

Logging and Log Analysis - The Essential

kamal hilmi othman

NISER

Series

1. **Logging and Log Analysis - The Essential**
2. TCP/IP - Packet Analysis
3. Network Security Monitoring - Using Snort
4. Honeypot / HoneyNet Systems – Tracking Intruder
5. Intrusion Detection and Prevention Systems

* Normally each topic is meant for 2 to 3 days, today, i'm taking only 30 mins!!

Philosophy

- Log Analysis
 - It is an active or continuous attempt to detect intrusive activity
- Process
 - Event -> Analyzed -> Information

Microscope ?

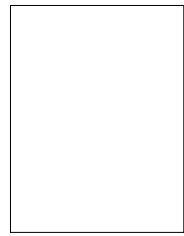
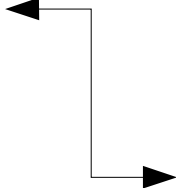
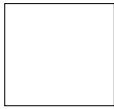
- Simple
 - Because they are there
- Complex
 - Policy
 - System Security
 - System Availability and Configuration

Log Component

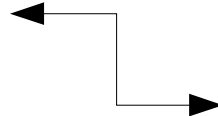
- Data Sources
 - Some is operating system dependent
 - Some require 'code reading'
- Transport
 - Mechanism
 - Project in 'securing' the transport
- Storage
 - File System
 - Rotation
 - <http://www.ietf.org/internet-drafts/draft-ietf-syslog-sign-14.txt>

The Big Picture

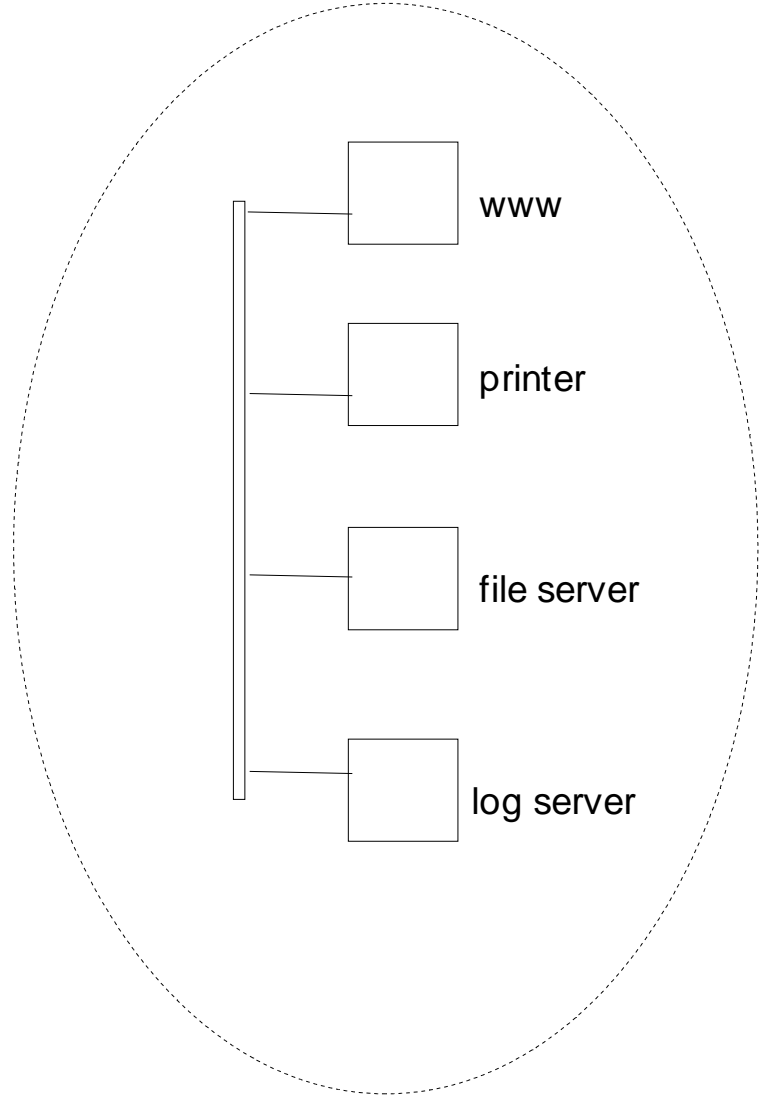
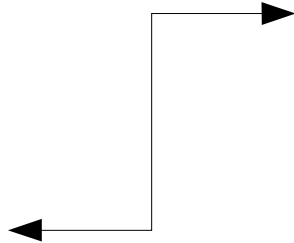
Branch2-log server



