Melhorando a Segurança de um VPS com CentOS 7

Sumário

Requisitos:

Instalar o CentOS 7

Atualizar,

Fazer upgrade

reboot

Instalar o LAMP

adduser ribafs

passwd ribafs

usermod -a -G wheel ribafs

mkdir /home/ribafs/backup

Implementemos a segurança, para estar usando o servidor de forma mais segura.

0. Cuidados Iniciais

Selecionar uma distribuição desejada e adequada para a finalidade.

Faça a instalação

Efetue login e atualize a distribuição em seguida. Ao final efetue um reboot.

Evite instalar pacotes para desenvolvimento como gcc, make, etc.

Evite instalar repositórios instáveis.

Para forçar a memória, logo após a configuração final do servidor, já crie um backup ou snapshot do mesmo e fique atento para criar outro backup logo que o servidor esteja concluído e bem configurado.

Agora (logo após a instalação do nginx, mysql e php) é uma boa hora para efetuar uma cópia dos scripts de configuração originais que estão funcionando. Para em caso de problema restaurar este script que funciona para que volte a funcionar. Guarde uma cópia no diretório /home/seuuser/backup do usuário que irá administrar o servidor:

- nginx.conf e default.conf
- php.ini e php-fpm.ini
...

Backup local do Servidor
Uma boa ideia é ter uma box no Vagrant do CentOS 7 x64 em seu desktop, sendo cópia fiel e original do servidor localmente, com todos os pacotes do servidor para ter uma cópia fiel do servidor em seu desktop. Em caso de problema no servidor poderá resolver com uma cópia do script do desktop.

Primeira Atualização

yum update
reboot

Gerenciador de Arquivos Modo Texto
Uma boa pedida é instalar o gerenciador de arquivos modo texto mc:

yum install mc

No centos instale o unzip:

yum install unzip
yum install net-tools

Backup Regular
Efetuar backup com frequência de tudo que tem no servidor, especialmente após alterações:
- sites
- aplicativos
- arquivos

Ajustar Fuso Horário

Mudar fuso horário para America/Fortaleza (no meu caso)

timedatectl set-timezone America/Fortaleza

Verificar timezona
timedatectl

ou
timedatectl list-timezones

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

Procurar diretórios com 777
find /var/www/html -type d -perm -o+w -exec ls -ld {} \;

Procurar contas sem senha
awk -F: '($2 == "") {print}' /etc/shadow

Limpar cache de RAM

Criar um script para rodar com mais praticidade

Executar antes free -m e após executar o script para comparar os valores.

sudo nano /usr/local/bin/m
sudo sysctl -w vm.drop_caches=3

sudo chmod +x /usr/local/bin/m

Rodar:
sudo m

Adicionar partição de Swap

Adicionar partição de swap com 2GB

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

mkswap /swapfile

swapon /swapfile

Adicionar ao fstab

nano /etc/fstab

/swapfile swap swap defaults 0 0

Testar

free -m

1. Habilitação e Configurar firewall com ufw

iptables -L

Ver arquivo texto com...

2. Secure shared memory no fstab

Edite o fstab e adicione a linha ao final. Somente após o reboot terá efeito:

nano /etc/fstab

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

3. Reforçar a segurança do SSH

Vamos otimizar a configuração do SSH:

Adicionar usuário administrador
Adicionar um usuário que gerenciará o computador com sudo e que será o único a acessar via ssh:

sudo su
adduser nomeuser # Troque nomeuser pelo login desejado
adduser nomeuser admin # No Debian o grupo admin precisa ser criado

```
usermod -aG wheel nomeuser
```

nano /etc/sudoers

Adicione a linha a seguir abaixo da linha do root
nomeuser ALL=(ALL) NOPASSWD:ALL

su - nomeuser
mkdir .ssh
chmod 700 .ssh
cd .ssh
ssh-keygen -b 1024 -f id_nomeuser -t dsa (Enter 2 vezes)
cat ../.ssh/id_nomeuser*.pub > ../.ssh/authorized_keys

exit

Escolha uma porta alta, como a 10522 ou mais alta

Agora já podemos sanear o SSH:

nano /etc/ssh/sshd_config

#Faça as alterações abaixo:
Port 65522
LoginGraceTime 30 # reduzir tempo do timeout
PasswordAuthentication yes
AllowUsers nomeuser root

service sshd restart
exit
Veja que mantive o acesso ao root. Mas após o primeiro acesso com o nomeuser e sentir segurança então remove o root da linha AllowUsers, além disso mudar no sshd_config a linha:

PermitRootLogin no

E reiniciar o ssh

Experimente agora conectar com o root.

