/nagios.cfg
```

```
htpasswd -c /etc/nagios3/htpasswd.users nagiosadmin
service nagios3 restart && service apache2 restart
```

No Cliente

```
apt-get install -y nagios-plugins nagios-nrpe-server
```

```
nano /etc/nagios/nrpe.cfg
```

```
log_facility=daemon
pid_file=/var/run/nagios/nrpe.pid
server_port=5666
nrpe_user=nagios
nrpe_group=nagios
allowed_hosts=198.211.117.129 #(IP do servidor)
dont_blame_nrpe=1
debug=0
command_timeout=60
connection_timeout=300
include=/etc/nagios/nrpe_local.cfg
include_dir=/etc/nagios/nrpe.d/
```

```
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
#command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/simfs
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
```

Verifique com  
df -h

Para ver qual é sua partição principal, aqui foi simfs

```
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/simfs
```

Adicionar ao iptables:

```
iptables -N NRPE
iptables -I INPUT -s 0/0 -p tcp --dport 5666 -j NRPE
iptables -I NRPE -s 198.211.117.129 -j ACCEPT
iptables -A NRPE -s 0/0 -j DROP
/sbin/iptables-save
```

```
service nagios-nrpe-server restart
```

No Servidor

Criar o arquivo:

```
/etc/nagios3/conf.d/ribafs.org.cfg
```

Adicione

```
define host {
    use                generic-host
    host_name          ribafs.org
    alias              ribafs.org
    address            21.129.54.124
}

define service {
    use                generic-service
    host_name          ribafs.org
    service_description PING
    check_command      check_ping!100.0,20%!500.0,60%
}

define service {
    use                generic-service
    host_name          ribafs.org
    service_description SSH
    check_command      check_ssh_port! 65522
    check_command      check_ssh
    notifications_enabled 0
}

define service {
    use                generic-service
    host_name          ribafs.org
    service_description Current Load
    check_command      check_load!5.0!4.0!3.0!10.0!6.0!4.0
}

service nagios3 restart
```



Acessando  
http://IP/nagios3

login - nagiosadmin  
senha - a cadastrada

## **8.9 - Melhor visualização dos acessos do Apache com o goaccess**

```
apt-get install goaccess  
goaccess -b -s -a -f /var/log/apache2/access.log
```

Mudando o número de linhas que retorna com -n  
Por padrão o comando tail, exibe as últimas 10 linhas do arquivo antes de começar a acompanhar os acréscimos. Para alterar este valor, caso você precise que algumas linhas antes sejam exibidas use o parâmetro -n [número de linhas], como no exemplo:

```
tail -n 35 /var/log/apache2/error.log
```

Logs vivos (monitorar em tempo real):

Usando o parâmetro -f é possível manter o tail em loop de forma que quando uma nova linha for adicionada no final do arquivo, ela será automaticamente exibida na tela:

```
tail -f /var/log/arquivo
```

Exemplo:

```
tail -f /var/log/apache2/error.log
```

## **8.10 - Deixando a saída dos logs colorida**

```
aptitude install ccze
```

Usando

```
tail -f /var/log/apache2/error.log | ccze
```

Usuários logados:

```
who
```

Usuário atual

```
whoami
```

## **8.11 - Desabilitando o login via SSH de todas as contas**

exceto do root e usuários com superprivilégios:

Crie o arquivo vazio:

```
touch /etc/nologin
```

Caso queira deixar um aviso a quem tentar logar:

```
sudo sh -c 'echo "Servidor em manutenção. Voltaremos as 1545" > /etc/nologin'
```

Para logar como root, remova:

```
sudo rm /etc/nologin
```

Alterando somente para um certo usuário

```
sudo usermod -s /usr/sbin/nologin username
```

## **8.12 - Monitorando ações dos usuários**

```
sudo less /var/log/auth.log
```

Monitorar últimos acessos

```
last
```

Monitorar últimos usuários que logaram

```
lastlog
```

## **8.13 - Dividindo a tela em duas**

Como dois terminais um acima e outro abaixo com o Splitvt

Divide tela ao meio abrindo dois terminais

Para mudar para cima ou abaixo, clicar com o mouse

A tela ficará dividida em duas. Digite "tty" e aperte [Enter] para ser mostrado o dispositivo correspondente. Você verá que este é um terminal virtual. Alterne de terminal apertando [Ctrl]+[W] e repita o procedimento. O resultado será o mesmo, mudando apenas de número. Para sair aperte [Ctrl]+[O] e então [Q].

Podemos chegar a conclusão de que sobre um terminal real rodavam dois terminais virtuais.

Help  
CTRL+O - h

## **8.14 - Usando htop**

apt-get install htop  
htop

## **8.15 - Que programas estão usando a banda**

apt-get install nethogs

Execute:  
ifconfig para ver as interfaces

nethogs  
nethogs eth0  
nethogs wlan0  
nethogs venet0:0

Listará o uso da banda por IP e serviços

Comandos:  
m - mudar para MB e outras unidades  
r, s, q - sair

## **8.16 - Monitorando a rede**

iptraf - monitorar a rede

apt-get install iptraf

iptraf

netstat -a

netstat -at

netstat -s

df  
df -h

du - mostra todos todos os subdiretórios e seus tamanhos

du -sh (silente e mostrando total do diretório atual em GB)

du -a (tamanhos de cada diretório e cada arquivo)

## **8.17 - Gerenciamento de Arquivos**

ncdu e mc - melhorar o gerenciamento de arquivos

apt-get install mc ncd

mc

ncdu

Memória e Swap

free

free -m

Swap

vmstat

vmstat -S M

vmstat -s -S M

## **8.18 - Usando o cron para executar comandos agendados**

Exemplo

Executar todos os dias as 2 horas e 15 minutos o download do arquivo com wget

```
15 2 * * * wget -c http://sites.com.br/arquivo.zip
```

```
45 19 1,15 * * /usr/local/bin/backup
```

Executar o comando 'backup' todo dia 1 e 15 às 19:45

Um script PHP que executa e fica rodando em segundo plano

```
* * * * /usr/bin/php /var/www/domain.com/backup.php > /dev/null 2>&1
```

Diagrama:

```
m h d m s
```

```
* * * * *
```

+----- minuto (0 - 59)

```
| +----- hora (0 - 23)
| | +----- dia of month (1 - 31)
| | | +----- mês (1 - 12)
| | | | +---- dia da semana (0 - 6) (Sunday=0)
| | | | |
* * * * * comando a ser executado
```

Editar sua agenda  
crontab -e

Listar tarefas agendadas  
crontab -l

Remover agenda  
crontab -r

Enviando saída para o e-mail do usuário que agendou:

```
crontab -e
```

```
SHELL=/bin/bash
PATH=/sbin:/bin/usr/bin
HOME=/home/ribafs
MAILTO="ribafs@gmail.com"
#Isto é um comentário
* * * * echo 'Rodar este comando a cada minuto'
```

Restringindo acesso:

Negar acesso a todos os usuários  
echo ALL >>/etc/cron.deny

Permitir apenas ao ribafs  
echo ribafs >>/etc/cron.allow

Executar um comando a cada reboot

Adicione a linha abaixo ao crontab -e:  
@reboot echo "Sua VPS reiniciou agora: "date

O comando echo "Sua..." será executado a cada reboot e então enviado para o e-mail cadastrado

Detalhes:

<https://www.digitalocean.com/community/articles/how-to-use-cron-to-automate-tasks-on-a-vps>

<http://www.devin.com.br/crontab>

## 8.19 - Verificando BlackLists

Quando um certo IP foi para uma lista negra por engano ou de qualquer forma queremos remover, que procedimentos devemos executar?

Ver a lista do **mod\_evasive**:

```
nano /etc/apache2/mods-available/mod-evasive.conf
```

Ver a lista do **Denyhosts**:

```
nano /etc/hosts.deny
```

Adicionar assim:

```
ALL: 65.61.204.40
```

Ver os Ips barrados pelo **fail2ban**:

```
iptables -L | grep IP
```

## 9.0 – Alguns Comandos Úteis no Linux

Executando comando remoto com SSH:

Vou executar

ls /home/ribafs no servidor ribafs.sub.es

```
ssh -p 65522 ribafs@ribafs.sub.es ls /home/ribafs
```

Reiniciar:

reboot

shutdown -r now

Desligar agora:

shutdown -h now

Adicionar Serviços ao Boot num Debian:

cd /etc/init.d (exemplo)

update-rc.d firewall defaults

Remover serviços do boot

cd /etc/init.d

update-rc.d -f firewall remove

Download no terminal com continuação em caso de queda

wget -c URL

Browser texto

lynx

Versão da distribuição e kernel

uname -r

uname -a

cat /proc/version

ccat /etc/issue

Hardware

cat cpuinfo

free -m

df -h

Tamanho dos arquivos

ls -lh

Processos

ps ax | grep postg

kill -9 PID

dmesg | grep eth0

Restartar serviço sem desrubar-lo

killall -HUP nmbd

## Firewall

iptables -L (ver atividade)

## Informações importantes

ping IP/domínio

## Ver número de linhas no nano

nano -c arquivo

whoami - quem está logado

locate arquivo - localizar

## Atualizar o banco de dados do locate agora:

updatedb

## Compactação

tar xpvf arquivo.tar.gz /diretorio

sudo apt-get install zip

zip -r nome.zip /diretorio

## Descompactar

tar zxpvf arquivo.tar.gz -C /diretorio

unzip nome.zip -d /diretorio

## Arquivos gzip

tar zxpvf nome.gzip

tar zxpvf nome.gzip -C /destino

## Permissões

chmod -R 755 /var/www

## Dono do diretório recursivamente

chown -R www-data /var/www

## Mostrar permissões

ls -la - mostra também arquivos ocultos (iniciados com .)

## Gerenciamento de pacotes

apt-get update

apt-get upgrade

apt-get install nomepacote

aptitude search pacote

apt-get remove --purge pacote (remove inclusive configurações)

apt-get autoclean



## Com arquivos

cat arquivo - ver arq texto  
touch arquivo - criar arquivo vazio

### Listagem com Paginação

more arquivo  
less arquivo.txt  
less é mais flexível, passa e volta

### Acesso remoto seguro

ssh IP/Dominio  
ssh ribafs@IP/dominio  
ssh -p 343 ribafs@IP/dominio

### No Amazon

ssh -p 33322 -i /home/ribafs/ribafs.pem ribafs@ribafs.org

scp arquivo ribafs@ribafs.org:/home/ribafs

scp ribafs@ribafs.org:/home/ribafs/arquivo.zip . (copiar para a pasta atual)

Copiar arquivos daqui para o 192.168.1.105

scp arquivo.zip ribafs@192.168.1.105

Copiar arquivos do 192.168.1.105 para cá, para a pasta atual (veja o ponto ao final):

scp ribafs@192.168.1.105:/home/ribafs .

Para a pasta /tmp

scp ribafs@192.168.1.105:/home/ribafs/arquivo.zip /tmp

Para portas diferentes

scp -P 343 arquivo ribafs@ribafs.org:/home/ribafs

## Portas mais comuns:

HTTP - 80

HTTPS - 443

SSH - 22

FTP - 21

MySQL - 3306

PostgreSQL - 5432

Webmin - 10000

POP3 - 110

SMTP - 25

IMAP - 993



Mostrar somente os exclusivos (sem os repetidos)  
uniq arquivo

Ordenar conteúdo de arquivo  
sort arquivo

Extraindo linhas de arquivos  
grep ban arquivo

vboxmanage | grep delete (procurará por delete na saída do comando vboxmanage)

Opções de grep

c.p = c qualquer letra p

^ - início de linha

\$ - final de linha

\*G - zero ou mais repetições de G

^and - qualquer palavra que inicie com and no início da linha

\$ana - palavras no final da linha terminadas com ana

Expressões Regulares com grep

grep -E '[a-zA-C]' frutas

grep -E '[g-i]' frutas

Trabalhando com campos de Arquivos Texto

-d - mostra o delimitador de caracteres

-f - faixa de caracteres a mostrar

cut -d: -f5,7 /etc/passwd

Retorna algo como: Ribamar FS:/bin/bash

Selecionar Específicos Caracteres em cada linha

cut -c2-4 arquivo

Seleciona os caracteres 2,3 e 4 de cada linha

paste - copia as linhas de vários arquivos e cola os conteúdos num arquivo resultante lado a lado.

paste arquivo1 arquivo2 arquivo3

join - junta os conteúdos de vários arquivos sem repetir colunas

join arquivo1 arquivo2

Sobrescrevendo apenas na tela ocorrências de strings

