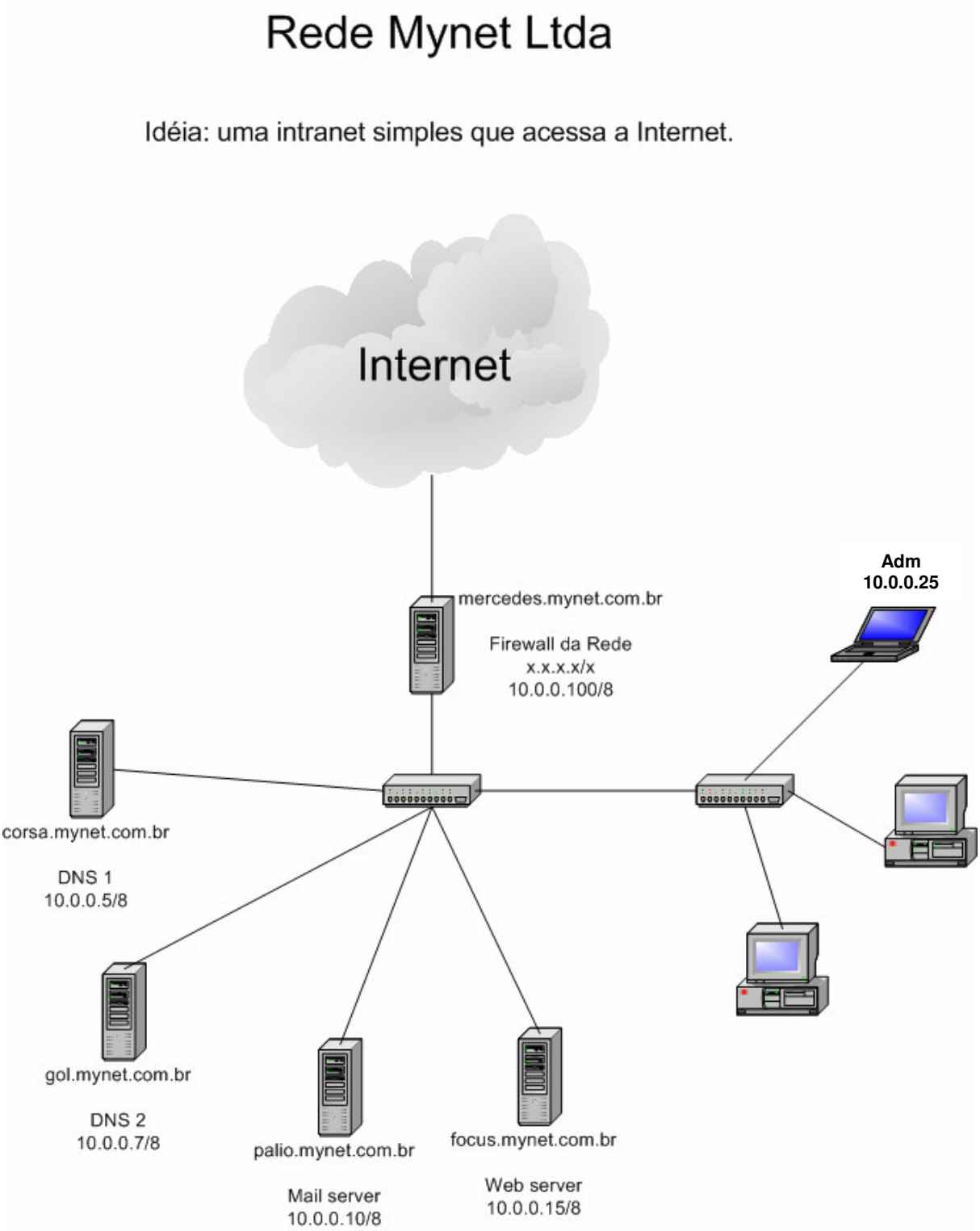
1ª Semana de Capacitação
e Desenvolvimento em
Software Livre

26 a 30 ABRIL Brasília - DF

Segurança e administração remota de servidor GNU/Linux: exemplo com DNS

(abordagem específica para Red Hat/Fedora - Slackware)

- João Eriberto Mota Filho -
www.eriberto.cjb.net


Rede Mynet Ltda
Idéia: uma intranet simples que acessa a Internet.
Internet
mercedes.mynet.com.br
Firewall da Rede
x.x.x.x/x
10.0.0.100/8
Adm
10.0.0.25
corsa.mynet.com.br
DNS 1
10.0.0.5/8
gol.mynet.com.br
DNS 2
10.0.0.7/8
palio.mynet.com.br
Mail server
10.0.0.10/8
focus.mynet.com.br
Web server
10.0.0.15/8

MEDIDAS DE SEGURANÇA ANTECEDENTES À INSTALAÇÃO

1) Baixar a distribuição de um local confiável (sugiro o site da distribuição ou www.linuxiso.org);
2) Conferir o MD5SUM dos arquivos baixados para evitar crash ou adulterações maliciosas.

