Logging

Rodrigo Arenas A.

roarenas@nic.cl

Logging

- ¿Que es?
  - Dejar registro de distintos eventos que suceden en nuestros sistemas
- ¿Quien registra?
  - Kernel, modulos, demonios, scripts
- ¿Como registrar?
  - Archivos, syslogd local, syslogd remoto
- ¿Niveles?
  - fatal, error, info, debug, warn, fatal

Logging

- Consideraciones de espacio
  - ¿Cuanta historia queremos guardar?
  - ¿Cada cuanto y que queremos registrar?
- ¿Donde?
  - /var/log
  - /var/syslog
  - /tmp
- ¿Archivos infinitos?
  - NO, rotacion

logrotate

```
    # see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# uncomment this if you want your log files compressed
compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own wtmp -- we'll rotate them here
/var/log/wtmp {
   monthly
   create 0664 root utmp
    rotate 1
}
/var/log/messages {
   rotate 5
   weekly
   postrotate
   /usr/bin/killall -HUP syslogd
  endscript
}
```

syslogd

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                 /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none          /var/log/messages
# The authpriv file has restricted access.
authpriv.*                              /var/log/secure
# Log all the mail messages in one place.
mail.*                                  -/var/log/maillog
# Log cron stuff
cron.*                                  /var/log/cron
```

maillog

Mar 29 14:17:32 mail postfix/smtpd[27007]: 69BDBCC8172: client=localhost.localdomain[127.0.0.1]

Mar 29 14:17:32 mail postfix/cleanup[26995]: 69BDBCC8172: message-id=<20110329171704.18AD31CF13@www.lacnic.net>

Mar 29 14:17:32 mail postfix/qmgr[2039]: 69BDBCC8172: from=<jpiquer@nic.cl>, size=1731, nrcpt=2 (queue active)

Mar 29 14:17:32 mail postfix/smtp[26300]: 5BEB1CC82E2: to=<furibe@nic.cl>, relay=127.0.0.1[127.0.0.1]: 10025, delay=0.11, delays=0.01/0/0.04/0.05, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 69BDBCC8172)

Mar 29 14:17:32 mail postfix/smtp[26300]: 5BEB1CC82E2: to=<roarenas@nic.cl>, relay=127.0.0.1[127.0.0.1]: 10025, delay=0.11, delays=0.01/0/0.04/0.05, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as 69BDBCC8172)

Mar 29 14:17:32 mail postfix/local[29188]: 69BDBCC8172: to=<furibe@mail.intra.nic.cl>, orig_to=<furibe@nic.cl>, relay=local, delay=0.16, delays=0.05/0/0/0.11, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail -a "$EXTENSION" DEFAULT=$HOME/Maildir/ MAILDIR=$HOME/Maildir)

Mar 29 14:17:32 mail postfix/local[26374]: 69BDBCC8172: to=<roarenas@mail.intra.nic.cl>, orig_to=<roarenas@nic.cl>, relay=local, delay=0.19, delays=0.05/0.02/0/0.12, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail -a "$EXTENSION" DEFAULT=$HOME/Maildir/ MAILDIR=$HOME/Maildir)

Mar 29 14:17:32 mail postfix/qmgr[2039]: 69BDBCC8172: removed

Detección de ataques I

Mar 29 12:29:58 base6.intra.nic.cl 350030: Mar 29 15:29:57.741: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 9027.e435.f0da Associated KEY_MGMT[NONE]

Mar 29 12:30:15 base6.intra.nic.cl 350031: Mar 29 15:30:14.614: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 9027.e435.f0da Reason: Sending station has left the BSS

Mar 29 12:37:05 base6.intra.nic.cl 350046: Mar 29 15:37:04.994: %DOT11-7-AUTH_FAILED: Station 18e7.f426.ba99 Authentication failed

Mar 29 12:42:58 base6.intra.nic.cl 350059: Mar 29 15:42:57.783: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station d8a2.5eb6.836a Reason: Sending station has left the BSS

