Secure Logging & Network Monitoring

ra1nb0w & A6U

24 Ottobre 2009

LINUX DAY ITALIA

Chi siamo?

- Studenti di Sicurezza Informatica presso l'Universita' degli Studi di Milano (DTI).
- ...

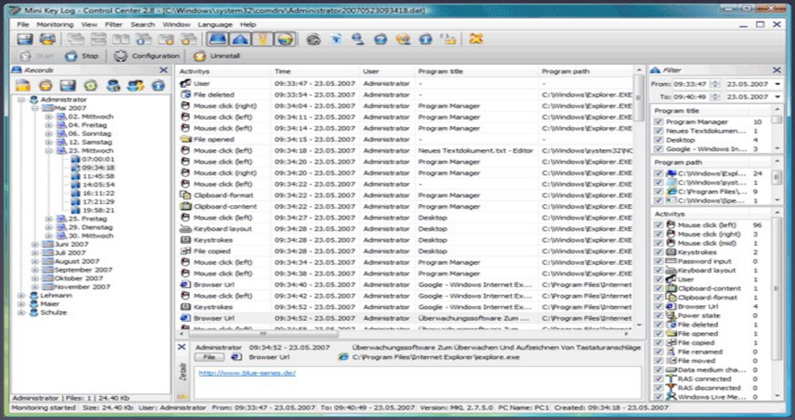
Di cosa parleremo...

- cos'e' un log e che informazioni contiene
- tipologie dei log e loro formati
- logging in *nix
- controllo degli accessi (tools)
- controllo del traffico in una rete
- logging centralizzato
- tools di management
- correlazione
- sistemi SIM (Security Information Management)

Cos'e' un log?

LOG

- Da wikipedia:
- “Con il significato di giornale di bordo, su cui vengono registrati gli eventi in ordine cronologico il termine è stato importato nell'informatica (1963) per indicare:
    - la registrazione cronologica delle operazioni man mano che vengono eseguite
    - il file su cui tali registrazioni sono memorizzate.”



Activitys	Time	User	Program title	Program path
User	09:33:47 - 23.05.2007	Administrator	-	-
File deleted	09:33:54 - 23.05.2007	Administrator	-	C:\Windows\Explorer.EXE
Mouse click (right)	09:34:04 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Mouse click (left)	09:34:11 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Mouse click (left)	09:34:14 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
File opened	09:34:15 - 23.05.2007	Administrator	-	-
Mouse click (left)	09:34:18 - 23.05.2007	Administrator	Neues Textdokument.txt - Editor	C:\Windows\system32\NC
Mouse click (left)	09:34:20 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Mouse click (right)	09:34:20 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Mouse click (left)	09:34:22 - 23.05.2007	Administrator	-	C:\Windows\Explorer.EXE
Clipboard-format	09:34:22 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Clipboard-content	09:34:22 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Mouse click (left)	09:34:27 - 23.05.2007	Administrator	Desktop	C:\Windows\Explorer.EXE
Keyboard layout	09:34:28 - 23.05.2007	Administrator	Desktop	C:\Windows\Explorer.EXE
Keystrokes	09:34:28 - 23.05.2007	Administrator	Desktop	C:\Windows\Explorer.EXE
File copied	09:34:28 - 23.05.2007	Administrator	Desktop	C:\Windows\Explorer.EXE
Mouse click (left)	09:34:34 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Mouse click (left)	09:34:38 - 23.05.2007	Administrator	Program Manager	C:\Windows\Explorer.EXE
Browser Url	09:34:40 - 23.05.2007	Administrator	Google - Windows Internet Ex...	C:\Program Files\Internet
Mouse click (left)	09:34:42 - 23.05.2007	Administrator	Google - Windows Internet Ex...	C:\Program Files\Internet
Keystrokes	09:34:52 - 23.05.2007	Administrator	Google - Windows Internet Ex...	C:\Program Files\Internet
Browser Url	09:34:52 - 23.05.2007	Administrator	Überwachungssoftware Zum ...	C:\Program Files\Internet

Administrator 09:34:52 - 23.05.2007 Überwachungssoftware Zum Überwachen Und Aufzeichnen Von Tastaturanschläge
Browser Url C:\Program Files\Internet Explorer\iexplore.exe
http://www.blue-series.de/