```
sed 's/banana/rapadura/g' frutas
```

Caso retiremos o g (globalmente) substituirá apenas a primeira ocorrência.

Removendo com confirmação

```
rm -i arquivo
```

```
df -h
```

```
du -sh
```

```
free -m
```

```
find . -name arquivo -exec lpr {} \;
```

```
find . -name arquivo -print
```

```
locate arquivo  
updatedb
```

```
mc
```

```
mcedit
```

```
nano
```

```
gedit
```

Compactando

```
zip -r etc.zip /etc
```

```
unzip etc.zip
```

```
tar xzpvf nome.tar.gz  
tar xzpvf nome.tar.gz -C /destino
```

```
tar zcpvf etc.tar.gz /etc
```

```
bunzip2 nome.tar.bz2
```

```
rar a arquivo.rar arquivo.txt  
rar x arquivo.rar
```

gunzip nome.gz

## Montando Dispositivos

```
mkdir /usb  
fdisk -l
```

```
mount /dev/sdb1 /usb
```

## Imagens com dd

Criando imagem da partição sda1  
dd if=/dev/sda1 of=imagem\_sda1

Montando o arquivo da imagem  
mount imagem\_sda1 /mnt -o loop

## Montando uma imagem ISO

### Criando imagem de CD

```
dd if=/dev/cdrom of=cdimagem.iso
```

Montando a imagem do CD  
mount cdimagem.iso /mnt -o loop

### Gravar diretório num CD

```
genisoimage -J -r -o diretorio.iso /home/ribafs/diretorio/
```

Montando a imagem diretorio.iso  
mount diretorio.iso /mnt -o loop

### Queimando imagem ISO em CD

```
wodim -v -dev=/dev/sr0 speed=16 -dao -data imagem.iso
```

## Ubuntu

Instalar ou desinstalar grupos de pacotes

```
tasksel
```

## Grep Dicas

by Nix Craft

```
grep 'word' filename  
grep 'word' file1 file2 file3  
grep 'string1 string2' filename  
cat otherfile | grep 'something'
```

command | grep 'something'  
command option1 | grep 'data'  
grep --color 'data' fileName  
grep -r 'string' directorio (busca recursiva no distório)

Search /etc/passwd file for boo user, enter:

```
$ grep boo /etc/passwd
```

Sample outputs:

```
foo:x:1000:1000:foo,,,:/home/foo:/bin/ksh
```

You can force grep to ignore word case i.e match boo, Boo, BOO and all other combination with the -i option:

```
$ grep -i "boo" /etc/passwd
```

Use grep recursively

You can search recursively i.e. read all files under each directory for a string "192.168.1.5"

```
$ grep -r "192.168.1.5" /etc/
```

OR

```
$ grep -R "192.168.1.5" /etc/
```

Sample outputs:

```
/etc/ppp/options:# ms-wins 192.168.1.50
```

```
/etc/ppp/options:# ms-wins 192.168.1.51
```

```
/etc/NetworkManager/system-connections/Wired connection
```

```
1:addresses1=192.168.1.5;24;192.168.1.2;
```

You will see result for 192.168.1.5 on a separate line preceded by the name of the file (such as /etc/ppp/options) in which it was found. The inclusion of the file names in the output data can be suppressed by using the -h option as follows:

```
$ grep -h -R "192.168.1.5" /etc/
```

OR

```
$ grep -hR "192.168.1.5" /etc/
```

Sample outputs:

```
# ms-wins 192.168.1.50
```

```
# ms-wins 192.168.1.51
```

```
addresses1=192.168.1.5;24;192.168.1.2;
```

Use grep to search words only

When you search for boo, grep will match fooboo, boo123, barfoo35 and more. You can force the grep command to select only those lines containing matches that form whole words i.e. match only boo word:

```
$ grep -w "boo" file
```

Use grep to search 2 different words

Use the egrep command as follows:

```
$ egrep -w 'word1|word2' /path/to/file
```

Count line when words has been matched

The grep can report the number of times that the pattern has been matched for each file using -c

(count) option:

```
$ grep -c 'word' /path/to/file
```

Pass the -n option to precede each line of output with the number of the line in the text file from which it was obtained:

```
$ grep -n 'root' /etc/passwd
```

Sample outputs:

```
1:root:x:0:0:root:/root:/bin/bash
1042:rootdoor:x:0:0:rootdoor:/home/rootdoor:/bin/csh
3319:initrootapp:x:0:0:initrootapp:/home/initroot:/bin/ksh
```

### Grep invert match

You can use -v option to print inverts the match; that is, it matches only those lines that do not contain the given word. For example print all line that do not contain the word bar:

```
$ grep -v bar /path/to/file
```

### UNIX / Linux pipes and grep command

grep command often used with shell pipes. In this example, show the name of the hard disk devices:

```
# dmesg | egrep '(s|h)d[a-z]'
```

Display cpu model name:

```
# cat /proc/cpuinfo | grep -i 'Model'
```

However, above command can be also used as follows without shell pipe:

```
# grep -i 'Model' /proc/cpuinfo
```

Sample outputs:

```
model          : 30
model name     : Intel(R) Core(TM) i7 CPU    Q 820 @ 1.73GHz
model          : 30
model name     : Intel(R) Core(TM) i7 CPU    Q 820 @ 1.73GHz
```

### How do I list just the names of matching files?

Use the -l option to list file name whose contents mention main():

```
$ grep -l 'main' *.c
```

Finally, you can force grep to display output in colors, enter:

```
$ grep --color vivek /etc/passwd
```

Fonte: <http://www.cyberciti.biz/faq/howto-use-grep-command-in-linux-unix/>





## 10.0 - Testando o Servidor

10.1 - Testando com nmap

10.2 - Outros Testes

### 10.1 - Testando com nmap

Depois de terminar, você pode testar o firewall usando o Nmap, a partir de outro micro da rede local ou da internet, para procurar vulnerabilidades. O Nmap é um pacote bastante popular. No Debian você pode instalá-lo pelo apt-get.

Caso a regra que bloqueia tudo esteja ativa, você vai ter o seguinte como resultado:

```
nmap -sS -v 192.168.0.33
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-03 10:12 BRT
Host 192.168.0.33 appears to be down, skipping it.
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.053 seconds
```

Ou seja, o Nmap não consegue sequer perceber que o PC está realmente lá, e avisa: "Se você realmente tem certeza que ele está online, experimente usar a opção -P0", o que não vai mudar muita coisa:

```
# nmap -P0 -v 192.168.0.33
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-03 10:14 BRT
Host 192.168.0.33 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.0.33 at 10:14
The SYN Stealth Scan took 1361 seconds to scan 1659 ports.
All 1659 scanned ports on 192.168.0.33 are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 1360.579 seconds
```

Como todas as portas estão em modo drop, onde o firewall simplesmente descarta os pacotes sem confirmar o recebimento, o teste demora muito tempo, quase 27 minutos para escanear apenas as primeiras 1659 portas. Uma varredura completa, em todas as 65 mil portas, levaria 17 horas e meia, isso executando o teste via rede local. Via internet, a varredura levaria vários dias e, mesmo assim, só apareceriam as portas manualmente abertas no seu script.

tcpdump: Monitorando conexões

Autor: Leandro Nascimento Souza <minimediale@gmail.com>

Data: 11/04/2007

tcpdump: Monitorando conexões

O tcpdump é um dos mais, se não o mais "famoso" sniffer para sistemas GNU/Linux. Com ele podemos realizar análises de redes e solucionar problemas. Sua utilização é simples e sem mistérios, bastando apenas ter os conhecimentos básicos de redes TCP/IP. Esta dica é apenas uma

introdução deste sniffer, maiores informações e documentação à seu respeito podem ser encontradas em seu site oficial:

<http://www.tcpdump.org>

A instalação do tcpdump em sistemas Debian é super simples, bastando executar o comando abaixo como super usuário (root):

```
# apt-get install tcpdump
```

Para iniciarmos a utilização do tcpdump precisamos especificar a interface de rede que queremos analisar com o parâmetro -i seguido da interface desejada, por exemplo, se quisermos analisar todo o tráfego que passa pela interface eth0, executaríamos a seguinte linha de comando:

```
# tcpdump -i eth0
```

Conexões de origem podem ser monitoradas utilizando o parâmetro src host, um exemplo simples seria monitorarmos o tráfego que vem de 192.168.0.9 para nosso computador, com o ip 192.168.0.2. A linha de comando ficaria da seguinte forma:

```
# tcpdump -i eth0 src host 192.168.0.9
```

Se quisermos monitorar as conexões especificando um host de destino, poderíamos fazê-lo com o parâmetro dst host, o exemplo abaixo mostra todo o tráfego do host 192.168.0.2 com 192.168.0.1, no caso, 192.168.0.1 é nosso gateway.

```
# tcpdump -i eth0 dst host 192.168.0.1
```

Com tcpdump também podemos especificar exceções com o parâmetro not host, por exemplo, em nosso servidor queremos ver todo o tráfego que se passa em sua interface, exceto o de 192.168.0.8, faríamos da seguinte forma:

```
# tcpdump -i eth0 not host 192.168.0.9
```

No tcpdump podemos também especificar portas de origem e destino com os comandos src port e dst port, um exemplo seria monitorarmos o tráfego destinado à porta 80 (http), para isso utilizaríamos a linha de comandos abaixo e navegaríamos em um site qualquer:

```
# tcpdump -i eth0 dst port 80
```

Para verificarmos o tráfego da porta de origem 32881 por exemplo, faríamos da seguinte forma:

```
# tcpdump -i eth0 src port 32881
```

Muitas opções avançadas podem ser obtidas com o tcpdump, essas são algumas opções básicas, porém fundamentais para quem quer aprender sobre sniffers.

<http://www.vivaolinux.com.br/dica/tcpdump-Monitorando-conexoes>

Nmap - Combinações para um bom scan

Autor: Daniel Romero <[infoslack@gmail.com](mailto:infoslack@gmail.com)>

Data: 04/01/2007

Nmap - Combinações para um bom scan

Bem, como a maioria conhece ou já ouviu falar, o nmap é o melhor scan da atualidade. Abaixo vou citar alguns comandos e as combinações que mais utilizo, me ajuda bastante. =)

```
# nmap -sTUR -O -v -p 1-65535 -P0 hostname.domain
```

Explicando o comando acima:

- s => scan type (tipo de scaneamento)
- T => utiliza o protocolo TCP
- U => utiliza o protocolo UDP
- R => utiliza o protocolo RPC
- O => tenta descobrir o sistema operacional
- v => verbose mode
- p => escaneia as portas de 1 a 65535
- sS => ativa o scan escondido, Scan Stealth

OBS: Sistemas que tiverem algum tipo de firewall instalado farão, na maioria das vezes, que o scan não seja efetuado ou que ele demore muito para terminar.

Continuando a explicação de cada opção...

Para fazer o scan de uma maneira mais rápida, substituímos o -p pela flag -F (default). Essa flag fará o scan somente das portas privilegiadas (0-1023) e nas portas mais usadas em serviços conhecidos (1024-49,151). Isso pode ser bem útil ao invés de passar por todas as 65.535 portas!

-P0 => Essa opção diz ao nmap para não pingar o host de destino. Isso é útil também quando se faz um scan em uma máquina que possua firewall. Se o firewall bloqueia pacotes ICMP (o que, pessoalmente, não acho uma boa idéia), o nmap nem vai rodar sobre o host.

A combinação mais viável acaba ficando assim:

```
# nmap -sS -O -P0 -v hostname.domain
```

Espero que isso ajude alguém. =)

<http://www.vivaolinux.com.br/dica/Nmap-Combinacoes-para-um-bom-scan>

NMAP