Mar 29 12:42:58 base6.intra.nic.cl 350060: Mar 29 15:42:58.106: %DOT11-6-ASSOC: Interface Dot11Radio0, Station d8a2.5eb6.836a Reassociated KEY_MGMT[NONE]

Mar 29 12:48:29 base6.intra.nic.cl 350071: Mar 29 15:48:28.813: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 2421.abfa.b60f Associated KEY_MGMT[NONE]

Mar 29 12:50:35 base6.intra.nic.cl 350076: Mar 29 15:50:34.978: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 2421.abfa.b60f Reason: Sending station has left the BSS

Detección de ataques II, /var/log/secure

Mar 29 14:28:34 nicolette sshd[11800]: Invalid user admin from 121.78.84.100

Mar 29 14:28:34 nicolette sshd[11802]: input_userauth_request: invalid user admin

Mar 29 14:28:34 nicolette sshd[11800]: pam_unix(sshd:auth): check pass; user unknown

Mar 29 14:28:34 nicolette sshd[11800]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=121.78.84.100

Mar 29 14:28:35 nicolette sshd[11799]: Received disconnect from 89.212.91.211: 11: Bye Bye

Mar 29 14:28:35 nicolette sshd[11798]: Received disconnect from 121.78.84.100: 11: Bye Bye

Mar 29 14:28:36 nicolette sshd[11801]: Failed password for invalid user account from 121.78.84.100 port 50999 ssh2

Mar 29 14:28:36 nicolette sshd[11800]: Failed password for invalid user admin from 121.78.84.100 port 50995 ssh2

¿Que hacer con la info?

- Análisis forenses
  - grep, egrep, awk
  - less, more
- Alertas
  - logwatch
  - nagios

Logwatch /var/log/secure

- Revisa los determinados y sumariza info

Mar 29 14:28:34 nicolette sshd[11800]: Invalid user admin from 121.78.84.100

Mar 29 14:28:35 nicolette sshd[11798]: Received disconnect from 121.78.84.100: 11: Bye Bye

Mar 29 14:28:36 nicolette sshd[11801]: Failed password for invalid user account from 121.78.84.100 port 50999 ssh2

Mar 29 14:28:36 nicolette sshd[11800]: Failed password for invalid user admin from 121.78.84.100 port 50995 ssh2

- Salida

Failed logins from:

admin/password from 121.78.84.100: 453 time(s)

admin/password from 121.78.84.101: 350 time(s)

cron.d check_checksum

- Revisa checksum de archivos y programas determinados
  - /var/log/wtmp
  - /var/www/htmldoc/index.html
  - /etc/password, /etc/shadow
  - /etc/sysconfig/iptables
- Politicas
  - Apagar equipo
  - Avisar por email
  - Bajar servicios e ir a runlevel 2

Cambios de configuración en Routers RANCID,http://www.shrubbery.net/

- Obtiene configuraciones
  - routers
  - switchs
  - accesspoint
- Guarda configuraciones
  - CVS
  - SVN
- Obtiene diferencias
- Avisa cambios
  - mail
  - nagios

Cambios de configuración en Routers RANCID,http://www.shrubbery.net/

From: rancid <rancid@example.com>
To: rancid-example@example.com
Subject: example router config diffs
Precedence: bulk

Index: configs/dfw.example.com
==========
retrieving revision 1.144
diff -u -4 -r1.144 dfw.example.com
@@ -57,14 +57,8 @@
 !Slot 2/MBUS: hvers 1.1
 !Slot 2/MBUS: software 01.36 (RAM) (ROM version is 01.33)
 !Slot 2/MBUS: 128 Mbytes DRAM, 16384 Kbytes SDRAM
 !
- !Slot 6: 1 Port Gigabit Ethernet
- !Slot 6/PCA: part 73-3302-03 rev C0 ver 3, serial CAB031216OL
- !Slot 6/PCA: hvers 1.1
- !Slot 6/MBUS: part 73-2146-07 rev B0 dev 0, serial CAB031112SB
- !Slot 6/MBUS: hvers 1.2
- !Slot 6/MBUS: software 01.36 (RAM) (ROM version is 01.33)
 !Slot 7: Route Processor
 !Slot 7/PCA: part 73-2170-03 rev B0 ver 3, serial CAB024901SI
 !Slot 7/PCA: hvers 1.4
 !Slot 7/MBUS: part 73-2146-06 rev A0 dev 0, serial CAB02060044
@@ -136,11 +130,8 @@
 boot system flash slot0:
 logging buffered 32768 debugging
 no logging console
 enable secret 5 $1$73Y1$grXuRjuZxfSiLYv1sBRUz0