From: 09:33:47 23.05.2007
To: 09:40:49 23.05.2007

Program title	
☑ Program Manager	10
☑ Neues Textdokumen...	1
☑ Desktop	4
☑ Google - Windows In...	3

Program path	
☑ C:\Windows\Expl...	24
☑ C:\Windows\syst...	1
☑ C:\Program Files\...	9
☑ C:\Windows\Spe...	1

Activitys	
☑ Mouse click (left)	96
☑ Mouse click (right)	3
☑ Mouse click (mid)	1
☑ Keystrokes	2
☑ Password input	0
☑ Keyboard layout	1
☑ User	1
☑ Clipboard-content	1
☑ Clipboard-format	1
☑ Browser Url	4
☑ Power state	0
☑ File deleted	1
☑ File opened	1
☑ File copied	1
☑ File renamed	0
☑ File moved	0
☑ Data medium cha...	0
☑ RAS connected	0
☑ RAS disconnected	0
☑ Windows Live Me...	0

Administrator | Files: 1 | 24.40 Kb
Monitoring started | Size: 24.40 Kb | User: Administrator | From: 09:33:47 - 23.05.2007 | To: 09:40:49 - 23.05.2007 | Version: MKL 2.7.5.0 | PC Name: PC1 | Created: 09:34:18 - 23.05.2007

A cosa serve un log?

- Il log più semplice, è un file sequenziale sempre aperto in append, che viene chiuso e conservato a cadenze regolari e reso disponibile per:
    - analisi delle segnalazioni di errore
    - produzione di statistiche di esercizio
    - ripristino di situazioni precedenti
    - analisi delle modifiche o delle operazioni fatte e dei responsabili di tali operazioni
    - riassunto di quanto successo in un determinato arco di tempo (ad esempio nelle chat).

Tipi di log

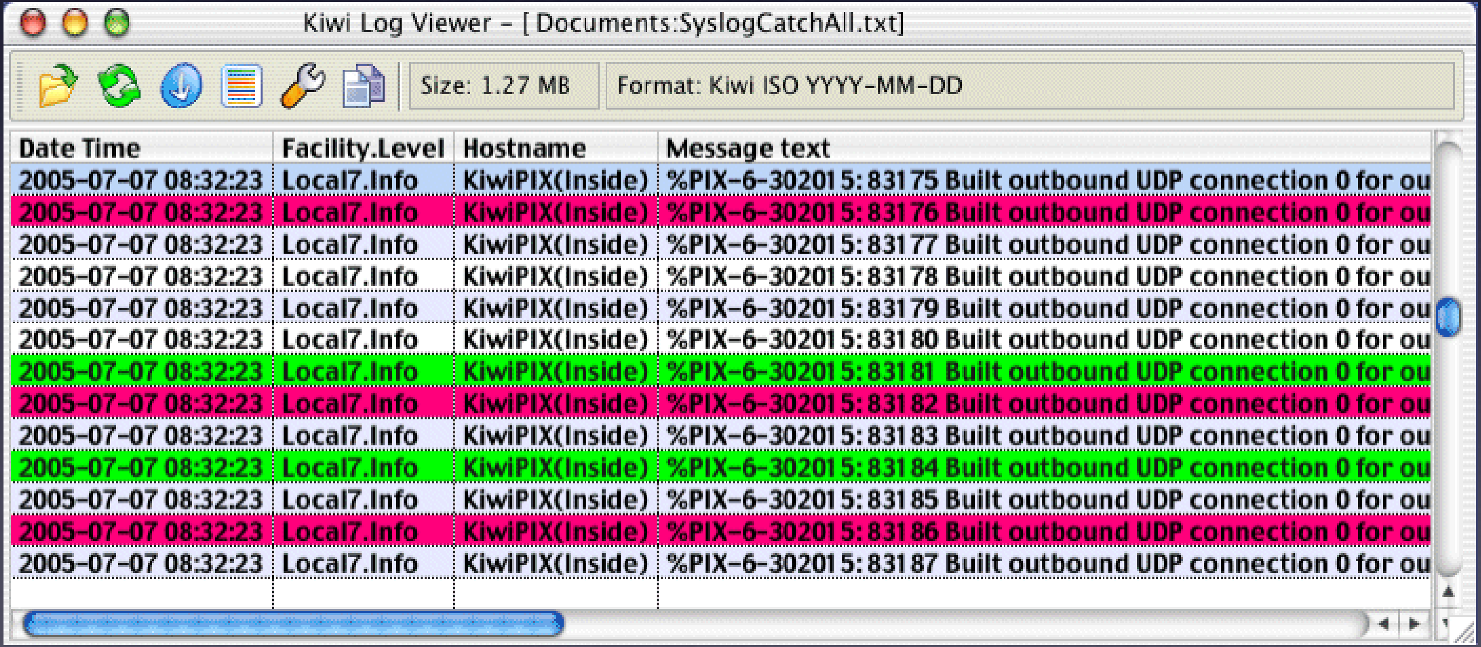
- *System log*:
  - i servizi di rete memorizzano gli eventi significativi che accadono nel sistema.
- *Application log:*
  - molte applicazioni prevedono i propri log su cui sono registrati eventi caratteristici dell'applicazione.
- *Database log:*
  - in questo caso è il sistema gestore di base dati (DBMS) che registra le operazioni fatte sulla base dati. (atomicita')