```
nmap -sTUR -O -v -p 1-65535 -P0 ribafs.org
```

```
nmap -O -v localhost
```

SirBagda – Guia do Nmap

Descrição:

O Nmap foi desenhado para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais.

O que são portas:

Imagine que as duas partes do endereço IP (a parte referente à rede e a parte referente ao host) correspondem ao CEP da rua e ao número do prédio. Um carteiro só precisa destas duas informações para entregar uma carta. Mas, dentro do prédio moram várias pessoas. O CEP e número do prédio só vão fazer a carta chegar até a portaria. Daí em diante é preciso saber o número do apartamento. É aqui que entram as famosas portas TCP.

Existem 65.536 portas TCP, numeradas de 0 a 65535. Cada porta pode ser usada por um programa ou serviço diferente, de forma que em teoria poderíamos ter até 65536 serviços diferentes ativos simultaneamente em um mesmo servidor, com um único endereço IP válido. O endereço IP contém o CEP da rua e o número do prédio, enquanto a porta TCP determina a que sala dentro do prédio a carta se destina.

Além das 65.536 portas TCP, temos o mesmo número de portas UDP, seu protocolo irmão. Embora seja um protocolo menos usado que o TCP, o UDP continua presente nas redes atuais pois oferece uma forma alternativa de envio de dados, onde em vez da confiabilidade é privilegiada a velocidade e a simplicidade. Ambos trabalham em conjunto com o IP, que cuida do endereçamento.

As portas:

21 TCP: FTP – O FTP é um dos protocolos de transferência de arquivos mais antigos e ainda assim um dos mais usados.

22 TCP: SSH – O SSH é o canivete suíço da administração remota em servidores Linux.

23 TCP: Telnet – O Telnet é provavelmente o protocolo de acesso remoto mais antigo.

25 TCP: SMTP – O SMTP é o protocolo padrão para o envio de e-mails.

53 UDP: DNS – Os servidores DNS são contatados pelos clientes através da porta 53, UDP.

67 e 68 TCP: Bootps e Bootpc – Estes dois protocolos podem ser usados em sistemas de boot remoto, onde os clientes não possuem HD nem CD-ROM e acessam todos os arquivos de que precisam a partir do servidor.

69 UDP: TFTP – O TFTP é uma versão simplificada do FTP, que utiliza portas UDP para a transferência dos dados.

80 TCP: HTTP – O HTTP é o principal protocolo da Internet, usado para acesso às páginas web.

110 TCP: POP3 – Servidores de e-mail, como o Postfix, armazenam os e-mails recebidos em uma pasta local.

123 UDP: NTP – O NTP (Network Time Protocol) é o protocolo usado para sincronizar o relógio em relação a outras máquinas da rede ou da Internet.

137 UDP, 138 UDP e 139 TCP: NetBIOS – Estas três portas são usadas pelo protocolo de compartilhamento de arquivos e impressoras em redes Microsoft.

143 TCP: IMAP – O IMAP é mais um protocolo para recebimento de e-mails, assim como o POP3.

177 TCP: XDMCP – O XDMCP é um protocolo de acesso remoto, suportado nativamente pelo X (o ambiente gráfico usado no Linux e em outros sistemas Unix).

389 TCP: LDAP – O LDAP é muito usado atualmente para criar servidores de autenticação e definir permissões de acesso para os diferentes usuários da rede.

443 TCP: HTTPS – O HTTPS permite transmitir dados de forma segura, encriptados usando o SSL.  
445 TCP: CIFS - O protocolo CIFS é uma versão atualizada do antigo protocolo NetBIOS, usado para a navegação e acesso a compartilhamentos em redes Windows.

Veja uma enorme lista das portas TCP/UDP e junto os trojans que atuam nas portas (em inglês):  
[Somente usuários registrados podem ver os Links. Clique aqui para se REGISTRAR]

Nmap mais que um scanner de portas:

Além da tabela de portas interessantes, o Nmap pode fornecer informações adicionais sobre os alvos, incluindo nomes de DNS reverso, possível sistema operacional, tipos de dispositivos e endereços MAC.

Sinopse:

nmap -Tipo de Scan –Opções -Especificação do alvo

Tipo de Scan & Opções:

Scan em massa:

-iL <arquivodeentrada>

Especifica um arquivo com uma lista de IP's para ser escaneado.

-iR <número de hosts>

Sorteia IP's e começa a escanea. Você deve determinar o número de host que deseja escanar para não para digite 0 (zero).

--exclude <host1[,host2][,host3],...>

Especifica uma lista de alvos, separados por vírgula, a serem excluídos do scan mesmo que façam parte da faixa de rede especificada.

--excluídefile <arquivo\_exclusão>

Oferece a mesma funcionalidade que a opção --exclude, exceto que os alvos a excluir são fornecidos em um <"arquivo separado">.

Descobrimo Hosts:

-sL (Scan Listagem)

O scan listagem é uma forma degenerada de descoberta de hosts que simplesmente lista cada host da rede especificada, sem enviar nenhum pacote aos hosts-alvos.

-sP (Scan usando Ping)

Esta opção diz ao Nmap para somente executar um scan usando o ping (descoberta de hosts), e então mostrar os hosts disponíveis que responderam ao scan.

-P0 (Sem ping)

Considera todos os IP's como online e tenta fazer sondagens agressivas.

-PS/PA/PU[listadeportas] (Ping usando TCP SYN)

Envia um pacote TCP SYN / ACK ou UDP vazio. Por padrão é enviado é enviado na porta 80, mas você pode alterar usando vírgulas (ex. -PS22, 23, 25, 80, 113, 1050, 35000), nesse caso as sondagens serão tentadas contra cada porta em paralelo.

-PE/PP/PM (Tipos de Ping do ICMP)

Envia um pacote ICMP echo request do tipo 8 (ou também timestamp, e netmask) esperando como resposta um tipo 0 echo reply. (Obs: não entendo nada disso).

-PR (Ping usando ARP)

O scan ARP encarrega o Nmap e seus algoritmos otimizados de fazer as requisições ARP.

-n (Não faça resolução DNS)

Diz ao Nmap para nunca fazer uma resolução DNS. Uma vez que o DNS é normalmente lento, isso acelera as coisas.

-R (resolução DNS para todos os alvos)

Diz ao Nmap para sempre fazer uma resolução DNS.

--system-dns (Usa a resolução DNS do sistema)

Especifique esta opção se desejar utilizar a resolução DNS do seu sistema. A resolução DNS do sistema é sempre usada em escaneamento IPv6.

--dns-servers <servidor1[,servidor2],...> (Servidores a utilizar para a pesquisa DNS reversa)

Opcionalmente você pode usar esta opção para especificar servidores de DNS alternativos.

Escaneamento de Portas:

-sS (scan TCP SYN)

O scan SYN é o tipo de escaneamento padrão do Nmap. Ele também permite uma diferenciação limpa e confiável entre os estados aberto (open), fechado (closed), e filtrado (filtered).

-sT (scan TCP connect)

O scan TCP connect é o scan padrão do TCP quando o scan SYN não é uma opção. Esse é o caso quando o usuário não tem privilégios para criar pacotes em estado bruto ou escanear redes IPv6.

-sU (scans UDP)

Mesmo sendo mais usado o protocolo TCP o Nmap tem uma opção de scan de protocolo UDP. Ele pode ser combinado com um tipo de escaneamento TCP como o scan SYN (-sS) para averiguar ambos protocolos na mesma execução.

-sN/sF/sX (scans TCP Null, FIN, e Xmas)

Esses três tipos de scan exploram uma brecha sutil na RFC do TCP para diferenciarem entre portas abertas e fechadas.

scan Null (-sN)

Não marca nenhum bit (o cabeçalho de flag do tcp é 0)

scan FIN (-sF)

Marca apenas o bit FIN do TCP.

scan Xmas(-sX)

Marca as flags FIN, PSH e URG, iluminando o pacote como uma árvore de Natal.

-sA (scan TCP ACK)

Ele nunca determina se uma porta está aberta (ou mesmo aberta|filtrada). Ele é utilizado para mapear conjuntos de regras do firewall, determinando se eles são orientados à conexão ou não e quais portas estão filtradas.

-sW (scan da Janela TCP)

Scan da Janela é exatamente o mesmo que o scan ACK, exceto que ele explora um detalhe da implementação de certos sistemas de forma a diferenciar as portas abertas das fechadas.

-sM (scan TCP Maimon)

A técnica é exatamente a mesma que os scans Null, FIN e Xmas, exceto que a sondagem é FIN/ACK. De acordo com a RFC 793 (TCP), um pacote RST deveria ser gerado em resposta a tal sondagem se a porta estiver aberta ou fechada. Entretanto, Uriel Maimon notou que muitos sistemas derivados do BSD simplesmente descartavam o pacote se a porta estivesse aberta.

--scanflags (scan TCP Personalizado)

A opção --scanflags permite que você desenhe seu próprio scan permitindo a especificação de flags TCP arbitrárias. Experimente algumas combinações de URG, ACK, PSH, RST, SYN, e FIN (ex. --scanflags URGACKPSHRSTSYNFIN) marca tudo, embora não seja muito útil para escaneamento.

-sI <hostzumbi[ortadesondagem]> (scan Idle)

Funciona como um proxy para fazer o scan (veja mais em português: [Somente usuários registrados podem ver os Links. Clique aqui para se REGISTRAR]).

-sO (Scans do protocolo IP)

Scans do Protocolo IP permitem que você determine quais protocolos IP (TCP, ICMP, IGMP, etc.) são suportados pela máquina-alvo.

-b <host para relay de ftp> (Scan de FTP bounce)

Isso permite que um usuário conecte-se a um servidor FTP, e então solicite que arquivos sejam enviados a um terceiro servidor.

Especificação de Portas e Ordem de Scan:

-p <faixa de portas> (Escaneia apenas as portas especificadas)

Esta opção especifica quais portas que você deseja escanear e prevalece sobre o padrão.

-F (Scan Rápido (portas limitadas))

Especifica que você deseja apenas escanear as portas listadas no arquivo nmap-services que vem com o nmap.

-r (Não usa as portas de forma aleatória)

Essa técnica de busca aleatória normalmente é desejável, mas você pode especificar -r para um escaneamento de portas sequencial.

Detecção de Serviço e Versão e SO:

-A

Para habilitar tanto a detecção de SO como a detecção de versão.

-sV

Habilita a detecção de versão.

--allports

Não exclui nenhuma porta da detecção de versão.

-O

Habilita a detecção de SO.

### **Enganando o Firewall/IDS**

-S <Endereço\_IP> (Disfarça o endereço de origem)

Em algumas circunstâncias o Nmap pode não conseguir determinar o seu endereço de origem (o Nmap irá dizer se for esse o caso). Nesta situação use o -S com o endereço IP da interface que deseja utilizar para enviar os pacotes.

-e <interface> (Usa a interface especificada)

Diz ao Nmap qual interface deve ser utilizada para enviar e receber pacotes.

--spooof-mac <endereço mac, prefixo, ou nome do fabricante> (Disfarça o endereço MAC)

Solicita ao Nmap que utilize o endereço MAC informado para todos os frames ethernet em estado bruto (raw) que ele enviar.

Estados das portas:

Aberto (open)

Filtrado (filtered)

Fechado (closed)

Não-filtrado (unfiltered)

Aberto (open) significa que uma aplicação na máquina-alvo está escutando as conexões/pacotes naquela porta.

Filtrado (filtered) significa que o firewall, filtro ou outro obstáculo de rede está bloqueando a porta de forma que o Nmap não consegue dizer se ela está aberta (open) ou fechada (closed).

Fechadas (closed) não possuem uma aplicação escutando nelas, embora possam abrir a qualquer instante.

Não filtradas (unfiltered) quando elas respondem às sondagens do Nmap, mas o Nmap não consegue determinar se as portas estão abertas ou fechadas.

O Nmap reporta as combinações aberta|filtrada (open|filtered) e fechada|filtrada (closed|filtered) quando não consegue determinar quais dos dois estados descrevem melhor a porta.

Sites Utilizados:

Site GuiadoHardware

Nmap.Org [Somente usuários registrados podem ver os Links. Clique aqui para se REGISTRAR]

Última edição por JeanM; 20-10-2009 às 13:45..

<http://forum.guiadohacker.com.br/showthread.php?t=3510>

Exemplos

Aqui estão alguns exemplos de utilização do Nmap, desde o simple e rotineiro, até o um pouco mais complexo e esotérico. Alguns endereços IP reais e nomes de domínio foram utilizados para tornar as coisas mais concretas. Nesses lugares você deve substituir os endereços/nomes pelos da sua própria rede. Embora eu não ache que o escaneamento de portas de outras redes seja, ou deva ser considerado, ilegal alguns administradores de rede não apreciam o escaneamento não-solicitado de suas redes e podem reclamar. Obter a permissão antecipadamente é a melhor opção.



Para fins de teste, você tem permissão para escanear o host `scanme.nmap.org`. Esta permissão inclui apenas o escaneamento via Nmap e não tentativas de explorar vulnerabilidades ou ataques de negação de serviço (denial of service). Para preservar a banda, por favor não inicie mais do que uma dúzia de scans contra o host por dia. Se esse serviço de alvo livre para escaneamento for abusado, será derrubado e o Nmap irá reportar `Failed to resolve given hostname/IP: scanme.nmap.org`. Essas permissões também se aplicam aos hosts `scanme2.nmap.org`, `scanme3.nmap.org`, e assim por diante, embora esses hosts ainda não existam.