Central-log server



Branch3-log server



www

printer

file server

log server

Where to start ?

- Logging Device as follows:
 - Firewalls
 - Web server
 - DHCP server
 - Web cache proxies
 - Mail server
 - Router and switches
 - Custom

Example Log

- Cisco Router

Jul 20 14:59:32 router 20: *Mar 1 01:39:25: %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.6.160)

Jul 20 15:01:07 router 21: *Mar 1 01:41:00: %SYS-5-CONFIG_I: Configured from console by vty0 (10.1.6.160)

Jul 20 15:10:43 router 22: *Mar 1 01:50:36: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 10.1.6.165

Jul 20 15:18:06 router 24: *Mar 1 01:57:58: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 10.1.6.165

Jul 20 15:18:06 router 25: *Mar 1 01:57:59: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 10.1.6.165

- Remote Apache logging

Jul 18 16:49:27 mapmin.tonjol.org httpd[779]: [error] [client 202.56.224.218] File does not exist: /htdocs/default.ida

Jul 18 23:53:28 mapmin.tonjol.org httpd[30023]: [error] [client 202.197.181.203] File does not exist: /htdocs/default.ida

Jul 20 00:39:32 mapmin.tonjol.org httpd[21509]: [error] [client 202.101.159.163] request failed: URI too long

Jul 21 05:06:39 mapmin.tonjol.org httpd[11348]: [error] [client 202.138.123.1] File does not exist: /htdocs/scripts/nsiislog.dll

Jul 21 05:06:39 mapmin.tonjol.org httpd[11348]: [error] [client 202.138.123.1] File does not exist: /htdocs/scripts/nsiislog.dll

Example Log (cont)

- Sudo

Jul 22 22:15:36 niser229 sudo: khilmi : user NOT in sudoers ; TTY=ttyfb ; PWD=/usr/home/khilmi ; USER=root ;
COMMAND=/sbin/reboot

Jul 22 22:15:36 niser229 sudo: khilmi : user NOT in sudoers ; TTY=ttyfb ; PWD=/usr/home/khilmi ; USER=root ;
COMMAND=/sbin/reboot

Jun 23 12:30:42 mybox.tonjol.org sudo: kamalrul : TTY=tty3 ; PWD=/home ; USER=root ; COMMAND=/usr/bin/su - saliman

Jun 23 13:31:01 mybox.tonjol.org sudo: kamalrul : 1 incorrect password attempt ; TTY=tty3 ; PWD=/home ; USER=root ;
COMMAND=/usr/bin/su - saliman

Jun 25 08:54:36 mybox.tonjol.org sudo: saliman : user NOT in sudoers ; TTY=tty0 ; PWD=/ ; USER=root ;
COMMAND=/usr/bin/find . -name snort

Jun 25 08:54:36 mybox.tonjol.org sudo: saliman : user NOT in sudoers ; TTY=tty0 ; PWD=/ ; USER=root ;
COMMAND=/usr/bin/find . -name snort

Jul 19 12:58:18 mybox.tonjol.org sudo: saliman : 3 incorrect password attempts ; TTY=tty0 ; PWD=/home/saliman ; USER=root
; COMMAND=/usr/bin/vi /etc/syslog.conf

Example Log (cont)