MEDIDAS DE SEGURANÇA NA INSTALAÇÃO

1) Não escolha nomes óbvios para os seus servidores, de forma a determinar as funções desses;
2) Não ative o firewall padrão na instalação;
3) Não instale pacotes desnecessários, mesmo que possam ser úteis um dia. Se houver necessidade, instale-os quando esse dia chegar (se chegar);
4) Não instale os compiladores C e C++ se não for necessário;
5) Evite instalar ambientes gráficos em servidores de rede;
6) 7) Ative o shadow e o MD5.

PACOTES OBRIGATÓRIOS NA INSTALAÇÃO

1) Instale o Sendmail e o Open SSH;
2) Instale o mc, o nmap e o iptraf.

MEDIDAS ADMINISTRATIVAS IMEDIATAS PÓS-INSTALAÇÃO

Após a instalação de um servidor, execute as seguintes medidas administrativas:

1) Verifique se a rede está no ar e em condições de operar;

2) Configure a resolução local de nomes[1]. Um exemplo de configuração para a máquina corsa.mynet.com.br:

```
127.0.0.1   localhost.localdomain      localhost
10.0.0.5    corsa.mynet.com.br         corsa
```

3) Insira a expressão `alias ps='ps ax'` no fim do arquivo /etc/profile.

MEDIDAS DE SEGURANÇA IMEDIATAS PÓS-INSTALAÇÃO

Após a instalação de um servidor, execute as seguintes medidas de segurança:

1) Cadastre uma senha de root bem escolhida;

2) Desative, permanentemente, todos os daemons que não forem utilizados. Não deixe nada que seja dispensável, mesmo que "um dia venha a ser útil";

[1] No RH, isso pode ser feito no arquivo /etc/hosts; no Slackware, ainda há o /etc/networks.

3) Configure, em /etc/aliases, as aliases administrativas de e-mail necessárias, como abuso, abuse, spam, suporte, postmaster, hostmaster e webmaster, redirecionando-as para root. Em seguida, redirecione o root para o seu e-mail de administrador[2];

4) Configure o TCP Wrappers[3];

5) Configure o firewall local[4] para permitir apenas os acessos necessários;

6) Configure o firewall local para aceitar somente um ping por segundo, evitando assim ataques ICMP. Isso pode ser conseguido com:

```
#iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
```

7) Edite o arquivo /etc/default/useradd[5], alterando o shell padrão para / ;

8) Configure o ssh para não aceitar conexões do root e mude a porta de conexão[6];

9) Cadastre um usuário padrão para usar ssh;

10) Habilite o fechamento automático de terminal, caso o tempo de idle atinja o limite de 20 minutos (1200 segundos). Para isso, insira no arquivo /etc/profile, como última linha, a entrada:

```
TMOUT=1200
```

11) Configure o logrotate, em /etc/logrotate.conf e /etc/logrotate.d ;

12) Se a distribuição permitir, faça a imediata verificação referente à atualização do sistema[7];

13) Faça uma checagem de portas abertas, utilizando o nmap contra o sistema. Feche os serviços desnecessários. Comandos:

```
#nmap  127.0.0.1
#nmap -sU 127.0.0.1
```

14) Sincronize todos os relógios para que os logs sejam fiéis. Utilize serviços de hora para isso;

15) Emita os comandos:

```
#df -h
#free
#top
#ps
```

e analise os resultados.

[2] Não esqueça de rodar o comando #newaliases no final.
[3] Arquivos /etc/hosts.allow e /etc/hosts.deny
[4] O firewall da própria máquina. Uma boa referência: www.iptablesbr.cjb.net .
[5] Apenas para RH.
[6] Não esqueça que para conetar você deverá especificar a porta e usuário: `ssh -l <usuario> -p <porta> <ip>`
[7] No RH: up2date. No Fedora: yum. No Slacware: slackpkg, baixado da Internet. No Debian: apt-get.