Livello di verbosity dei log

- debug: messaggi utili al debug;
- info: informazioni generali;
- notice: condizioni normali ma significative;
- warn: warning;
- error: errori generali
- crit: condizioni critiche;
- alert: bisogna provvedere immediatamente;
- emerg/fatal: il sistema è in grave pericolo;

Informazioni contenute in un log

- Timestamp
- Eventi
- Sorgente / Destinazione [IP]
- Protocolli / Applicazione
- Livello
- ....



Kiwi Log Viewer – [Documents:SyslogCatchAll.txt]

Size: 1.27 MB

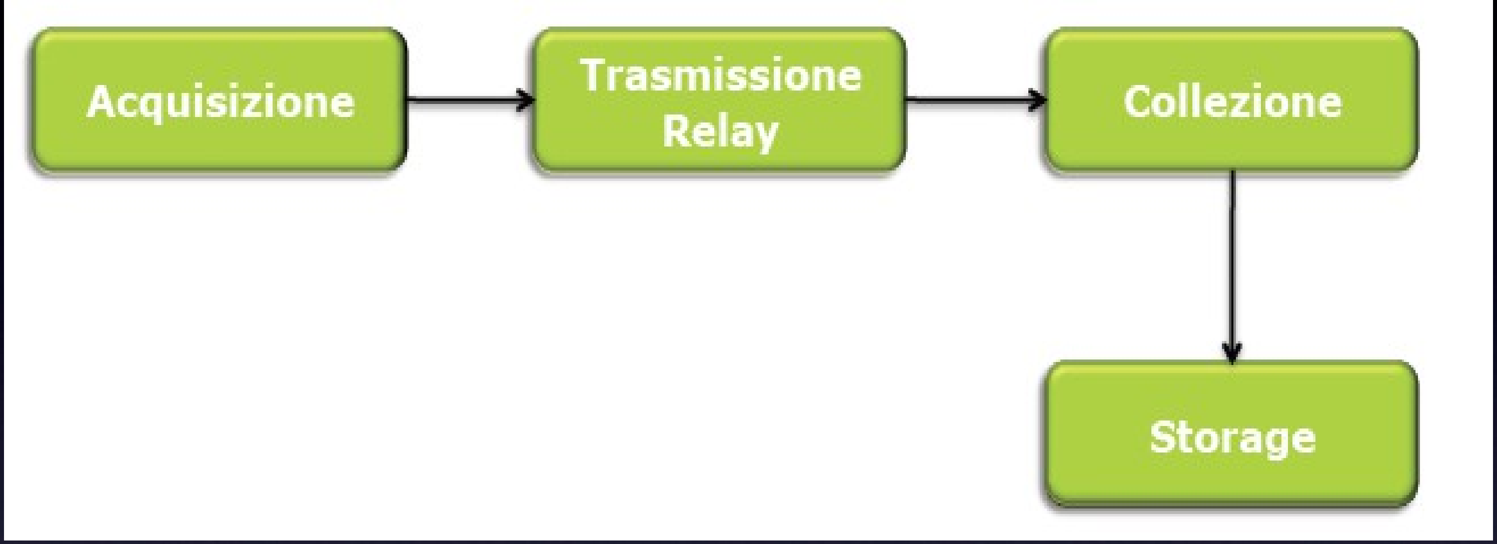
Format: Kiwi ISO YYYY-MM-DD

Date Time	Facility.Level	Hostname	Message text
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83175 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83176 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83177 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83178 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83179 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83180 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83181 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83182 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83183 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83184 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83185 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83186 Built outbound UDP connection 0 for ou
2005-07-07 08:32:23	Local7.Info	KiwiPIX(Inside)	%PIX-6-302015: 83187 Built outbound UDP connection 0 for ou

ldap log example

```
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149973 SEARCH RESULT tag=101 err=0
nentries=0 text=
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149974 SRCH
base="ou=DNS,dc=home,dc=irh,dc=it" scope=2 deref=0 filter="(&(zoneName=home.irh.it)
(relativeDomainName=sip.ciaociao.it))"
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149974 SEARCH RESULT tag=101 err=0
nentries=0 text=
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149975 SRCH
base="ou=DNS,dc=home,dc=irh,dc=it" scope=2 deref=0 filter="(&(zoneName=home.irh.it)
(relativeDomainName=_udp.sip.ciaociao.it))"
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149975 SEARCH RESULT tag=101 err=0
nentries=0 text=
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149976 SRCH
base="ou=DNS,dc=home,dc=irh,dc=it" scope=2 deref=0 filter="(&(zoneName=home.irh.it)
(relativeDomainName=_sip._udp.sip.ciaociao.it))"
Oct 11 14:37:02 ciccio slapd[25269]: conn=3388 op=149976 SEARCH RESULT tag=101 err=0
nentries=0 text=
```