- Application

Jul 20 10:24:47 niser229 gaim: stack overflow in function yahoo_web_pending

Jul 20 10:24:47 niser229 gaim: stack overflow in function yahoo_web_pending

- SSH

Jun 29 14:22:01 ikanbuntal sshd: refused connect from 66.98.156.55

Jul 3 03:13:18 ikanbuntal sshd: refused connect from 199.106.89.58

sshd[6169]: fatal: Local: Corrupted check bytes on input.

sshd[6253]: fatal: Local: crc32 compensation attack: network attack detected

Example Log (cont)

- Solaris System

May 16 22:46:08 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Segmentation Fault - core dumped

May 16 22:46:21 victim-host last message repeated 7 times

May 16 22:46:22 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Bus Error - core dumped

May 16 22:46:24 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Segmentation Fault - core dumped

May 16 22:46:56 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Bus Error - core dumped

May 16 22:46:59 victim-host last message repeated 1 time

May 16 22:47:02 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Segmentation Fault - core dumped

May 16 22:47:07 victim-host last message repeated 3 times

May 16 22:47:09 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Hangup

May 16 22:47:11 victim-host inetd[600]: /usr/lib/fs/cachefs/cachefs: Segmentation Fault - core dumped

Example Log (cont)

- Solaris System

Jun 19 06:22:17 kaputbox su: [ID 810491 auth.crit] 'su root' failed for test on /dev/pts/1

Jun 19 06:26:17 kaputbox halt: [ID 662345 auth.crit] halted by test

Jun 19 06:26:17 kaputbox syslogd: going down on signal 15

Jun 21 07:14:19 kaputbox in.ftpd[20747]: [ID 120637 daemon.warning] softup (bogus) LOGIN FAILED [from 211.142.52.86]

Jun 21 07:14:22 kaputbox in.ftpd[20749]: [ID 120637 daemon.warning] up (bogus) LOGIN FAILED [from 211.142.52.86]

Jun 21 07:14:28 kaputbox in.ftpd[20752]: [ID 120637 daemon.warning] upload (bogus) LOGIN FAILED [from 211.142.52.86]

Syslog

- RFC 3164
- Widely use
- Standard logging transport for 'Unix'
- Great API (Simplicity)
- Uncontrolled and unverified data stream
- Unreliable transport

Syslog (cont)

- Component

syslogd

- UDP
- Configurable and Flexible
- Plain text

newsyslog (BSD)

- Configurable and Flexible
- Moves old messages to `.[0-9].gz` and expire them

Syslog (cont)

- Association

Facility

- part of the system generating the message.
- keywords: auth, authpriv, console, cron, daemon, ftp, kern, lpr, mail, mark, news, ntp, security, syslog, user, uucp and local0 through local7.

Level

- severity of the message
- keywords: emerg, alert, crit, err, warning, notice, info and debug.

Syslog (cont)

- Logging

Local

/etc/syslog.conf

facility.level <Tab><Tab> action

action – local file, user, remote host, console

Remote

facility.level <Tab><Tab> @loghost

good practice: root, @ loghost

Syslog (cont)

- Securing Your Syslog Server
 - Filter the incoming
 - Secure tunneling
 - Hard to delete
 - Re-compile syslog
 - Host protection

Syslog (cont)

- Detail (FreeBSD 4*)
 - /usr/src/usr.sbin/syslogd/syslogd.c
 - /usr/src/sys/sys/syslog.h
 - man syslog
 - man syslogd
 - man newsyslog
 - man logger