```
nmap -v scanme.nmap.org
```

Esta opção escaneia todas as portas TCP reservadas na máquina `scanme.nmap.org`. A opção `-v` habilita o modo verboso (verbose).

```
nmap -sS -O scanme.nmap.org/24
```

Inicia um scan SYN camuflado contra cada máquina que estiver ativa das 255 possíveis da rede "classe C" onde o Scanme reside. Ele também tenta determinar qual o sistema operacional que está rodando em cada host ativo. Isto requer privilégio de root por causa do scan SYN e da detecção de SO.

```
nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
```

Inicia uma enumeração de hosts e um scan TCP na primeira metade de cada uma das 255 sub-redes de 8 bits possíveis na classe B do espaço de endereçamento 198.116. Também testa se os sistemas estão executando sshd, DNS, pop3d, imapd ou a porta 4564. Para cada uma destas portas encontradas abertas, a detecção de versão é usada para determinar qual aplicação está executando.

```
nmap -v -iR 100000 -P0 -p 80
```

Pede ao Nmap para escolher 100.000 hosts de forma aleatória e escaneá-los procurando por servidores web (porta 80). A enumeração de hosts é desabilitada com `-P0` uma vez que enviar primeiramente um par de sondagens para determinar se um hosts está ativo é um desperdício quando se está sondando uma porta em cada host alvo.

```
nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20
```

Este exemplo escaneia 4096 endereços IP buscando por servidores web (sem usar o ping) e grava a saída nos formatos XML e compatível com o programa grep.

## NMAP - A flag completa

Aprenda um pouco mais sobre o NMAP, essa poderosa ferramenta de portscan muito utilizada no sistema operacional linux.

Como todos sabem, o nmap é o mais famoso portscan existente hoje. (<http://www.insecure.org/nmap>). É uma ótima ferramenta para administradores, para descobrir portas abertas em seu sistema, e possivelmente acusar alguma vulnerabilidade no mesmo.

Só que também é muito utilizado por hackers, para descobrir falhas no sistema, em portas abertas desnecessariamente.

Estava estudando alguns comandos do nmap, com algumas referências do "Building Secure Servers

with Linux" (O'Reilly), e achei uma tag fenomenal:

```
# nmap -sTUR -O -v -p 1-65535 -P0 hostname.domain
```

Bom, agora, explicando:

-sTUR --> este é o scan type. Eu utilizei os 3 protocolos disponíveis (Tcp, Udp e Rpc) Tem a opção de se usar o -sS somente, para fazer o "Scan Stealth"

-O --> tenta descobrir o sistema operacional

-v --> verbose mode

-p 1-65535 --> varrer todas as portas

Ai é que está a sacada ! Essa flag diz para o NMAP realizar o scan em TODAS as 65535 portas disponíveis. Bom, isso é que me complicou um pouco ...

Se você rodar o NMAP com essa flag em um sistema que estiver com firewall, pode esperar BASTANTE, porque o scan é bem lento ... eu fechei todas as portas da minha máquina, deixando somente alguns poucos serviços rodando (samba, www, ntp, ).

```
# nmap -sTUR -O -p 1-65535 -P0 matrix
```

O tempo total de scan foi de 192'47" !!! Mais de 3 horas !!!

Fora que o /var/log/messages ficou enorme!

Para fazer o scan de uma maneira mais rápida, substituímos o -p pela flag -F (default) Essa flag fará o scan somente nas portas privilegiadas (0-1023) e nas portas mais usadas em serviços conhecidos (1024-49,151). Isso pode ser bem útil ao invés de passar por todas as 65.535 portas!

-P0 --> Essa opção diz ao nmap para não pingar o host de destino. Isso é útil, também, quando se faz um scan em uma máquina que possua firewall. Se o firewall bloqueia pacotes ICMP (o que, pessoalmente, não acho uma boa ideia), o nmap nem vai rodar sobre o host. Fora que o ping gera um pequeno delay.

Agora, a flag mais usual acaba sendo essa:

```
# nmap -sS -O -P0 -v localhost
```

```
Starting nmap 3.27 ( www.insecure.org/nmap/ )
Host localhost (127.0.0.1) appears to be up ... good.
Initiating SYN Stealth Scan against localhost (127.0.0.1) at 20:09
Adding open port 515/tcp
Adding open port 22/tcp
Adding open port 13/tcp
Adding open port 9/tcp
Adding open port 587/tcp
Adding open port 80/tcp
Adding open port 5432/tcp
Adding open port 3306/tcp
```

Adding open port 37/tcp  
Adding open port 631/tcp  
Adding open port 25/tcp  
The SYN Stealth Scan took 1 second to scan 1623 ports.  
For OSScan assuming that port 9 is open and port 1 is closed and neither are firewalled  
Interesting ports on localhost (127.0.0.1):  
(The 1612 ports scanned but not shown below are in state: closed)  
Port State Service  
9/tcp open discard  
13/tcp open daytime  
22/tcp open ssh  
25/tcp open smtp  
37/tcp open time  
80/tcp open http  
515/tcp open printer  
587/tcp open submission  
631/tcp open ipp  
3306/tcp open mysql  
5432/tcp open postgres  
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20  
Uptime 0.110 days (since Thu Sep 11 17:31:26)  
TCP Sequence Prediction: Class=random positive increments  
Difficulty=4383797 (Good luck!)  
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 5.860 seconds

Esse texto é de autoria de Alessandro Luiz Petrocino  
<http://www.sputnix.com.br/tutoriais/seguranca/nmap-a-flag-completa/>

Tutorial: Usando o nmap para verificação de vulnerabilidades  
postado em Março 14, 2013 by Hernane Carvalho

Olá a todos mais uma vez

Desta vez gostaria de mostrar pra vocês como usar o nmap para checar a existência da vulnerabilidade MS08-067, para quem não conhece essa vulnerabilidade pode ser explorada pelo Worm Conficker. Algumas ferramentas como Metasploit também podem ser usadas para explorar essa vulnerabilidade, basta usar o seguinte comando:

```
nmap --script smb-check-vulns.nse -p445 <host> (No de um host alvo apenas)
```

```
"nmap -PN -T4 -p139,445 -n -v --script=smb-check-vulns --script-args  
safe=1 [target networks] (No caso de escanear todo um segmento de rede)"
```

A resposta será algo parecido com isso informando se o alvo é vulnerável ou não

```
Host script results:  
| smb-check-vulns:  
| MS08-067: NOT VULNERABLE  
| Conficker: Likely CLEAN
```

- | regsvc DoS: regsvc DoS: NOT VULNERABLE
- | SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
- | MS06-025: NO SERVICE (the Ras RPC service is inactive)
- | MS07-029: NO SERVICE (the Dns Server RPC service is inactive)

Caso vc encontre uma máquina vulnerável vc pode explorar essa falha usando essa dica aqui

<http://hernaneac.net/2012/11/28/explorando-vulnerabilidades-usando-metasploit-framework/>

## Nmap Network Scanning

### Usage and Examples

Prev Chapter 8. Remote OS Detection Next

### Usage and Examples

The inner workings of OS detection are quite complex, but it is one of the easiest features to use. Simply add `-O` to your scan options. You may want to also increase the verbosity with `-v` for even more OS-related details. This is shown in Example 8.1.

Example 8.1. OS detection with verbosity (`-O -v`)

```
# nmap -O -v scanme.nmap.org
```

Starting Nmap ( <http://nmap.org> )

Nmap scan report for scanme.nmap.org (74.207.244.221)

Not shown: 994 closed ports

| PORT      | STATE    | SERVICE     |
|-----------|----------|-------------|
| 22/tcp    | open     | ssh         |
| 80/tcp    | open     | http        |
| 646/tcp   | filtered | ldp         |
| 1720/tcp  | filtered | H.323/Q.931 |
| 9929/tcp  | open     | nping-echo  |
| 31337/tcp | open     | Elite       |

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6.39

OS details: Linux 2.6.39

Uptime guess: 1.674 days (since Fri Sep 9 12:03:04 2011)

Network Distance: 10 hops

TCP Sequence Prediction: Difficulty=205 (Good luck!)

IP ID Sequence Generation: All zeros

Read data files from: /usr/local/bin/./share/nmap

Nmap done: 1 IP address (1 host up) scanned in 5.58 seconds

Raw packets sent: 1063 (47.432KB) | Rcvd: 1031 (41.664KB)

Including the `-O -v` options caused Nmap to generate the following extra line items:

Device type

Example 8.2. Using version scan to detect the OS

```
# nmap -sV -O -v 129.128.X.XX
```

Starting Nmap ( <http://nmap.org> )

Nmap scan report for [hostname] (129.128.X.XX)

Not shown: 994 closed ports

| PORT      | STATE    | SERVICE      | VERSION                         |
|-----------|----------|--------------|---------------------------------|
| 21/tcp    | open     | ftp          | HP-UX 10.x ftpd 4.1             |
| 22/tcp    | open     | ssh          | OpenSSH 3.7.1p1 (protocol 1.99) |
| 111/tcp   | open     | rpc          |                                 |
| 445/tcp   | filtered | microsoft-ds |                                 |
| 1526/tcp  | open     | oracle-tns   | Oracle TNS Listener             |
| 32775/tcp | open     | rpc          |                                 |

No exact OS matches for host

TCP Sequence Prediction: Class=truly random  
Difficulty=9999999 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: HP-UX

<http://nmap.org/book/osdetect-usage.html>

## **10.2 - Outros testes**

Testando portas abertas

Testando com telnet

Por exemplo: na dúvida se uma máquina está conectando ao mysql em outra:

```
telnet IPouDominioMaquinaremota 3306
```

Ele te dirá algo.

Se disser que não tem rota

Testando rotas

```
route -n
```

Testar sintaxe do Apache

```
apache2ctl configtest
```

Teste de Portas Abertas

```
iptables -L
```

```
iptables -L | grep 80
```

```
netstat -lutan
```

```
netstat -lute
```

```
telnet localhost porta
```

Testando as portas com nc  
nc -v -w 2 localhost -z 1-65535  
v - verbose  
w - segundos

nc -l 3333  
nc 192.168.0.1 3333 (conectar ao servidor)  
nc localhost 80  
nc -z 192.168.1.103 80-9000

Descobrir Função dos Serviços Instalados

whatis nomeserviço

whatis apache2

Testando se o servidor está no ar, caso não esteja, a máquina é desligada  
Esta é uma dica sobre um script que faz o teste de comunicação com o servidor ou qualquer outra máquina na rede.

Ele testa a comunicação com o servidor, caso o servidor esteja online, ele permanece no ar, caso ocorra o contrário, o servidor não responde, a máquina é automaticamente desligada.

```
#!/bin/bash
echo "Teste de Comunicação com o Servidor"
if ! ping -c 3 IPdoServidor >/dev/null; then
    echo "Servidor down!!!"
    shutdown -h 5
else
    echo "Servidor up!!!"
    exit 1
fi
exit
http://www.vivaolinux.com.br/dica/Testando-se-o-servidor-esta-no-ar-caso-nao-esteja-a-maquina-e-desligada
```

Testando um servidor web usando o telnet (Apache, HTTPd, IIS e outros)

Autor: Fábio Berbert de Paula <[fberbert@gmail.com](mailto:fberbert@gmail.com)>

Data: 01/08/2008

Testando um servidor web usando o telnet (Apache, HTTPd, IIS e outros)

Este é um recurso muito útil, já usei muito, passei um tempo sem precisar e quando precisei não lembrava mais como fazer, tendo que buscar no Google para lembrar da sintaxe correta novamente. Então aqui vai a documentação no VOL para eu saber onde procurar quando precisar, e claro, para ajudar a quem venha a precisar.

Exemplo: estou num terminal e quero saber se o Viva o Linux está no ar.