MEDIDAS ADMINISTRATIVAS E DE SEGURANÇA PERIÓDICAS

1) Não permita que usuários tenham senhas fracas. Tente quebrar as senhas dos seus usuários periodicamente;

2) Dê lock[8] nas senhas de usuários que estiverem afastados da empresa (férias por exemplo);

3) Assine boletins de segurança[9] e leia-os sempre;

4) Mantenha os servidores atualizados;

5) Rode ferramentas de invasão e auditoria de segurança[10] semanalmente contra o seu sistema;

6) Faça com que a máquina selecione informações dos logs e as remeta para você diariamente. Utilize cron para isso;

7) Instale e gerencie um IDS;

8) Retire o shell dos usuários que não precisarem dele;

9) Altere a senha de root periodicamente;

10) Faça backups regulares das suas configurações;

11) Evite executar serviços em demasia. Coloque tais serviços no ar somente quando precisar (use o cron!);

12) Participe de uma boa lista de discussão sobre redes Linux[11];

13) Mantenha a data e a hora dos servidores constantemente atualizados.

[8] #passwd -l <usuário> e #passwd -u <usuário>
[9] Uma sugestão: http://www.securitytracker.com/signup/signup_now.html .
[10] Sugiro o Nessus.
[11] Uma sugestão: http://br.groups.yahoo.com/group/servux .

ANEXO A

INSTALAÇÃO DO LINUX PARA ESTUDO DO CASO EM PAUTA

Pacotes da Série A (Base Linux System)

kernel-ide
aaa_base
bash
bin
bzip2
coreutils
cxxlibs
dcron
devfsd
devs
e2fsprogs
elflibs
elvis
etc
findutils
floppy
gawk
glibc-solibs
glibc-zoneinfo
grep
gzip
hotplug
isapnptools (apenas para ISA)
kbd
kernel-modules
less
lilo
loadlin
logrotate
module-init-tools
openssl-solibs
pciutils
pgktools
procps
reiserfsprogs
sed
shadow
slocate
sysklogd
syslinux
sysvinit
tar
umsdos-progs
usbutils
util-linux

Pacotes da Série AP (Applications)

diffutils
groff
lsof
man
man-pages
mc

Pacotes da Série L (Libraries)

glibc
svgalib

Pacotes da Série N (Network/News/Mail/UUCP)

bind
gnupg
iptables
iptraf
lynx
nail
nmap
openssh
openssl
procmail
sendmail
tcpdump
tcpip
traceroute
wget

ANEXO B

ARQUIVOS DE CONFIGURAÇÃO DO DNS

/etc/resolv.conf

```
nameserver 10.0.0.25
```

/etc/host.conf

```
order bind,hosts
multi on
```

/etc/named.boot

```
directory                       /var/named
cache       .                   named.ca
primary     localhost           localhost.zone
primary     127.in-addr.arpa    named.local
primary     mynet.com.br        mynet.com.br
primary     10.in-addr.arpa     10.0.0.0
xfrnets     10.0.0.7
```

/etc/named.conf

(obtido pelo comando #named-bootconf.sh < named.boot > named.conf)

```
options {
        directory "/var/named";
        allow-transfer {
                10.0.0.7;
        };
};

zone "." {
        type hint;
        file "named.ca";
};

zone "localhost" {
        type master;
        file "localhost.zone";
};

zone "127.in-addr.arpa" {
        type master;
        file "named.local";
};

zone "mynet.com.br" {
        type master;
        file "mynet.com.br";
};

zone "10.in-addr.arpa" {
        type master;
        file "10.0.0.0";
};
```

/var/named/localhost.zone

```
$TTL    86400
@               IN SOA      localhost.  root (
                            20040429            ; serial (d. adams)
                            3H              ; refresh
                            15M             ; retry
                            1W              ; expiry
                            1D )            ; minimum

                        IN NS   corsa.mynet.com.br.
localhost.                  IN A        127.0.0.1
```

/var/named/named.local

```
$TTL    86400
@       IN      SOA     localhost. root.localhost.  (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum
            IN      NS      corsa.mynet.com.br.

1.0.0       IN      PTR     localhost.
```