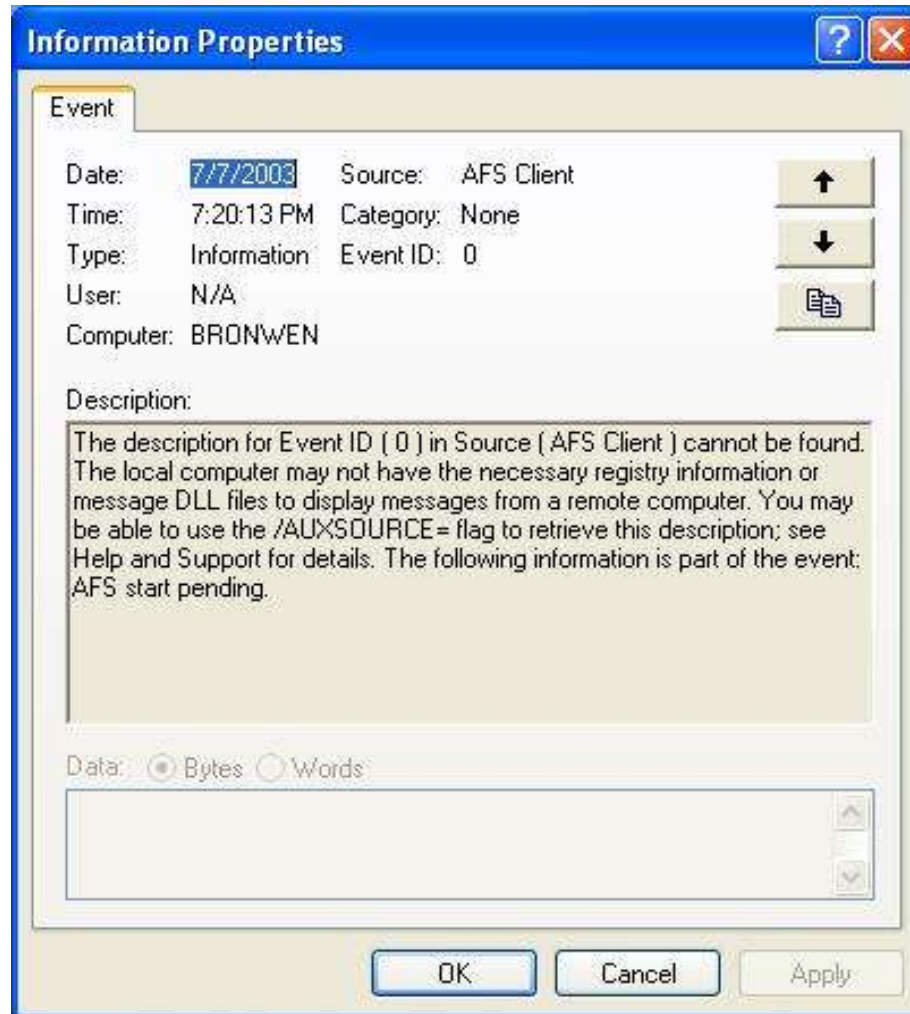
Syslog (cont)

- Syslog replacement
 - Syslog-Ng
 - Minirsyslogd

Windows System Logs

- No build-in remote logging capability
- Binary file
- Detail message
- Application and System Event Log

Windows System Logs (cont)



Windows System Logs (cont)



The screenshot shows a Windows Event Viewer window titled "Event Detail". The window has a dark blue title bar with a close button (X) on the right. The main content area is light gray and contains the following information:

Date:	7/10/01	Event ID:	7001
Time:	10:30:39 AM	Source:	Service Control Manager
User:	N/A	Type:	Error
Computer:	CISSVMAIL1	Category:	None

Below the metadata, there is a section labeled "Description:" with a vertical scrollbar on the right. The text in the description box reads:

The Microsoft Exchange Information Store service depends on the Microsoft Exchange Directory service which failed to start because of the following error:
The operation completed successfully.