```
$ telnet www.vivaolinux.com.br 80
```

```
Trying 76.74.236.7...
Connected to vivaolinux.com.br.
Escape character is '^]'.
GET /index.php HTTP/1.1
Host: www.vivaolinux.com.br
[ENTER]
quit
```

O resultado será o código-fonte HTML da página inicial do VOL. Auto-explicativo, não?

80 é a porta padrão do servidor web.

Essa mesma teoria se aplica a outros tipos de serviço, tais como (e principalmente) smtp e pop. Em outra dica mostro como fazer.

Um abraço.

[http://www.vivaolinux.com.br/dica/Testando-um-servidor-web-usando-o-telnet-\(Apache-HTTPd-II-S-e-outros\)](http://www.vivaolinux.com.br/dica/Testando-um-servidor-web-usando-o-telnet-(Apache-HTTPd-II-S-e-outros))

Como testar se uma estação está acessando um servidor interna ou externamente?

Usando o ping

```
ping www.servidor.com.br
```

```
host www.servidor.com.br
```

Ou

```
dig www.servidor.com.br
```





## **11.0 - Ferramentas Úteis**

11.1 - Testando desempenho de grandes servidores

11.2 - Varrendo uma rede com Wireshark

11.3 - Instalar o webmin

### **11.1 - Testando desempenho de grandes servidores**

Uma ferramenta free – Jmeter

```
apt-get install jmeter
```

Tutorial

<http://www.linuxdescomplicado.com.br/2013/12/saiba-como-testar-o-desempenho-dos.html>

### **11.2 - Varrendo uma rede com Wireshark**

O Wireshark é uma ferramenta com muitos recursos e disponível para Linux e Windows. É uma ferramenta gráfica para instalar no desktop.

```
apt-get install wireshark
```

### **11.3 - Instalar o webmin**

Caso não tenha muita necessidade do webmin, é prudente deixar ele inacessível. Mantenha a porta 10000 bloqueada e libere somente quando quiser usar.

Para ajudar a gerenciar o site remotamente.

Adicionar o repositório abaixo:

```
nano /etc/apt/sources.list
```

```
## Repositório Debian Sarge para instalação do Webmin
```

```
deb http://download.webmin.com/download/repository sarge contrib
```

```
wget http://www.webmin.com/jcameron-key.asc
```

```
apt-key add jcameron-key.asc
```

```
apt-get update
```

```
apt-get install webmin
```

Acesse com:

```
https://IP:10000
```

Libere a porta

```
nano /etc/default/iptables
```

```
-A INPUT -p tcp --dport 10000 -j ACCEPT
```

```
/etc/init.d/iptables restart
```

## 11.4 - Logrotate

Tutorial: Usando o logrotate

Por Diego Queiroz dos Santos

08/02/2009

Um bom tutorial de Diego Queiroz, que vai nos falar mais sobre o logrotate.

logrotate é designado para facilitar a administração de sistemas que criam grande quantidade de logs. Ele rotaciona, compacta, remove e ainda envia notificações por e-mail. Cada "logfile" pode ser manuseado diariamente, semanalmente, mensalmente ou quando o arquivo tornar-se muito grande.

Clique no link abaixo para ler a notícia na íntegra!

Normalmente, o logrotate roda diariamente com o processo cron. Ele não vai alterar um registro mais que uma vez em um dia a menos que o critério para que o log seja baseado no tamanho do arquivo, assim o logrotate será executado mais de uma vez por dia, ou a menos o -f ou -force seja usado.

Opções para chamar o logrotate:

-d - Liga o modo debug.

-f, --force - Diz para o logrotate forçar a rotação

-m, --mail <comando> - Diz ao logrotate qual comando usar para mandar emails. O comando aceita dois argumentos: 1) O assunto da mensagem, e 2) o destinatário.

-s, --state <statefile> - Diz ao logrotate para usar um arquivo de state alternativo.

-v, --verbose - Ativa o modo verbose

Arquivo de configuração: /etc/logrotate.conf

O arquivo de configuração funciona com chamadas globais e chamadas locais, sendo que as locais sobrescrevem as globais. Os comentários são feitos com um # seguido de um espaço em branco. Lembrando que algumas definições podem ser setadas no global. Veja o exemplo:

```
/var/log/mail.log {  
rotate 5  
mail shaamangra@gmail.com  
size 1M  
postrotate
```

```
if [ -f /var/run/sendmail ]; then
/etc/init.d/sendmail restart > /dev/null
fi
endscript
}
```

O arquivo /var/log/mail.log vai ser rotacionado 5 vezes, sendo que o limite para cada arquivo é de 1024k. O postrotate diz que vai ser executado tais comandos APÓS o log ser rotacionado. Logo depois vai ser mandado um email para shaamangra@gmail.com.

Opções do logrotate:

compress - Arquivos devem ser compactados  
compresscmd - Especifica o comando a ser usado para compactar. O padrão é gzip.  
uncompresscmd -Especifica o comando a ser usado para descompactar. O padrão é gunzip  
compressext - Especifica a extensão usada nos logfiles  
compressoptions - Opções usadas pelo compactador  
copy - Faz uma copia do log, mas não muda o original. Essa opção pode user usada para fazer um snapshot do arquivo atual.  
create modo dono grupo - Imediatamente após a rotação, depois do script postrotate rodar, o arquivo é criado com o mesmo nome do arquivo principal. Modo especifica as permissões, dono o dono do arquivo e grupo o grupo do dono do arquivo.  
daily - Arquivos são rotacionados diariamente  
dateext - usa AAAA MM DD para datas.  
ifempty - rotaciona os arquivos mesmo que esteja vazio.  
include arquivo ou diretório - Lê o arquivo ou diretório como parte da configuração.  
mail endereço - Quando um log é rotacionado, é mandado um email para o endereço.  
missinok - Se o log estiver faltando, vá para o próximo sem me alertar com uma mensagem de erro.  
nomissinok - Contrário de missionok  
monthly - arquivos rotacionados mensalmente  
nocompress - não compacta  
nocopy - contrário de copy  
nomail - contrário de mail  
notifempty - contrário de ifempty  
noolddir diretório - Logs são movidos para o diretório para rotação. O diretório deve ser o mesmo physical device.  
postrotate/endscript - As linhas entre postrotate e endscrip são executadas APÓS do log ser rotacionado  
prerotate/endscript - As linhas entre prerotate e endscrip são executadas ANTES do log ser rotacionado.  
rotate X - Arquivos são rotacionados X vezes antes de ser mandado email ou arquivo ser removido.  
size - size[G|M|k] - Arquivos são rotacionados quando chega ao tamanho especificado  
wekley - logs são rotacionados semanalmente

Espero ter ajudado em algo.

Abraço a todos !!

<http://www.fug.com.br/content/view/556/60/>

Outros bons:

<https://www.digitalocean.com/community/articles/how-to-manage-log-files-with-logrotate-on-ubuntu-12-10>

<http://www.thegeekstuff.com/2010/07/logrotate-examples/>

## **12.0 - Dicas Extras**

- 12.1 - Exportar livro de endereços do Gmail para ser importado no RoundCube
- 12.2 - Firewall Básico com UFW
- 12.3 - Dicas para promover seu site
- 12.4 - Codificação de Caracteres
- 12.5 - Instalação e Configurações do Tomcat7
- 12.6 - Tuning do Apache
- 12.7 - DNS Free
- 12.8 - Erro comum no SSH
- 12.9 - Script para redirecionamento de página

### ***12.1 - Exportar livro de endereços do Gmail para ser importado no RoundCube***

Quem usa o e-mail do Gmail tem um grande livro de endereços, contendo todos os e-mails de quem enviou para você e dos que você enviou.

Estes e-mails podem ser úteis se for usar o RoundCube, pois ele também completa os e-mails quando vamos criar um e-mail.

Para exportar o Livro no Gmail

- Abra o Gmail
- Acima e à esquerda clique na combo Gmail – Depois clique em Contatos
- Clique acima na combo Mais – Depois em Exportar...
- Selecione o formato vCard e clique em Exportar

Importar no WebMmail RoundCube

- Abra seu webmail no Roundcube
- Clique acima e à direita em Catálogo de Endereços
- Clique em Importar
- Clique em Selecionar arquivo e Selecione o arquivo exportado do Gmail
- Clique em Importar e aguarde

Agora quando criar um novo e-mail, ao iniciar a digitação no campo Para, ele irá auto-completando para você.

### ***12.2 - Firewall Básico com UFW***

Quando instalamos o iRedMail ele usa como firewall o IPTables e é interessante nos adaptarmos ao mesmo e continuar usando. Caso contrário precisaremos efetuar todas as configurações do firewall por nós. Eu preferi manter. Mesmo que um tutorial no Ocean sugira que não usemos o firewall do iRedMail mas nosso próprio. Tive problemas e então mantive o do iRedMail.

Mas se resolver usar seu próprio firewall abaixo segue um tutorial sobre o UFW do Ubuntu, que realmente simplifica este trabalho.

Antes de usar um firewall precisamos ter em mente ou anotadas as portas que iremos liberar e as

que precisaremos redireccionar/forward.

community documentation: <https://help.ubuntu.com/community/UFW>

server guide: <https://help.ubuntu.com/10.04/serverguide/C/firewall.html>

ufw manual: <http://manpages.ubuntu.com/manpages/lucid/en/man8/ufw.8.html>

project wiki: <https://wiki.ubuntu.com/UncomplicatedFirewall>

nice article: <http://savvyadmin.com/ubuntu-ufw/>

Firewall no Ubuntu

Usage: ufw COMMAND

Commands:

|                        |                                     |
|------------------------|-------------------------------------|
| enable                 | Enables the firewall                |
| disable                | Disables the firewall               |
| default ARG            | set default policy to ALLOW or DENY |
| logging ARG            | set logging to ON or OFF            |
| allow deny RULE        | allow or deny RULE                  |
| delete allow deny RULE | delete the allow/deny RULE          |
| status                 | show firewall status                |
| version                | display version information         |

sudo ufw logging on

sudo su

apt-get install ufw

Habilitando

ufw enable

Status

ufw status

ufw status verbose

Configurando os defaults (fecha todas as entradas e abre todas as saídas):

Fecha todas as portas de intradas

sudo ufw default deny incoming

Abrindo todas de saídas

sudo ufw default allow outgoing

Send mais restritivo (fechando as saídas):

sudo ufw default deny outgoing

Abrir somente as desejadas

ufw allow 80 ufw allow 443 ufw allow 22

sudo aptitude install -y ufw

sudo ufw enable

Mostrar comandos

```
sudo ufw show
```

Mostrar estado (ativo/inativo):

```
sudo ufw status
```

```
sudo ufw allow <port>/<optional: protocol>
```

```
sudo ufw allow ssh
```

```
sudo ufw allow http
```

Ou

```
sudo ufw allow 22/tcp
```

```
sudo ufw allow 22/udp
```

```
sudo ufw allow 80
```

```
sudo ufw deny from 209.51.172.195
```

Lista de serviços

```
sudo ufw app list
```

```
less /etc/services
```

Habilitar logs

```
sudo ufw logging on
```

Desabilitar

```
sudo ufw logging off
```

Permitir pacotes de 207.46.232.182:

```
sudo ufw allow from 207.46.232.182
```

Permitir Sub-rede Específica

Você pode usar uma máscara de sub-rede:

```
sudo ufw allow from 192.168.1.0/24
```

Permitir por Porta e IP Específicos

```
sudo ufw allow from <endereço IP> to <protocolo> port <número da porta>
```

Exemplo: permitir acesso do endereço IP 192.168.0.4 à porta 22 para todos os protocolos:

```
sudo ufw allow from 192.168.0.4 to any port 22
```

Permitir por Porta, Endereço IP e Protocolo Específico

```
sudo ufw allow from <endereço ip> to <protocolo> port <número da porta> proto <nome do protocolo>
```

Exemplo: permitir acesso do endereço 192.168.0.4 à porta 22 usando TCP:

```
sudo ufw allow from 192.168.0.4 to any port 22 proto tcp
```

```
sudo ufw deny from 192.168.0.1 to any port 22
```

```
sudo ufw deny from 192.168.0.7 to any port 22
```

```
sudo ufw allow from 192.168.0.0/24 to any port 22 proto tcp
```

Faixas:

```
sudo ufw allow 1000:2000/tcp
```

Excluindo regras

```
sudo ufw delete allow 80/tcp
```

```
sudo ufw delete allow 1000:2000/tcp
```

Resetar todas as regras e voltar tudo ao default:

```
sudo ufw reset
```

Routing and NAT

```
nano /etc/default/ufw
```

Mudar DEFAULT\_FORWARD\_POLICY para "ACCEPT"

```
nano /etc/ufw/sysctl.conf
```

Descomentar /net/ipv4/ip\_forward=1

```
nano /etc/ufw/before.rules
```

Adicionar:

```
# nat Table rules
```

```
*nat
```

```
:POSTROUTING ACCEPT [0:0]
```

```
# Forward traffic from eth1 through eth0.
```

```
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
```

```
# don't delete the 'COMMIT' line or these nat table rules won't be processed
```

```
COMMIT
```

Para habilitar Port Forwarding adicione, trocando [portNumber]:

```
-A PREROUTING -i eth1 -p tcp --dport 3389 -j DNAT --to 192.168.139.101:[portNumber]
```

Outra:

```
sudo ufw allow proto tcp from 192.168.1.100 to any port 22
```

Ver a construção:

```
sudo ufw --dry-run allow http
```



## 12.3 - Dicas para promover seu site

Pagerank

<http://www.marketingdebusca.com.br/pagerank/>

Divulgando seu blog: Comentários em outros blogs

Neste novo artigo da série Divulgando seu blog, tratarei dos comentários feitos em outros blogs, que é uma ótima forma de divulgar seu trabalho, atraindo visitantes para seu blog, desde que ela seja bem feita. Além disso, essa ação tem outros objetivos importantes:

É uma forma de reconhecer o bom trabalho de quem tem o mesmo trabalho que você para manter um blog.

Cria relacionamento com outras pessoas que passam pelas mesmas situações que você. Como em qualquer outra área da vida, esse “network” é importante e deve ser cultivado, pois essas pessoas podem ajudá-lo futuramente – ou vice-versa.

Você consegue links para o seu site e isso é importante para os mecanismos de busca. O Google e outros buscadores usam esses links como um dos fatores para “pontuar” e “classificar” seu site. De forma simplificada, quanto mais links você tem, melhor pontuado será seu site. Este item só é válido para blogs que não estejam com o recurso do “nofollow” ativado para os comentários. Para saber mais sobre isso, leia o artigo O que é Nofollow?.

Vamos às dicas:

Procure blogs relacionados ao mesmo tema do seu. Normalmente, os visitantes desses blogs são as pessoas que se interessam pelo assunto que você trata, e é neles que você deve concentrar seus comentários. Há diversas formas de encontrar blogs relacionados: no Google, no “blogroll” (lista de blogs) de outros blogs e mesmo nos comentários de blogs que você já visita.

Para facilitar o acompanhamento desses blogs, utilize o recurso do RSS. Isso evita a necessidade de ter que entrar em todos os blogs todos os dias para saber se foi colocada um novo post. Existem hoje muitas ferramentas gratuitas que simplificam o trabalho de acompanhamento de RSS, como o Internet Explorer e o Windows Live Mail. Particularmente, optei pelo Google Reader que, além de ter uma interface simples, possibilita o acompanhamento a partir de qualquer computador. Outra vantagem do Google Reader: você não precisa saber o endereço do feed de RSS. Ao adicionar uma inscrição, basta digitar o endereço do blog (por exemplo, [www.tdseries.com.br](http://www.tdseries.com.br)), que ele já encontra o feed automaticamente.

Leve a sério o comentário que você está fazendo. Pense nele como se fosse um post de seu próprio blog e tenha os mesmos cuidados com o conteúdo, a ortografia, a gramática etc.

Leia o post que está comentando antes de escrever sobre ele. Pode parecer óbvio, mas há pessoas que não se dão o trabalho de ler o post antes de escrever.

Ao escrever, tenha em mente que seu comentário deve estar relacionado ao que foi postado. Não use o comentário apenas para fazer propaganda de seu blog (“Olá, visite meu blog!”). Elogie ou critique o post, concorde ou discorde com o que foi escrito. Assim, o autor do post (ou os visitantes do blog) se interessarão pelo que você escreveu e sentirão curiosidade em conhecer mais sobre seu

trabalho.

Normalmente, os blogs dão várias opções para você se identificar. A dica óbvia: nunca comente como “anônimo”. Além de não levar ao seu objetivo de divulgação, muitos autores apagam esses comentários. A “Conta do Google” não costuma ser uma boa alternativa também, já que o link será criado para o seu perfil, e não para o seu blog. As melhores opções costumam ser o “OpenID” ou o “Nome/URL”, pois quem clicar no seu nome será direcionado diretamente para o seu blog.

Comente sempre. O ideal é que você escreva diversos comentários diariamente, desde que siga as orientações anteriores. Isso dá trabalho, mas o resultado a longo prazo compensa.

Para ter sucesso na obtenção de parcerias, cito algumas dicas importantes:

Cuide de seu blog - Antes de sair pelo mundo buscando parcerias, cuide de seu blog. Da mesma forma que na vida real, você está vendendo um produto e precisa torná-lo atraente para seus clientes potenciais. Com certeza, antes de outra pessoa aceitar sua parceria, ela visitará seu blog, para analisar se a troca valerá a pena. Escolha um template interessante e capriche nos posts.

Acumule conteúdo - Também antes de propor uma parceria, acumule conteúdo em seu blog. Quanto menos conteúdo você tiver, menor a chance de conseguir uma parceria. É sabido que muitos blogs são abandonados pelos seus proprietários antes mesmo de completar um mês de existência. Assim, vale a pena fazer seu “dever de casa”, preparando uma boa quantidade de posts de qualidade, antes de se oferecer a outros blogs.

Tenha bom senso – A parceria precisa ser boa para ambos os blogs. Se você está começando agora, dificilmente conseguirá parceria com um blog que já tem centenas de visitas diárias, porque esse blog teria pouco ou nenhum benefício. Assim, procure quem está também começando agora, pois a parceria beneficiará a ambos. Com o tempo, você estará apto a buscar parcerias maiores.

Procure blogs com mesmo tema – Normalmente, é mais fácil conseguir parcerias em blogs que tratem de assuntos similares ao seu. Isso porque o visitante desse site normalmente se interessará também pelo seu conteúdo.

Procure seus amigos – No início, você terá mais dificuldades em encontrar quem queira fazer parceria com você. Por isso, é normal recorrer aos amigos que já tenham blog. A amizade pode contar pontos nessa hora e ajudar na aprovação.

Cuidado com suas escolhas – Da mesma forma que uma parceria pode beneficiá-lo, ela também pode prejudicá-lo. Dependendo do assunto de seu blog, você pode não querer vê-lo associado à pirataria, pornografia ou conteúdo ilegal. Sempre digo isso, mas não é uma crítica: se você tem um site com esse conteúdo, é normal buscar parceria em sites similares.

Não peça a parceria em comentários – Embora muitos façam isso, é deselegante colocar um post no blog desejado solicitando a parceria. É mais “profissional”, por assim dizer, entrar em contato direto com o dono do blog, solicitando a parceria. Normalmente, os blogs possuem uma área para contato ou trazem o e-mail do proprietário. Quando for escrever, tenha novamente em mente a imagem do produto que você quer vender: indique seu endereço, descreva seu blog, fale sobre como a parceria trará benefício mútuo.

Seja moderado – Um blog com dezenas de links de “parceiros” nem sempre é um bom blog. Assim, seja seletivo e só faça parcerias com blogs que realmente lhe trarão benefício.

Isso tudo dito, um último alerta: a troca de links não é vista com bons olhos por todos. Existem blogueiros conceituados que insistem que só precisa pedir links quem não tem um bom blog. Um bom artigo tratando sobre isso pode ser lido em <http://viamaolotado.com/parcerias-entre-blogs/>. Leia e tome sua própria decisão.

### Divulgação do novo feed em seu blog

A forma mais direta e simples, é colocar um link em seu blog para que as pessoas possam ver e assinar seu feed. O ideal é você colocar um link em local de fácil acesso, logo no início de preferência, justamente para chamar a atenção. O link chamará mais atenção caso seja acompanhado pela figura que identifica o RSS. Fazendo uma busca pelo Google, é fácil encontrar diversas imagens gratuitas para esse fim. Lembre-se de colocar o endereço de seu novo feed criado acima.

Caso ainda tenha dúvidas, uma dica é criar um “gadget” de HTML e colocar um código similar ao abaixo, adaptando-o para sua necessidade:

```
<a href="http://feeds2.feedburner.com/GerenciandoBlog" target="_blank">  
 </a>
```

Se você preferir, pode utilizar também o código gerado pelo próprio FeedBurner. Isso é feito na aba “Publicize”, opção “Chicklet Chooser”. Você seleciona a opção desejada, e o código HTML é mostrado numa caixa no final da página.

### Notificação por e-mail

Outra opção interessante na área de “Publicize” é a geração de um código para permitir aos seus leitores cadastrarem seu e-mail para receberem as atualizações de seu blog. Isso é feito na opção “Email Subscriptions”.

Para ativar esse recurso, basta clicar no botão “Activate”, e você será levado para uma área onde irá configurá-lo. Lá, você deve escolher o idioma em que o form de inscrição será mostrado. Basta copiar o código HTML e copiá-lo para sua página. Caso seja usuário do Blogger, você pode escolher essa opção na caixa “Use as a widget in”, e o trabalho será feito automaticamente.

Você pode unir as duas únicas dicas em um único controle HTML, e ter um resultado como o seguinte:

### RSS

#### Receba atualizações por e-mail

Para ter esse efeito, o código utilizado foi o abaixo (que você precisa adaptar para o seu próprio feed):

```
<a href="http://feeds2.feedburner.com/GerenciandoBlog" target="_blank">  
 </a><br/>  
<a href="http://feedburner.google.com/fb/a/mailverify?uri=GerenciandoBlog&loc=pt_BR" target="_blank">Receba atualizações por e-mail</a>
```

Dica para saber quantos e quais sites estão linkando o seu. Faça uma busca no Google assim:

link: seusite.com.br

## 12.4 - Codificação de Caracteres

Um probleminha chato em sites e aplicativos web é a codificação de caracteres errada. Quando acessamos um site e ele mostra vários caracteres estranhos onde deveria ter um acento.

Isso pode ser contornado pedindo ao navegador que mostre outra codificação, geralmente UTF-8 ou ISO-8859-1.

Mas para uma solução definitiva, que deve vir do site e não do cliente, para prevenir problemas de codificação em páginas, adicione na página a linha respectiva da linguagem que está usando, veja:

HTML

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
```

XML ou JavaScript ou AJAX

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

ASP:

```
<% Response.Charset="ISO-8859-1" %>
```

PHP:

```
<?php header("Content-Type: text/html; charset=UTF-8",true) ?>
```

JSP:

```
<%@ page contentType="text/html; charset=ISO-8859-1" %>
```

## 12.5 - Instalação e Configurações do Tomcat7

```
apt-get update  
apt-get upgrade
```

```
apt-get install tomcat7  
apt-get install tomcat7-docs tomcat7-admin tomcat7-examples tomcat7-user
```

```
/etc/init.d/tomcat7 stop
```

```
nano /var/lib/tomcat7/conf/tomcat-users.xml
```

Adicione as linhas abaixo logo acima de </tomcat-users>

```
<role rolename="manager-gui"/>  
<role rolename="manager-script"/>  
<role rolename="admin"/>  
<role rolename="manager"/>  
<role rolename="tomcat"/>  
<user username="tomcat" password="senhatomcat"  
roles="manager-gui,admin-gui,manager,admin,manager-script,admin-script"/>
```

```
nano /etc/default/tomcat7
```

Adicione ao final:

AUTHBIND=yes

Alterar Porta, se necessário, no arquivo:  
nano /etc/tomcat7/server.xml

Na linha:

```
<Connector port="8080" protocol="HTTP/1.1"
```

```
/etc/init.d/tomcat7 restart
```

Testar com:

```
http://localhost:8080/manager/html
```

Login – tomcat Senha - senhatomcat

Detalhes: <http://www.debianadmin.com/how-to-setup-apache-tomcat-55-on-debian-etch.html>

Bom tutorial

<https://www.digitalocean.com/community/articles/how-to-install-apache-tomcat-on-ubuntu-12-04>

## 12.6 - Tuning do Apache

As configurações de tuning do Apache2 estão totalmente ligadas a quantidade de recursos ( CPU, memória e banda ) disponíveis:

Por exemplo para um servidor QuadCore com 8 GB e um link de 5Mb eu recomendo a seguinte configuração:

```
nano /etc/apache2/apache2.conf
```

```
<IfModule mpm_prefork_module>
  StartServers      15
  MinSpareServers   10
  MaxSpareServers   40
  MaxClients        256
  MaxRequestsPerChild 1000
</IfModule>
```

#Este não altera

```
<IfModule mpm_worker_module>
  StartServers      2
  MinSpareThreads   25
  MaxSpareThreads   75
  ThreadLimit       64
  ThreadsPerChild   25
  MaxClients        150
  MaxRequestsPerChild 0
</IfModule>
```

```
<IfModule mpm_event_module>
  StartServers      2
  MaxClients        150
```

```
MinSpareThreads 25
MaxSpareThreads 75
ThreadLimit 64
ThreadsPerChild 250
MaxRequestsPerChild 0
</IfModule>
```

Descrição de cada diretiva:

StartServers – Configura o número de processos filhos criados na inicialização ( Recomendado deixar o valor padrão )

MinSpareServers – Número mínimo de processos que não manipulam requisições. ( Recomendado deixar o valor padrão )

MaxSpareServers – Número máximo de processos que não manipulam requisições. ( Recomendado deixar o valor padrão )

ServerLimit – Valor máximo da diretiva MaxClients. ( Deve ser igual ou superior ao MaxClients )

MaxClients – Número máximo de conexões simultâneas. ( Varia de acordo com os recursosdisponíveis )

MaxRequestsPerChild – Limite de requisições que um processo filho poderá manipular. ( 0 significa ilimitado )

Dica Importante: Para testes de benchmark do Apache2 recomendo o uso do AB ( Apache Benchmark )

Configuração

/etc/apache2/conf.d

Algumas sugestões

Para melhorar a segurança do Apache2, abra o arquivo

nano /etc/apache2/conf.d/security

e altere as seguintes opções:

```
ServerSignature off
```

```
ServerTokens Prod
```

Explicando:

\* ServerSignature off -> Desabilita as mensagens de informação do servidor;

\* ServerTokens Prod -> Desabilita o envio de Tokens HTTP;

\* TraceEnable off -> Desabilita o parâmetro utilizado para teste e diagnósticos.

<http://www.vivaolinux.com.br/dica/Seguranca-no-Apache>

```
<IfModule Mod_Security.c> # Activamos el Mod_Security
```

```
SecFilterEngine On
```

```
# Escanear el contenido de la petición POST
```

```
SecFilterScanPOST On
```

```
# Escanear la respuesta de la petición (si se quiere evitar mostrar ciertos mensajes de error)
```

```
SecFilterScanOutput On
```

```
# Chequear codificación URL
```

SecFilterCheckURLEncoding On

# Chequear Codificación Unicode  
SecFilterUnicodeEncoding On

#Esta opción debe estar activada solo si la Aplicación utiliza codificación Unicode.  
#En cualquier otro caso puede interferir con la operatoria normal del sitio web.  
SecFilterCheckUnicodeEncoding Off

#Permitir solo cierto valores de los bytes.  
#Hay que tener en cuenta cuales son los caracteres que se utilizan en nuestro sistema.  
#En este caso estamos permitiendo todos  
SecFilterForceByteRange 1 255

#Loguear peticiones, solo las invalidas, para posterior análisis.  
SecAuditEngine RelevantOnly

#Ubicación de los ficheros de logs.  
SecAuditLog logs/audit\_log

#Por defecto, denegar las peticiones con mensaje de estado "500".  
SecFilterDefaultAction "deny,log,status:500"

# REGLAS

# De aquí en adelante irán las reglas que queremos aplicar, para proteger nuestra  
# aplicación.

#Con esta directiva cambiaremos la identificación de la versión del Servidor Web.  
#Nuestro servidor se identificará como si fuera un "Microsoft IIS/1.0"  
SecServerSignature "Microsoft IIS/1.0"  
SecServerResponseToken Off

# Aquí evitaremos ataques simples de XSS  
SecFilter "<(.\n)+>"  
SecFilter "<[:space:]]\*script"

#SQL Injection  
SecFilter "delete[:space:]]+from"  
SecFilter "insert[:space:]]+into"  
SecFilter "select.+from"  
SecFilter ".\*[%;\"]+.\*"

#Controlo el Campo Nombre del Formulario para que no sea mayor a 6 caracteres,  
#protección contra #Buffer Overflow, si nuestro parámetro "nombre" es vulnerable.  
SecFilterSelective ARG\_nombre ".{6,}" "redirect:http://www.google.es"

#Nuestra aplicación es muy compleja y depende del RegisterGlobals, pero hay un  
#formulario de autenticación que se puede saltar enviando la variable valido=1 o ok=1  
SecFilterSelective "ARG\_valido|ARG\_ok" "1"

#Controlamos que se envíen los dos cabezeras (HTTP\_USER\_AGENT y HTTP\_HOST) en las

```
#peticiones generalmente los atacantes y algunas herramientas de escaneo
#no enviaran estas cabezeras.
SecFilterSelective "HTTP_USER_AGENT| HTTP_HOST" "^$"

# Prohibimos subir ficheros
SecFilterSelective "HTTP_CONTENT_TYPE" multipart/form-data)"
# Si alguien quiere acceder a /admin/administrar.php lo redirigimos a www.google.com
Secfilter "/admin/administrar.php" redirect:http://www.google.com

#Regla que controla la respuesta del servidor web, supongamos que hay un error en
#el código de la aplicación que nos da el famoso error del SQLServer exponiendo
#la consulta que ha fallado, pues con esta regla podemos hacer que devuelva una
#página de error controlada.
SecFilterSelective OUTPUT "ODBC SQL Server Driver"
redirect:http://www.mypage.com/error.php

</IfModule>
```

## 10 Tips to Secure Your Apache Web Server on UNIX / Linux

by Ramesh Natarajan on March 22, 2011

Ver módulos instalados  
apache2 -l

### 3. Restrict access to root directory (Use Allow and Deny)

Secure the root directory by setting the following in the httpd.conf

```
<Directory />
  Options None
  Order deny,allow
  Deny from all
</Directory>
```

In the above:

- \* Options None – Set this to None, which will not enable any optional extra features.
- \* Order deny,allow – This is the order in which the “Deny” and “Allow” directives should be processed. This processes the “deny” first and “allow” next.
- \* Deny from all – This denies request from everybody to the root directory. There is no Allow directive for the root directory. So, nobody can access it.

### 4. Set appropriate permissions for conf and bin directory

bin and conf directory should be viewed only by authorized users. It is good idea to create a group, and add all users who are allowed to view/modify the apache configuration files to this group.

Let us call this group: apacheadmin

Create the group.



```
groupadd apacheadmin
```

Allow access to bin directory for this group.

```
chown -R root:apacheadmin /usr/local/apache2/bin  
chmod -R 770 /usr/local/apache2/bin
```

Allow access to conf directory for this group.

```
chown -R root:apacheadmin /usr/local/apache2/conf  
chmod -R 770 /usr/local/apache2/conf
```

Add appropriate members to this group. In this example, both ramesh and john are part of apacheadmin

```
# vi /etc/group  
apacheadmin:x:1121:ramesh,john
```

## 5. Disable Directory Browsing

If you don't do this, users will be able to see all the files (and directories) under your root (or any sub-directory).

For example, if they go to `http://{your-ip}/images/` and if you don't have an `index.html` under images, they'll see all the image files (and the sub-directories) listed in the browser (just like a `ls -l` output). From here, they can click on the individual image file to view it, or click on a sub-directory to see its content.

To disable directory browsing, you can either set the value of `Options` directive to "None" or "-Indexes". A - in front of the option name will remove it from the current list of options enforced for that directory.

Indexes will display a list of available files and sub-directories inside a directory in the browser (only when no `index.html` is present inside that folder). So, Indexes should not be allowed.

```
<Directory />  
Options None  
Order allow,deny  
Allow from all  
</Directory>
```

(or)

```
<Directory />  
Options -Indexes  
Order allow,deny  
Allow from all  
</Directory>
```

## 6. Don't allow .htaccess

Using `.htaccess` file inside a specific sub-directory under the `htdocs` (or anywhere outside), users can

overwrite the default apache directives. On certain situations, this is not good, and should be avoided. You should disable this feature.

You should not allow users to use the .htaccess file and override apache directives. To do this, set “AllowOverride None” in the root directory.

```
<Directory />  
Options None  
AllowOverride None  
Order allow,deny  
Allow from all  
</Directory>
```

## 7. Disable other Options

Following are the available values for Options directive:

- \* Options All – All options are enabled (except MultiViews). If you don’t specify Options directive, this is the default value.
- \* Options ExecCGI – Execute CGI scripts (uses mod\_cgi)
- \* Options FollowSymLinks – If you have symbolic links in this directory, it will be followed.
- \* Options Includes – Allow server side includes (uses mod\_include)
- \* Options IncludesNOEXEC – Allow server side includes without the ability to execute a command or cgi.
- \* Options Indexes – Disable directory listing
- \* Options MultiViews - Allow content negotiated multiviews (uses mod\_negotiation)
- \* Options SymLinksIfOwnerMatch – Similar to FollowSymLinks. But, this will follow only when the owner is same between the link and the original directory to which it is linked.

Never specify ‘Options All’. Always specify one (or more) of the options mentioned above. You can combine multiple options in one line as shown below.

Options Includes FollowSymLinks

The + and – in front of an option value is helpful when you have nested directories, and would like to overwrite an option from the parent Directory directive.

In this example, for /site directory, it has both Includes and Indexes:

```
<Directory /site>  
Options Includes Indexes  
AllowOverride None  
Order allow,deny  
Allow from all  
</Directory>
```

For /site/en directory, if you need Only Indexes from /site (And not the Includes), and if you want to FollowSymLinks only to this directory, do the following.

```
<Directory /site/en>  
Options -Includes +FollowSymLink  
AllowOverride None
```

```
Order allow,deny
Allow from all
</Directory>
```

- \* /site will have Includes and Indexes
- \* /site/en will have Indexes and FollowSymLink

## 8. Remove unwanted DSO modules

If you have loaded any dynamic shared object modules to the apache, they'll be present inside the httpd.conf under "LoadModule" directive.

Please note that the statically compiled apache modules will not be listed as "LoadModule" directive.

Comment out any unwanted "LoadModules" in the httpd.conf

```
grep LoadModule /usr/local/apache2/conf/httpd.conf
```

## 9. Restrict access to a specific network (or ip-address)

If you want your site to be viewed only by a specific ip-address or network, do the following:

To allow a specific network to access your site, give the network address in the Allow directive.

```
<Directory /site>
Options None
AllowOverride None
Order deny,allow
Deny from all
Allow from 10.10.0.0/24
</Directory>
```

To allow a specific ip-address to access your site, give the ip-address in the Allow directive.

```
<Directory /site>
Options None
AllowOverride None
Order deny,allow
Deny from all
Allow from 10.10.1.21
</Directory>
```

## 10. Don't display or send Apache version (Set ServerTokens)

By default, the server HTTP response header will contains apache and php version. Something similar to the following. This is harmful, as we don't want an attacker to know about the specific version number.

```
Server: Apache/2.2.17 (Unix) PHP/5.3.5
```

To avoid this, set the ServerTokens to Prod in httpd.conf. This will display "Server: Apache"

without any version information.

```
# vi httpd.conf
ServerTokens Prod
```

Following are possible ServerTokens values:

- \* ServerTokens Prod displays “Server: Apache”
- \* ServerTokens Major displays “Server: Apache/2”
- \* ServerTokens Minor displays “Server: Apache/2.2”
- \* ServerTokens Min displays “Server: Apache/2.2.17”
- \* ServerTokens OS displays “Server: Apache/2.2.17 (Unix)”
- \* ServerTokens Full displays “Server: Apache/2.2.17 (Unix) PHP/5.3.5” (If you don’t specify any ServerTokens value, this is the default)

Apart from all the above 10 tips, make sure to secure your UNIX / Linux operating system. There is no point in securing your apache, if your OS is not secure. Also, always keep your apache version upto date. The latest version of the apache contains fixes for all the known security issues. Make sure to review your apache log files frequently.

