Monitorando um servidor Linux Ubuntu 16.04

Espaço em disco
df -h

Memória RAM e Swap
free -m

Monitorar serviços na memória com sysv-rc-conf

Instalar
sudo apt install sysv-rc-conf

Testando se portas estão abertas
telnet smtp.gmail.com 587
telnet smtp.gmail.com 25

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

Monitorar login do root

sudo apt install mailutils

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

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

11 Varrendo portas abertas com Nmap

O nmap é um software para descobrir a rede e para auditar segurança. Melhor é instalar no desktop para varrer do mesmo.

Instalação
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.

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

- atualizar permissões do /var/www/html

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

Mysql /var/log/mysql
error.log

Outros /var/log

auth.log
fail2ban.log

mysql.err
mysql.log
syslog
user.log

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 bluetooth remove

Ferramentas para gerenciar serviços no boot

sysv-rc-conf - mostra todos os runlevel
rcconf - pode alterar, mas mostra poucos
chkconfig - só mostra, não altera

apt-get install sysv-rc-conf rcconf chkconfig

Desativar os serviços não usados

Usuários logados:
who

Usuário atual
whoami

Dividindo a tela em duas

Como dois terminais um acima e outro abaixo com o Splitvt

sudo apt install 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.

Usando htop

apt-get install htop

htop

Monitorando a rede

iptraf - monitorar a rede

apt-get install iptraf

Usando
iptraf

netstat -a
netstat -at
netstat -s

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)

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

Como saber que portas estão abertas
apt-get install nmap
nmap -v localhost
nmap -v 192.168.0.1

Instalar no desktop
sudo apt-get install wireshark

Monitorando logs

tail -f 50 /var/log/mail.log
less +F /var/mail.log

Monitorando a rede com ngrep
apt-get install ngrep
ngrep -h (help)

Usando:
Ficar escutando na porta 25
ngrep -d any port 25

Monitorar todas as atividades cruzando origem e destino da porta 25 (SMTP)
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 tráfico na rede baseado no syslog procurando a ocorrência da palavra ``error''.
ngrep -wi -d any 'user|pass' port 21

Monitorar qualquer tráfico cruzando origem e destino na porta 21
Origem: http://ngrep.sourceforge.net/usage.html

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/

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

apt install tiger tripwire

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

Criar banco de dados

tripwire --init
Entre com a senha fornecida acima.

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

Executando tiger

tiger

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

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

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