Windows System Logs (cont)

- Remote logging
 - Event Reporter
 - BackLog
 - Ntsyslog
 - Kiwi Syslog (client)

Logging Architecture

- Build your own!
- Design Principal
 - Push
 - Each host sending logdata on-time or on selected interval
 - Pull
 - Run fetch process from log server to collect logs from a list of systems

Logging Architecture (cont)

- Push
 - Pro
 - Quickly transmits
 - Great scale
 - Con
 - Using syslog – subject to data lost
 - Server doesn' t track client status (otherwise monitor)

Logging Architecture (cont)

- Pull

- Pro

- Log is not lost when server is down
 - Decision on server – when to collect
 - Server could detect client status

- Con

- If client is compromised before log is transferred, they maybe lost
 - Require per-machine configuration

Building Log Process

- Matching
 - Pattern matching
 - May completely or partially contain the pattern.
- Normalization
 - Take a log message and match them against templates, common dictionary.
- Signatures
 - Matching rule coupled to an alert.
 - 2 ways
 - Look for all the known stuff (aka IDS)
 - Throw away all the known (aka artificial ignorance approach)

Known Stuff

- Community info
- Pattern Matching
- Tweak, tweak, tune, tune

Artificial Ignorance (MJR Stuff)

- <http://honor.trusecure.com/pipermail/firewall-wizards/1997-September/001324.html>
- Log processing technique of determining step-wise what to ignore.
- Everything not uninteresting **must** be interesting.

Analysis Principal

- Baselining
- Thresholding
- What's Interesting?
- What to look for
- Other supporting log to look for

Baselining

- What's normal ?
 - How many applications / facilities / system report to loghost ?
 - Top ten most frequent – is a good start
 - Network traffic protocol and DNS request
 - Log amount per hour/day
 - Number of processes running at any time

Thresholding

- From baseline , what's weird ?
- Number of times that event happen in a given time period.
- Notify when a message doesn't appear!!

What's Interesting ?

- It depends!
- Need to know your environment – application, system, hardware, security alert
- What is your expected behavior?.. in order to get to know suspicious behavior
- Normal know – find weird
- Statistical output

What to Look for

Some example

- Passwords changed by someone other than user
- Process dying
- Long messages full of random characters
- Unexpected configuration changes
- Least frequent message
- Message with words – fatal, panic
- Failed logon from non-local domain
- Sudden increase or decrease
- Single event

Syslog Quick Watch (DIY)

- Test processing tool
 - awk
 - sed
 - grep
 - shell utilities
 - Perl , esp Regex
- Plotting
 - gnuplot

Syslog Quick Watch (DIY) (cont)

- Processing ('artificial ignorance approach')

```
khilmi@logsvr$ more jun-log | wc -l
```

```
76517
```

```
khilmi@logsvr$
```

```
khilmi@logsvr$ cat jun-log | grep -iv restart | grep -iv newsyslog | grep -v cmd | grep -iv sm-mta | grep -iv  
sendmail | grep -iv /bsd | grep -iv /kernel | grep -iv crontab | grep -iv cron | wc -l
```

```
188
```

```
khilmi@logsvr$
```

- Filter message against a pattern list of uninteresting stuff
- Uses several weeks/months' logs
- Tune, tune, tune

Syslog Quick Watch (DIY) (cont)

- Alert

- Swatch <http://swatch.sourceforge.net/>

- Conf file:

```
watchfor /SYN-FIN/
```

```
    mail addressess=0199999999@sms.celcom.com.my
```