## **12.7 - DNS Free**

<http://freedns.afraid.org/signup/>

Sobre a idoneidade

<http://www.scamadviser.com/check-website/freedns.afraid.org>

Adicionado:

[tiagoarts.com](http://tiagoarts.com)

NS records got from your nameservers listed at the parent NS are:

```
ns1.afraid.org. ['50.23.197.95'] (NO GLUE) [TTL=172800]
ns4.afraid.org. ['70.39.97.253'] (NO GLUE) [TTL=172800]
ns3.afraid.org. ['69.197.18.162'] (NO GLUE) [TTL=172800]
ns2.afraid.org. ['208.43.71.243'] (NO GLUE) [TTL=172800]
```

Reverso

190.18.197.69.in-addr.arpa -> 69.197.18.190.afraid.org

Outros DNS Free

<https://dns.he.net/>

Registrar

<https://dashboard.opendns.com/>

Efetuar login

<https://store.opendns.com/setup/>

Vídeo com ajuda

<https://store.opendns.com/setup/>

<https://store.opendns.com/setup/operatingsystem/ubuntu>

Outro

<http://www.xname.org/>

## 12.8 - Erro comum no SSH

Quando reinstalar o VPS o SSH não irá conectar normalmente.

Apresenta a mensagem:

```
ssh root@162.243.89.121
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
```

...

```
Offending ECDSA key in /home/ribafs/.ssh/known_hosts:6
```

```
remove with: ssh-keygen -f "/home/ribafs/.ssh/known_hosts" -R 162.243.89.121
```

Então selecione apenas `ssh-keygen -f "/home/ribafs/.ssh/known_hosts" -R 162.243.89.121`

Cole no terminal e ENTER

```
ssh-keygen -f "/home/ribafs/.ssh/known_hosts" -R 162.243.89.121
```

Agora repita o procedimento para conectar.

Antes vá até seu e-mail, copie a senha recebida e cole no prompt do SSH.

Imediatamente troque a senha de root e remova o e-mail recebido com a senha provisória.

## 12.9 - Script para redirecionamento de página

HTML

```
<meta http-equiv="refresh" content="0;url=http://www.seudominio.com.br/">
```

.HTACCESS

```
Redirect /paginavelha.html http://www.seudominio.com.br/index.php
```

ASP

```
<% response.redirect("http://www.seudominio.com.br/") %>
```

## PHP

```
<?php header ("location: http://www.seudominio.com.br/"); php?>
```

## JAVA

```
<% String redirectURL = "http://www.seudominio.com.br/";  
response.sendRedirect(redirectURL); %>
```

## ASP.NET

```
<script runat="server">  
Response.Redirect("http://www.seudominio.com.br");  
</script>
```

## ColdFusion

```
<.cfheader name="Location" value="http://www.seudominio.com.br">
```

## Perl

```
$q = new CGI;  
print $q->redirect("http://www.seudominio.com.br/");
```

## Ruby On Rails

```
def old_action  
redirect_to "http://www.seudominio.com.br/"  
end
```

## 13.0 - Servidor de Testes de Segurança

Agora chegou a hora de testar a segurança de servidores.

Vamos instalar um servidor somente para testar sua segurança. Para isso instalaremos em etapas, como abaixo.

Servidor - ribafs.sub.es no DigitalOcean

Cliente - Os testes serão efetuados de uma máquina desktop com o Kali Linux instalado.

### Primeira Etapa:

- Instalar um servidor web típico de hospedagem compartilhada, sem nada de segurança extra:
  - Instalar LAMP
  - Instalar Joomla 2.5 e o 3.2 com conteúdo de exemplo para os testes.

### Segunda Etapa:

- Adicionar iRedMail, que já implementa alguma segurança

### Terceira Etapa:

- Reforçar a segurança:
  - Cuidados com a segurança
  - mod\_evasive e mod\_security
  - etc.
- Configurar o logwatch e o logcheck para enviar um e-mail a cada dia para nosso e-mail, assim como configurar o fail2ban para nos enviar um e-mail a cada IP banido.

### Quarta Etapa

- Honeypot
- E/ou abrir bem as portas e retirar segurança e monitorar com mod\_security detectOnly e outros.

Sugestões de Honeypot para Ubuntu:

-

<https://www.digitalocean.com/community/articles/how-to-set-up-an-artillery-honeypot-on-an-ubuntu-vps>

-

<https://www.digitalocean.com/community/articles/how-to-install-kipko-an-ssh-honeypot-on-an-ubuntu-cloud-server>





## 14.0 - Referências

### VPS Free

Amazon oferece um pequeno servidor grátis por um ano:

<https://aws.amazon.com/ec2/>

A RedHat oferece VPS free

<https://www.openshift.com/>

A DigitalOcean oferece cupons (ou outro termo) para que possamos testar seu serviço gratuitamente por um mês ou oferece 5 ou 10 dólares, o que corresponde a um mês ou dois num servidor básico. Mas para conseguir precisará procurar em algum fórum ou blog alguém divulgando um link.

Site Oficial do iRedMail, contendo download, documentação e forum.

<http://iredmail.org/index.html>

[http://iredmail.org/install\\_iredmail\\_on\\_ubuntu.html](http://iredmail.org/install_iredmail_on_ubuntu.html)

Melhor tutorial que encontrei para instalação do iRedMail no Amazon

<http://jeffreifman.com/how-to-install-your-own-private-e-mail-server-in-the-amazon-cloud-aws/>

Links sobre a DigitalOcean

<https://www.digitalocean.com/about>

<http://techcrunch.com/2013/06/27/digitalocean-wants-to-challenge-amazon-linode-and-co-with-better-prices-marketing-and-focus-on-simplicity/>

<https://www.digitalocean.com/community/articles/how-to-use-the-digitalocean-docker-application>

<https://www.digitalocean.com/community/articles/how-to-launch-your-site-on-a-new-ubuntu-12-04-server-with-lamp-sftp-and-dns>

Melhorando o desempenho

<https://www.digitalocean.com/community/articles/how-to-install-and-use-memcache-on-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-protect-ssh-with-fail2ban-on-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-install-and-use-postgresql-on-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-install-joomla-on-a-virtual-server-running-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-install-drupal-on-a-virtual-server-running-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-install-denyhosts-on-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/one-click-install-wordpress-on-ubuntu-12-10-with-digitalocean>

<https://www.digitalocean.com/community/articles/how-to-setup-a-firewall-with-ufw-on-an-ubuntu-and-debian-cloud-server>

<https://www.digitalocean.com/community/articles/installing-the-cacti-server-monitor-on-ubuntu-12-04-cloud-server>

<https://www.digitalocean.com/community/articles/how-to-configure-the-apache-web-server-on-an-ubuntu-or-debian-vps>

<https://www.digitalocean.com/community/articles/how-to-manage-log-files-with-logrotate-on-ubuntu-12-10>

<https://www.digitalocean.com/community/articles/how-to-use-ps-kill-and-nice-to-manage-processes-in-linux>

<https://www.digitalocean.com/community/articles/how-to-install-alternative-php-cache-apc-on-a-cloud-server-running-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-install-phpbb-forums-on-ubuntu-12-10>

<https://www.digitalocean.com/community/articles/how-to-scale-web-applications-on-ubuntu-12-10>

<https://www.digitalocean.com/community/articles/how-to-configure-remote-backups-using-bacula-in-an-ubuntu-12-04-vps>

<https://www.digitalocean.com/community/articles/installing-and-configuring-bacula-on-an-ubuntu-12-04-vps>

<https://www.digitalocean.com/community/articles/how-to-use-roles-and-manage-grant-permissions-in-postgresql-on-a-vps--2>

<https://www.digitalocean.com/community/articles/how-to-use-rsync-to-sync-local-and-remote-directories-on-a-vps>

<https://www.digitalocean.com/community/articles/how-to-install-zend-framework-on-an-ubuntu-12-04-vps>

<https://www.digitalocean.com/community/articles/how-to-install-kippo-an-ssh-honeypot-on-an-ubuntu-cloud-server>

<https://www.digitalocean.com/community/articles/how-to-install-cakephp-on-an-ubuntu-12-04-vps>

<https://www.digitalocean.com/community/articles/installing-and-using-ranger-a-terminal-file-manager-on-a-ubuntu-vps>

<https://www.digitalocean.com/community/articles/how-to-use-dig-whois-ping-on-an-ubuntu-vps-to-query-dns-data>

<https://www.digitalocean.com/community/articles/how-to-monitor-system-authentication-logs-on-ubuntu-12-04-vps>

[buntu](#)

<https://www.digitalocean.com/community/articles/how-to-use-pam-to-configure-authentication-on-an-ubuntu-12-04-vps>

<https://www.digitalocean.com/community/articles/how-to-secure-postgresql-on-an-ubuntu-vps>

<https://www.digitalocean.com/community/articles/how-to-use-top-netstat-du-other-tools-to-monitor-server-resources>

<https://www.digitalocean.com/community/articles/how-to-enable-multiple-sites-on-a-drupal-installation-on-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-use-gpg-to-encrypt-and-sign-messages-on-an-ubuntu-12-04-vps>

<https://www.digitalocean.com/community/articles/how-to-install-and-set-up-openerp-7-0-on-a-debian-7-ubuntu-13-10-vps>

<https://www.digitalocean.com/community/articles/how-to-monitor-system-authentication-logs-on-ubuntu>

<https://www.digitalocean.com/community/articles/how-to-install-and-use-bastille-to-harden-an-ubuntu-12-04>

<https://www.digitalocean.com/community/articles/how-to-understand-the-filesystem-layout-in-a-linux-vps>

<https://www.digitalocean.com/community/articles/how-to-install-iredmail-on-ubuntu-12-04-x64>

<https://www.digitalocean.com/community/articles/how-to-set-up-a-host-name-with-digitalocean>

## **Livros**

Webmin kompakt - Holger Reibold

MODSECURITY HANDBOOK - The Complete Guide to Securing Your Web Applications

Web Penetration Testing with Kali Linux - Joseph Muniz e Amir Lakhani da Packt

**Importante site para monitorar segurança de sites:**

<https://securityheaders.com/>

**Extensão que mostra várias informações importantes sobre site visitado:**

Wappalyzer

## Posfácio

Deixando uma reflexão: depois de instalar vários servidores tipo VPS, no Amazon, no Digital Ocean, no Servermania e no FreeVPS eu conclui que a segurança não ficava nunca como eu gostaria. Veja que a segurança recebeu a maior atenção em termos de conteúdo no livro. Nunca eu ficava seguro pra valer após uma instalação. A instalação e configuração dos servidores estava funcionando redondinho, mas o que dizer da segurança? Poderia garantir que o servidor não seria invadido? Não, não poderia. Vários recursos importantes foram adotados em termos de segurança, alguns que testam a nossa segurança como o Nikto; outros que reforçam como o fail2ban, como o denyhosts; outros que nos avisam por e-mail de problemas e acontecimentos como o logcheck e o logwatch. Mas destes o que mais me impressiona é o mod\_security, que em tempo real barra tentativas de ataque, identificando-as e dando nome aos bois. Muito trabalhoso de configurar mas mesmo assim vale a pena.

Como o resultado foi positivo decidi compartilhar com a intenção de colaborar com outras pessoas para que aprendam a instalar servidores tipo VPS e que aprendam um pouco sobre segurança e o que é mais importante, que se interessem por segurança de forma a procurar estudar e tornar a cada dia seu servidor mais seguro.

A segurança requer conhecimento, trabalho e atitude, uma atitude proativa de zelo.

Lembre de que atualizações e backup são duas das mais importantes medidas em termos de segurança.

### Licença

A licença deste livro é a GPL 2, pois é a licença de boa parte dos softwares abordados, exceto quando em conflito com algum tutorial, quando então se deve respeitar a licença do tutorial.

### Direitos Autorais

Este livro seria bem pequeno se aqui relatasse somente minhas experiências e conhecimento. Aqui citei vários tutoriais de terceiros, sempre com o devido crédito. Traduzi vários outros, geralmente citando o link do original. Como todo o conteúdo é relativo a software livre e open source não tive muitas outras preocupações.

Mas caso alguém identifique algum tutorial de sua autoria, que eu haja esquecido de citar a fonte e queira que eu o faça basta me contatar pelo [ribafs@gmail.com](mailto:ribafs@gmail.com) assim também por qualquer outro motivo.

### Correções e sugestões

Caso encontre algum erro técnico ou de português e queira nos ajudar enviando a correção, por favor será muito bem-vindo.