Problematiche di gestione

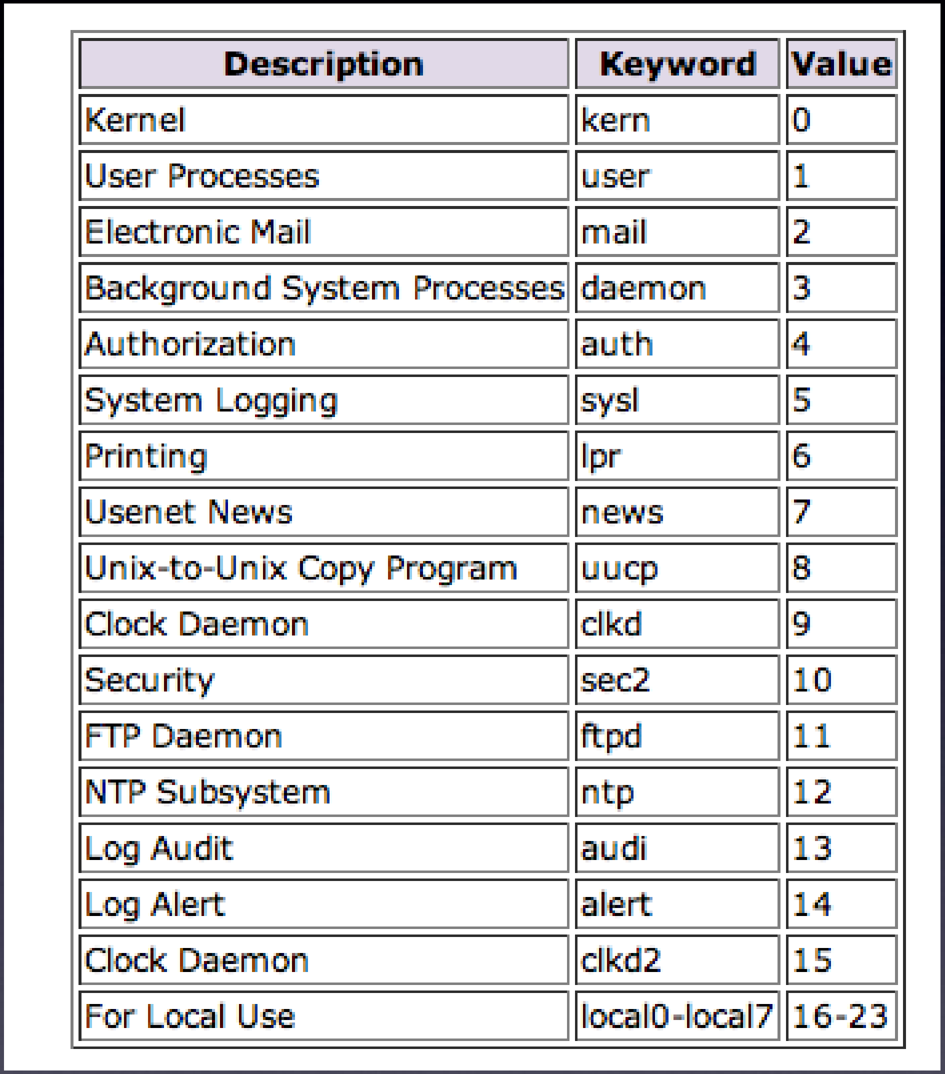


- Integrita'
- Autenticita'
- Time Stamping (sincronizzazione)

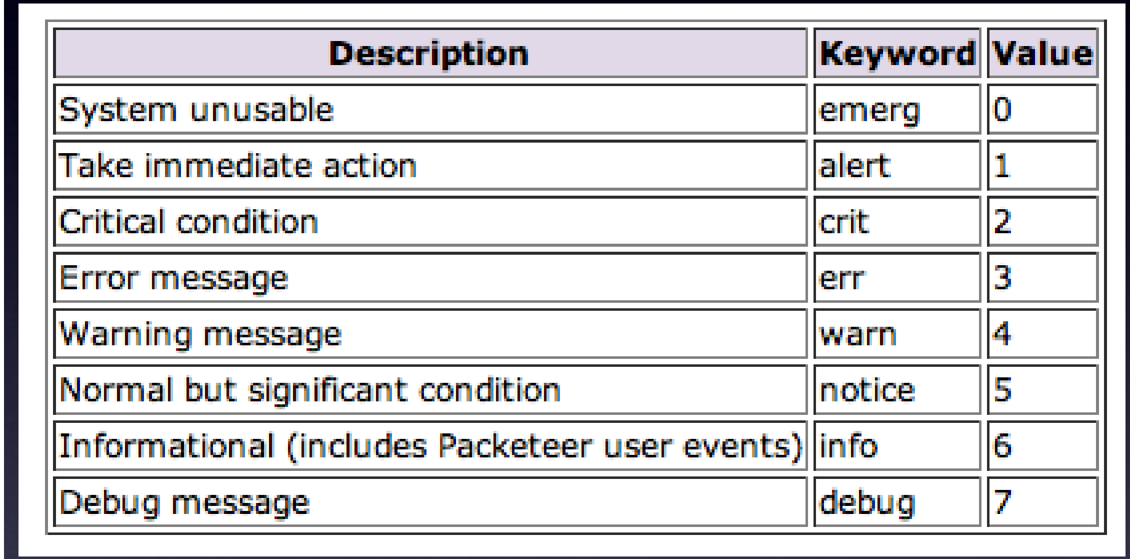
Syslog

- Sicuramente il protocollo piu' diffuso e utilizzato
- Possibilita' di uso con ssl/tls (a pagamento)
- Formato human-readable
- Standard regolamentato dalla RFC 3164
- Protocollo UDP (porta 514)
- Utilizzo del demone syslogd
- Facility / Severity