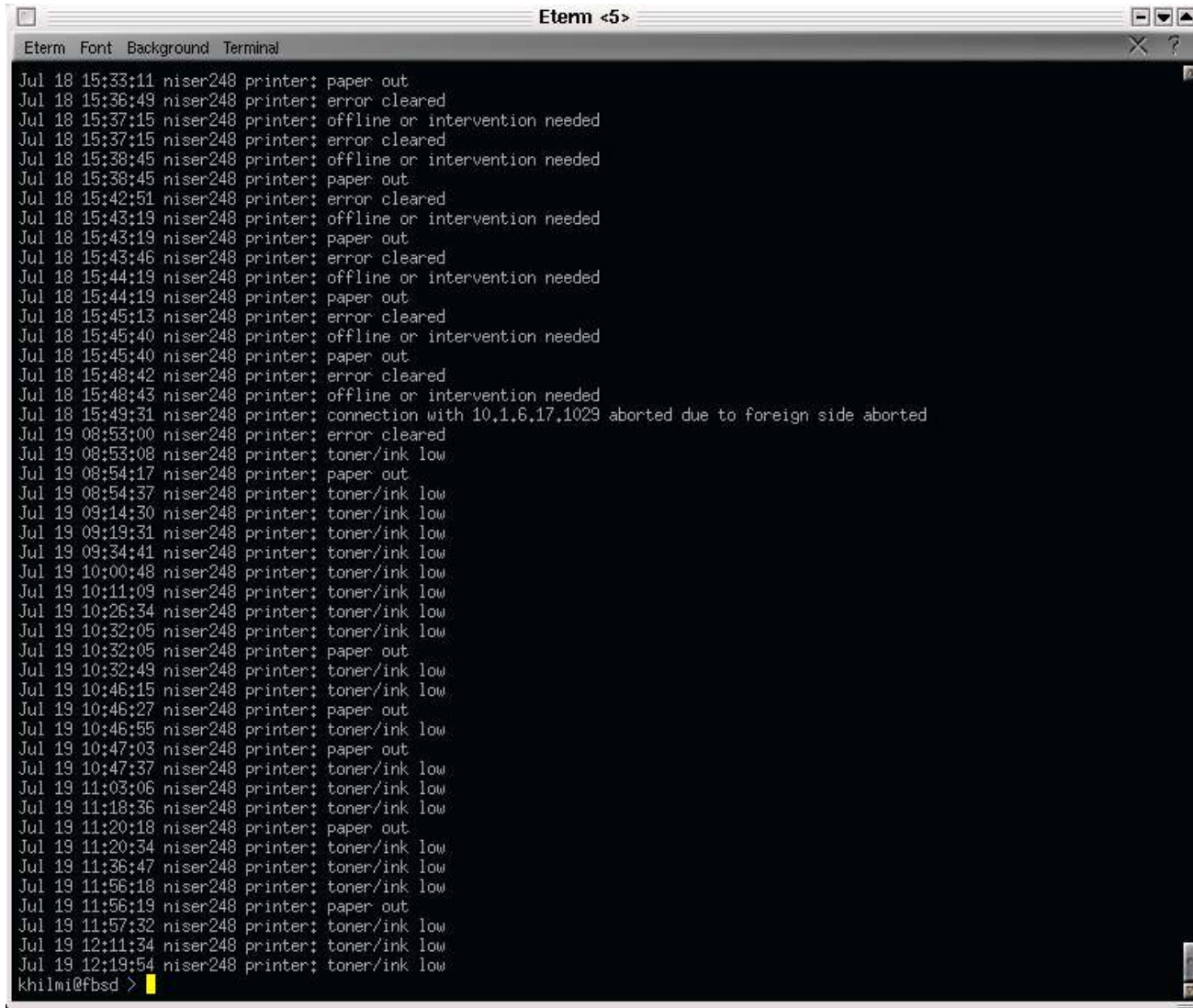
```
watchfor /SYN/
```

```
    mail addressess=0199999999@sms.celcom.com.my
```

```
watchfor /apache-chunking:/
```

```
    mail=alert,subject=apache chunking
```

Watching your printer



The image shows a terminal window titled "Eterm <5>". The terminal displays a series of log entries for a printer named "niser248". The logs are timestamped and include the following messages:

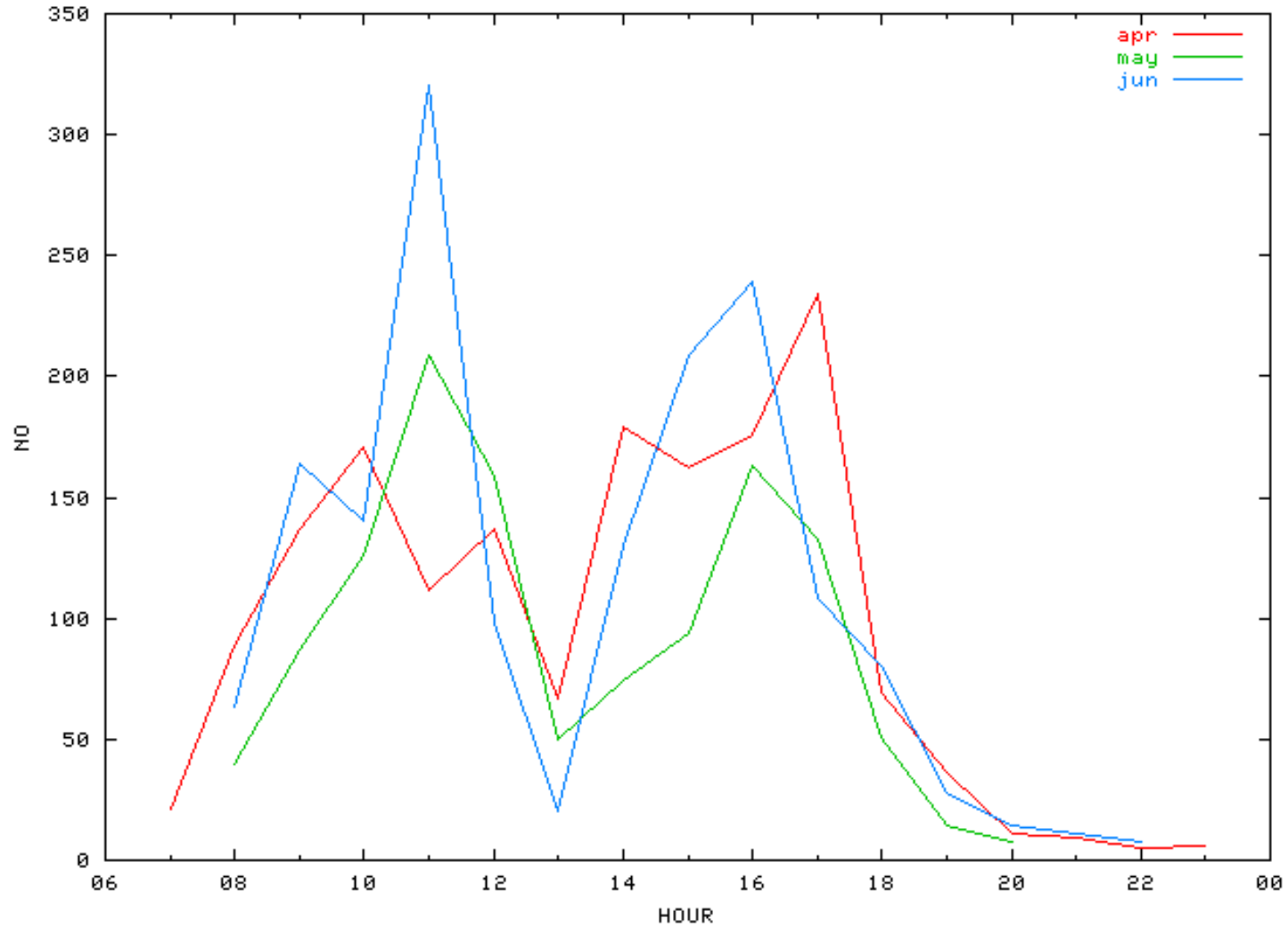
```
Jul 18 15:33:11 niser248 printer: paper out
Jul 18 15:36:49 niser248 printer: error cleared
Jul 18 15:37:15 niser248 printer: offline or intervention needed
Jul 18 15:37:15 niser248 printer: error cleared
Jul 18 15:38:45 niser248 printer: offline or intervention needed
Jul 18 15:38:45 niser248 printer: paper out
Jul 18 15:42:51 niser248 printer: error cleared
Jul 18 15:43:19 niser248 printer: offline or intervention needed
Jul 18 15:43:19 niser248 printer: paper out
Jul 18 15:43:46 niser248 printer: error cleared
Jul 18 15:44:19 niser248 printer: offline or intervention needed
Jul 18 15:44:19 niser248 printer: paper out
Jul 18 15:45:13 niser248 printer: error cleared
Jul 18 15:45:40 niser248 printer: offline or intervention needed
Jul 18 15:45:40 niser248 printer: paper out
Jul 18 15:48:42 niser248 printer: error cleared
Jul 18 15:48:43 niser248 printer: offline or intervention needed
Jul 18 15:49:31 niser248 printer: connection with 10.1.6.17,1029 aborted due to foreign side aborted
Jul 19 08:53:00 niser248 printer: error cleared
Jul 19 08:53:08 niser248 printer: toner/ink low
Jul 19 08:54:17 niser248 printer: paper out
Jul 19 08:54:37 niser248 printer: toner/ink low
Jul 19 09:14:30 niser248 printer: toner/ink low
Jul 19 09:19:31 niser248 printer: toner/ink low
Jul 19 09:34:41 niser248 printer: toner/ink low
Jul 19 10:00:48 niser248 printer: toner/ink low
Jul 19 10:11:09 niser248 printer: toner/ink low
Jul 19 10:26:34 niser248 printer: toner/ink low
Jul 19 10:32:05 niser248 printer: toner/ink low
Jul 19 10:32:05 niser248 printer: paper out
Jul 19 10:32:49 niser248 printer: toner/ink low
Jul 19 10:46:15 niser248 printer: toner/ink low
Jul 19 10:46:27 niser248 printer: paper out
Jul 19 10:46:55 niser248 printer: toner/ink low
Jul 19 10:47:03 niser248 printer: paper out
Jul 19 10:47:37 niser248 printer: toner/ink low
Jul 19 11:03:06 niser248 printer: toner/ink low
Jul 19 11:18:36 niser248 printer: toner/ink low
Jul 19 11:20:18 niser248 printer: paper out
Jul 19 11:20:34 niser248 printer: toner/ink low
Jul 19 11:36:47 niser248 printer: toner/ink low
Jul 19 11:56:18 niser248 printer: toner/ink low
Jul 19 11:56:19 niser248 printer: paper out
Jul 19 11:57:32 niser248 printer: toner/ink low
Jul 19 12:11:34 niser248 printer: toner/ink low
Jul 19 12:19:54 niser248 printer: toner/ink low
khilmi@fbbsd >
```