Gere as chaves do SSH em seu micro desktop com:

```
ssh-keygen -t rsa -b 4096
```

Apenas tecle Enter duas vezes

Então copie sua chave para o servidor, para que possa conectar sem digitar a senha. Na primeira vez te pedirá a senha mas sua senha do desktop, mas memorizará e não mais pedirá. Assim ficará mais seguro.

ssh-copy-id ribafs@ip_servidor -p 10522

Mesmo com scp não pedirá senha.

Sugestão - Criar um script para conectar:

sudo nano /usr/local/bin/docean

ssh -p 65522 ribafs@128.199.63.251

sudo chmod +x /usr/local/bin/docean

Conecte com
docean

Monitorar login do root

sudo yum install mailx

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" ribafs@gmail.com

OBS.: para envio de e-mail precisa de solicitar do suporte a liberação. Problema de spam.

Notificação de acesso via ssh pelo ribafs

cd /home/ribafs
nano .bashrc
echo 'ALERT - Root Shell Access (ServerName) on:' `date` `who` | mail -s "Alert: Root Access from `who | cut -d'(' -f2 | cut -d')' -f1`" ribafs@gmail.com

4. Reforçar a segurança da rede configurando o sysctl

Para prevenir fontes de roteamento de pacotes de entrada e logs de IPs malformados

sudo nano /etc/sysctl.conf

Descomente

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

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

# Block SYN attacks
net.ipv4.tcp_syncookies = 1

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

Adicione ao final:

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

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

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

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

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

# Log Martians
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

Reiniciar
```

```
sudo sysctl -p
```

5. Prevenir IP Spoofing

Edite o

nano /etc/host.conf
E deixe seu conteúdo assim:

order bind,hosts
multi on
nospoof on

6. Reforçar a segurança do PHP

Uma boa forma de melhorar a segurança do php é instalando o phpsecinfo:
https://github.com/funkatron/phpsecinfo
http://phpsec.org/projects/phpsecinfo/

E corrigir os erros apontados com as respectivas recomendações.

Algumas sugestões para reforçar a segurança do PHP:

edite o php.ini e faça as alterações:

nano /etc/php.ini

ALERTA – ao efetuar as alterações abaixo faça uma a uma, sempre reiniciando o apache e abrindo o site e efetuando um refresh para testar. Caso tenha problema desfaça ou ajuste o parâmetro com problema.

disable_functions = exec,system,shell_exec,passthru,
html_errors = Off
mail.add_x_header = Off
session.name = NEWSESSID

Na linha com disable_functions já existem várias funções por padrão que são desabilitadas. Não as remova, apenas adicione as recomendações acima ao início, separadas por vírgula.
Com a ajuda do PHPsecinfo também ajustei estes abaixo:

allow_url_fopen = Off
upload_tmp_dir = /usr/share/nginx/html/phpup

Criei o diretório /usr/share/nginx/html/phpup
Estes dois últimos parâmetros devem ser adotados com cuidado, de acordo com a sua necessidade. Abaixo são os valores default na versão 7 do php:

post_max_size = 8M
upload_max_filesize = 2M

```
service nginx restart
```

Depois dos ajustes acima alguma coisa pode não funcionar. Então efetue os ajustes devidos, sem exagerar.

Proteger arquivos de configuração do apache, php e mysql contra escrita:

/etc/php//php.ini
/etc/nginx/conf.d/default.conf e demais
/etc/mysql/my.cnf

8. Instalar e Configurar ModSecurity e ModEvasive

9. Scannear logs e banir hosts suspeitos

Usando DenyHosts e Fail2Ban

Denyhosts – bloqueia ataques de SSH adicionando entradas ao /etc/hosts.dny. Também avisa ao administrador sobre hosts suspeitos, ataques de usuários e logins suspeitos.

sudo apt install denyhosts

Após instalar edite o
sudo nano /etc/denyhosts.conf

E atualize seu e-mail e outras configurações que desejar.

```
ADMIN_EMAIL = ribafs@gmail.com
SMTP_HOST = localhost
SMTP_PORT = 25
#SMTP_USERNAME=foo
#SMTP_PASSWORD=bar
SMTP_FROM = DenyHosts nobody@localhost
#SYSLOG_REPORT=YES

service denyhosts restart
```

Fail2Ban
O fail2ban é mais eficiente que o denyhosts, pois ele extende a monitoração de logs para outros serviços além do ssh, como o apache, courier, ftp e mais.

O fail2ban escaneia arquivos de log e bane IPs que parecem suspeitos (muitas tentativas erradas de senha, procurando por exploits, etc)
Geralmente bloqueia através do firewall por um certo tempo que é configurável

Instalação

sudo apt install fail2ban

Após instalar edite

sudo nano /etc/fail2ban/jail.conf

E crie o filtro de regras requerido
Ative todos os serviços que deseja que o fail2ban monitore

Para que monitore o ssh, altere enable para true:

OBS: atente para mudar de ssh para o número que escolheu, caso não use a 22.