Facility / Severity

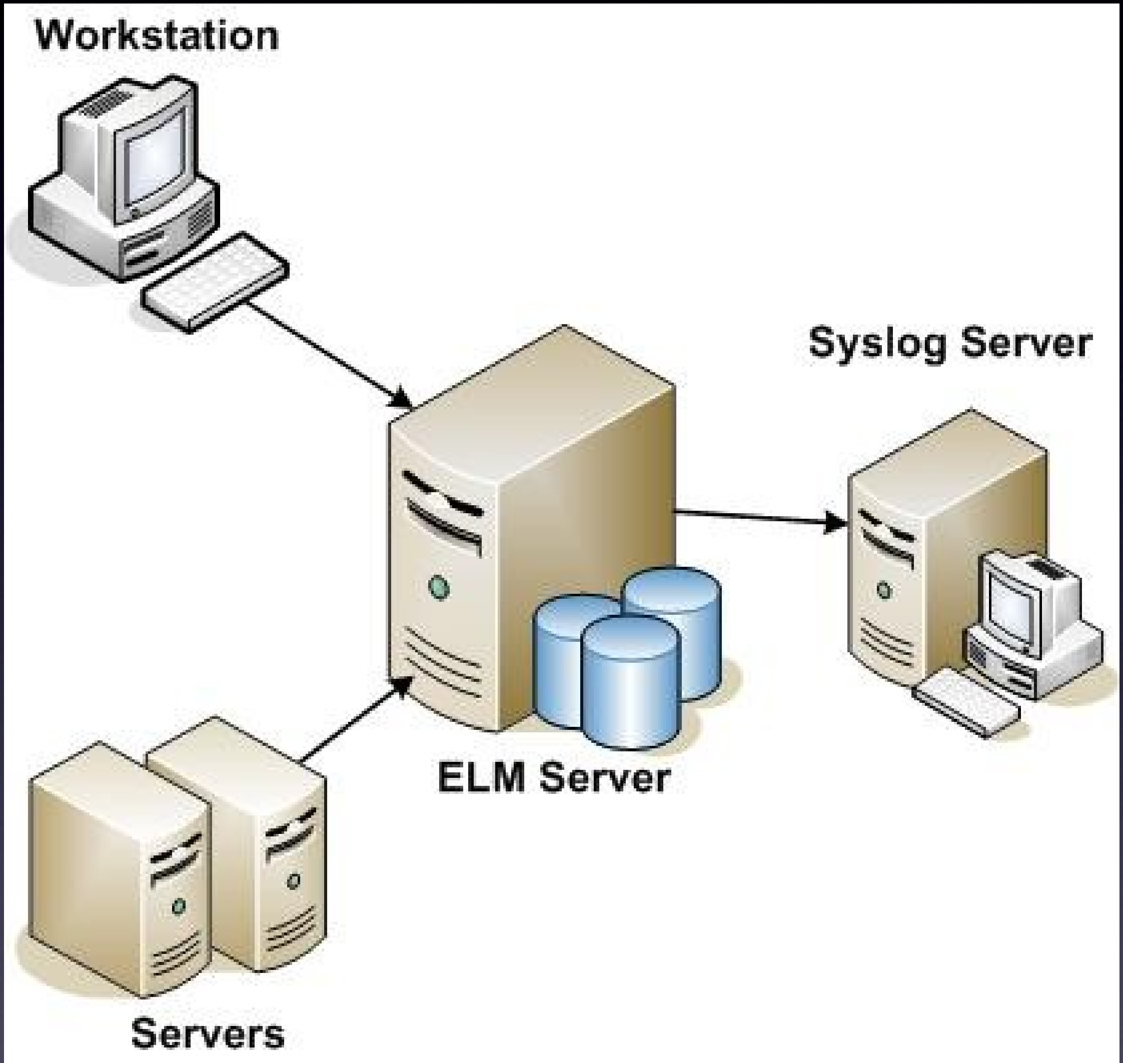


Description	Keyword	Value
Kernel	kern	0
User Processes	user	1
Electronic Mail	mail	2
Background System Processes	daemon	3
Authorization	auth	4
System Logging	sysl	5
Printing	lpr	6
Usenet News	news	7
Unix-to-Unix Copy Program	uucp	8
Clock Daemon	clkd	9
Security	sec2	10
FTP Daemon	ftpd	11
NTP Subsystem	ntp	12
Log Audit	audi	13
Log Alert	alert	14
Clock Daemon	clkd2	15
For Local Use	local0-local7	16-23



Description	Keyword	Value
System unusable	emerg	0
Take immediate action	alert	1
Critical condition	crit	2
Error message	err	3
Warning message	warn	4
Normal but significant condition	notice	5
Informational (includes Packeteer user events)	info	6
Debug message	debug	7

Esempio di utilizzo



Altri protocolli

- Netflow
  - Sviluppato da Cisco
  - Molto usato per il traffico di rete
- Snmp
  - Controllo dello stato degli apparati
- ...