Watching your printer (cont)

- Log Uniq
 - Jul 14 10:11:57 niser248 printer: cover/door open
 - Jul 19 08:53:00 niser248 printer: error cleared
 - Jul 18 15:48:43 niser248 printer: offline or intervention needed
 - Jul 7 11:48:54 niser248 printer: output full
 - Jul 12 17:38:13 niser248 printer: paper jam
 - Jul 19 11:56:19 niser248 printer: paper out
 - Jul 19 12:19:54 niser248 printer: toner/ink low
 - Jul 18 15:49:31 niser248 printer: connection with 10.1.6.X.1029 aborted due to foreign side aborted
 - Jul 6 11:14:22 niser248 printer: connection with 10.1.6.X.1407 aborted due to idle timeout

Watching your printer (cont)

printer utilisation per hour for apr - jun 2004



Generic Process

- Design Process
 - Server - separate file systems
 - Priority and Event
 - Rotation
 - Enterprise or Multiple Site
- Policy Creation
 - Know your system!
- Build
 - Test and test and test
 - Document it!

Avoid This!

1. Collecting it and not looking at it
2. Watching logs from perimeter systems while ignoring internal systems
3. Designing your log architecture before you decide what you are going to collect
4. Only looking for what you know you want to find instead of just looking to see what you find

Golden Rule

Look for anything ...

....that appears out of ordinary.

Reference

- Book – none , few are covered in System Administrator guide.
- Website - <http://www.loganalysis.org>
- Mailing List -
<http://lists.shmoo.com/mailman/listinfo/loganalysis>

end()

thanks

khilmi at niser.org.my