/var/named/mynet.com.br

```
$TTL    86400
@               1D IN SOA       mynet.com.br. root (
                                20040429            ; serial (d. adams)
                                3H              ; refresh
                                15M              ; retry
                                1W              ; expiry
                                1D )            ; minimum

                            IN NS   corsa.mynet.com.br.
                            IN MX   5       palio.mynet.com.br.

corsa.mynet.com.br.     IN A    10.0.0.5
www.mynet.com.br.       IN A    10.0.0.15
smtp.mynet.com.br.      IN A    10.0.0.10
pop3.mynet.com.br.      IN A    10.0.0.10
```

/var/named/10.0.0.0

```
$TTL    86400
@               1D IN SOA       mynet.com.br. root (
                                20040429            ; serial (d. adams)
                                3H              ; refresh
                                15M              ; retry
                                1W              ; expiry
                                1D )            ; minimum

                            IN NS   corsa.mynet.com.br.

5.0.0   IN PTR  corsa.mynet.com.br.
15.0.0  IN PTR  www.mynet.com.br.
10.0.0  IN PTR  smtp.mynet.com.br.
10.0.0  IN PTR  pop3.mynet.com.br.
```

Para ver detalhes de configuração DNS, não deixe de dar uma olhada em http://br.groups.yahoo.com/group/servux/message/8553 e http://br.groups.yahoo.com/group/servux/message/3446 .

ANEXO C

EXEMPLOS DE ROTINAS CRON E AUDITORIA DE LOG

Vamos admitir que estamos dentro de uma empresa que funciona de segunda a sexta, das 11:00 às 18:00. Você, administrador da rede, nunca chega antes do horário mas sai até 1 hora depois do fim do expediente.

Você possui uma máquina que é o proxy transparente da sua rede.

Em /etc/adm você implementou uma rotina shell script chamada secure.log:

```
#!/bin/bash
cat /var/log/secure*|grep password|grep "`date --date '1 day ago' '+%b %e'`"
```

Você também implementou um cron da seguinte forma[12]:

```
# by eriberto em 23 Abr 04
#
# segunda a sexta - atividades do sendmail, ssh e apache
#
50    10    *    *    1-4    /etc/init.d/sendmail start > /dev/null[13]
52    10    *    *    1-4    /etc/init.d/sendmail stop > /dev/null
55    10    *    *    1-4    /etc/init.d/sshd start > /dev/null; /etc/init.d/httpd start > /dev/null
10    19    *    *    1-4    /etc/init.d/sshd stop > /dev/null; /etc/init.d/httpd stop > /dev/null
#
# terca-feira - verificacao de espaco em disco
#
00    10    *    *    2     /usr/bin/df -h
#
# quarta-feira - atualizacao do yum e do sistema
#
00    3     *    *    3     /usr/bin/yum list > /dev/null
00    9     *    *    3     /usr/bin/yum -y update
#
# diariamente - verificacao de logins remotos
#
00    1     *    *    *     /etc/adm/secure.log
#
# diariamente - execucao do sarg
#
58    23    *    *    *     /usr/sbin/sarg
```

Se fosse um servidor pop3, por exemplo, você poderia controlar as 20 maiores caixas postais com o arquivo:

```
#!/bin/bash
ls -lSh /var/spool/mail | tail -n 20
```

SEJA CRIATIVO!

Não deixe de olhar: http://br.groups.yahoo.com/group/servux/message/8242

[12] a) Exemplo baseado na distribuição Red Hat/Fedora. b) O caminho completo de um comando pode ser descoberto com #which <comando>.

[13] /dev/null evita o envio de msg desnecessárias por e-mail

BIBLIOGRAFIA E FONTES DE AJUDA

1. Listas de discussão

Servux - voltada para Linux em rede - http://br.groups.yahoo.com/group/servux

Links Servux - http://br.groups.yahoo.com/group/servux/links/Mensagens_001047609003

Linux Shell Script - http://br.groups.yahoo.com/group/shell-script

2. Sites

Iptables BR - http://www.iptablesbr.cjb.net

Underlinux - http://www.underlinux.com.br

Security Tracker - http://www.securitytracker.com

Linux Security - http://www.linuxsecurity.com

BR Linux - http://www.br-linux.org

3. Livros

Linux e Seus Servidores - João Eriberto Mota Filho

Programação Shell Linux - Julio Cezar Neves

Segurança contra hackers Linux - Brian Hatch, James Lee e George Kurtz

4. Download de programas e iso

Linux ISO - http://www.linuxiso.org

Kurumin - http://www.kurumin.org

Fresh Meat - http://www.freshmeat.net

RPM Find - http://www.rpmfind.net

RPM Pbone - http://rpm.pbone.net