```
[sshd]

enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3
```

Caso o seu ssh esteja usando outra porta, mude port = suaporta

Checar status:

fail2ban-client status

Restartar
/etc/init.d/fail2ban restart

Desbloquear um certo IP bloqueado por engano
iptables -L -n

Checar porta 443
iptables -L -n | grep 443

Caso o comando acima mostre o IP 201.14.45.23 rodamos o seguinte comando para liberar:
iptables -D fail2ban-SSH -s 201.14.45.23 -j DROP

Comando mais específico:
fail2ban-client set ssh-iptables unbanip IpaRemover

Whitelisting

Whitelisting é configurada no jail.conf usando uma lista separada por espaço

```
[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
```

10. Detectar Intrusões – PSAD

PSAD é uma coleção de 3 pequenos daemons do sistema, que rodam para analisar mensagens de log do iptables para detectar scanneamento de portas e outros tráficos suspeitos.

Instalação

```
sudo apt install psad
```

Configuração básica

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

- **EMAIL_ADDRESSES** – mude para seu e-mail
- **ENABLE_AUTO_IDS** - se Y o psad agirá automaticamente
- **ENABLE_AUTO_IDS_EMAILS** - se **Y** psad mandará um e-mail em cada suspeita

```
sudo service psad restart
```

11. Checar por RootKits – RKHunter e CHKRootKit

Rootkits e RKHunter basicamente fazem a mesma coisa, procuram rootkits no sistema. Nenhuma ofensiva aqui, apenas mostram o que veem.

Instalação

```
sudo apt install rkhunter chkrootkit
```

Executando chkrootkit

```
sudo chkrootkit
```

Atualizando e rodando rkhunter

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

12 Varrendo portas abertas com Nmap

O nmap é um software para descobrir a rede e para auditar segurança.

Instalação
sudo apt install nmap

Varrer seu sistema por portas abertas

nmap -v -sT localhost

Saída
Not shown: 995 closed ports
PORT   STATE SERVICE
25/tcp   open smtp
80/tcp   open http
443/tcp open https
3306/tcp open mysql
5432/tcp open postgresql

Lembrando que varre apenas até a porta 1000, portando não mostrou a do ssh
Outro detalhe é que para acesso extereno somente as portas 80 e 443, as demais oferecem acesso somente interno.

O acesso externo se dá ao mysql somente através do Apache. O visitante do site acessa o site pela porta 80 ou 443 e chega até aqui ao servidor, aqui o apache vai ao mysql e solicita o que deseja. O mysql somente é acessado via localhost.

sudo nmap -v -sS localhost.

13. Instalar e configurar o Apparmor

É um software que melhora o kernel para isolamento de aplicativos. Este confinamento é provido por perfis de aplicativos do kernel.

Mais detalhes:
https://wiki.ubuntu.com/AppArmor
https://help.ubuntu.com/lts/serverguide/apparmor.html
https://help.ubuntu.com/community/AppArmor

Instalação
sudo apt-get install apparmor apparmor-profiles

Checar funcionamento
sudo apparmor_status
ou

sudo aa-status

14. Auditar segurança do sistema com Tiger e Tripwire

Tiger é uma ferramenta de segurança que pode ser usada para auditoria e detecção de intrusão do sistema.

Tripwire é um sistema de detecção de intrusão (HIDS) que checa a integridade de arquivos e pastas.

Detalhes
https://www.digitalocean.com/community/tutorials/how-to-use-tripwire-to-detect-server-intrusions-on-an-ubuntu-vps

Instalação

sudo apt install tiger tripwire

Responda sim para fornecer senha para arquivos e guarde bem as senhas

Criar banco de dados

sudo tripwire --init
Entre com a senha fornecida acima.

Criar arquivo de polícia
```
sudo twadmin --create-polfile /etc/tripwire/twpol.txt
```
Entre com a senha fornecida acima.

Executando tiger

sudo tiger

Toda a saída do tiger pode ser vista em:
/var/log/tiger

Para visualizar o relatório de segurança do tiver:
```
sudo less /var/log/tiger/security.report*
```

Aqui ele gerou este:
/var/log/tiger/security.report.ribafs.org.180214-20:50

15. Atualizar a disribuição

Atualizar automaticamente somente as atualizações 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

Atualiza o servidor manualmente pelo menos uma vez por dia.

16. Usar Senhas Fortes

De que vai adiantar ter todo este trabalho de escolher uma boa hospedagem, de isntalar um sistema operacional seguro, atualizar o sistema e efetuar diversas medidas para melhorar a segurança, nada vai adiantar se usarmos senhas fracas.

É como cagar e não limpar o c*.

Senhas fortes são grandes (8 dígitos ou mais) e usam uma mistura de algarismos, letras minúsculas, letras maiúsculas e símbolos.

17. Melhorando a segurança de sites com Joomla

O site está em
/var/www/html/portal

- Copiar configuration.php para o /var/www com o nome cfg.php
- Remover todo o conteúdo do /portal/configuration.php e deixar apenas estas duas linhas:

```
<?php
require_once( dirname( __FILE__ ) . '/../../cfg.php' );
```

Obs.: lembre de fazer o backup do arquivo cfg.php, que agora está fora do html.

18. Melhorar a segurança no Desktop

Melhorar a segurança no desktop é importane para maior segurança do servidor. Hábitos saudáveis como usar um sistema operacional seguro e atualizado, como usando o firewall ativo e fechando tudo que pode.

Assim como também instalando boas ferramentas de monitoramento do servidor.

Instalar no micro desktop o W3AF

apt-get install w3af

Traz uma interface para a console e uma gráfica/web

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

19. Melhorando a Segurança do MySQL

Uma forma de melhorar a segurança do mysql é criar usuários restritos, que somente tenham poder de agir num banco específico.

O exemplo abaixo é usado para criar um usuário a ser usado em site com Joomla:

mysql -u root -p
create database portal;

GRANT ALL PRIVILEGES ON portal.* TO portal@localhost IDENTIFIED BY 'senha' WITH GRANT OPTION;
\q

Importar Script:
mysql -u root -p portal < portal.sql

Exportar banco para script:
mysqldump -u root -p portal > portal.sql

Também importante é executar

mysql_secure_installation

20. Melhorando a segurança com Lynis

Executa diversos testes a procura de vulnerabilidade no sistema.

Instalação (abaixo é uma só linha)

```
wget -O - http://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add - > /dev/null

echo "deb [arch=amd64] https://packages.cisofy.com/community/lynis/deb/ trusty main" | sudo tee -a /etc/apt/sources.list.d/cisofy-lynis.list

sudo apt-get update
```

sudo apt install lynis

Atualização

sudo lynis --help

sudo lynis update info

Executando
sudo lynis audit system

Guarda os relatórios em
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat

Dica: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

Audit remoto

sudo lynis audit system remote ribafs.org

How to perform a remote scan:
  ============================
  Target : ribafs.org
  Command : ./lynis audit system --quick ribafs.org

  * Step 1: Create tarball
    mkdir -p ./files && cd .. && tar czf ./lynis/files/lynis-remote.tar.gz --exclude=files/lynis-remote.tar.gz ./lynis && cd lynis

* Step 2: Copy tarball to target ribafs.org
  scp -q ./files/lynis-remote.tar.gz ribafs.org:~/tmp-lynis-remote.tgz

* Step 3: Execute audit command
  ssh ribafs.org "mkdir -p ~/tmp-lynis && cd ~/tmp-lynis && tar xzf ../tmp-lynis-remote.tgz && rm ../tmp-lynis-remote.tgz && cd lynis && ./lynis audit system --quick ribafs.org"

* Step 4: Clean up directory
  ssh ribafs.org "rm -rf ~/tmp-lynis"

* Step 5: Retrieve log and report
  scp -q ribafs.org:/tmp/lynis.log ./files/ribafs.org-lynis.log
  scp -q ribafs.org:/tmp/lynis-report.dat ./files/ribafs.org-lynis-report.dat

* Step 6: Clean up tmp files (when using non-privileged account)
  ssh ribafs.org "rm /tmp/lynis.log /tmp/lynis-report.dat"

Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

21. Cuidados Extras

Busca por backdoors

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

Referência
https://geek.linuxman.pro.br/geek/ubuntu-pronto-para-guerra
https://www.thefanclub.co.za/how-to/how-secure-ubuntu-1604-lts-server-part-1-basics
https://linux-audit.com/ubuntu-server-hardening-guide-quick-and-secure/
https://hostpresto.com/community/tutorials/how-to-install-and-use-lynis-on-ubuntu-14-04/