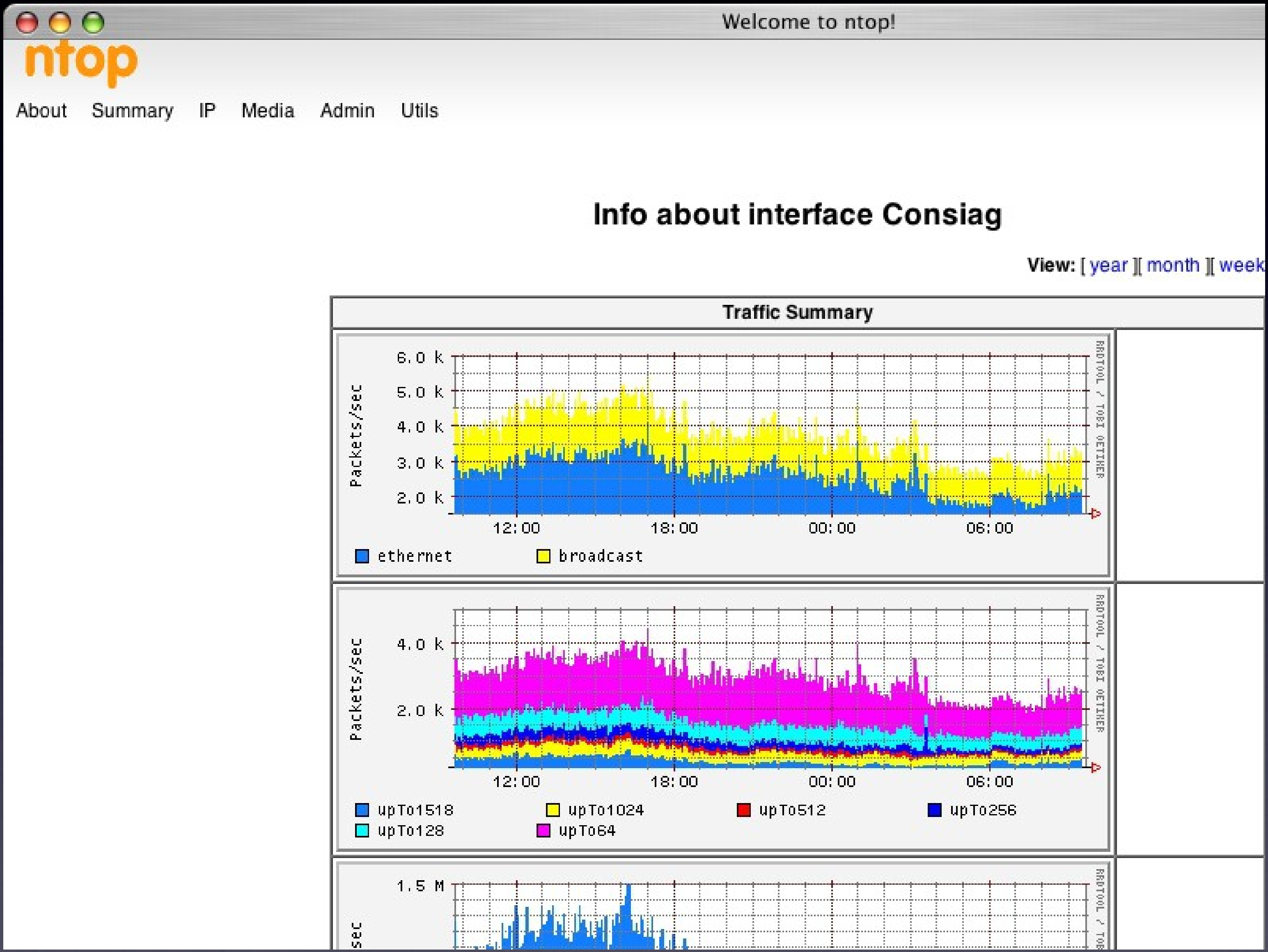
Logging in *unix

- /var/log/* ← folder
- /var/log/lastlog
- dmesg <> /var/log/kern.log (debian)
- /var/log/messages (sistema + kernel)
- /var/log/syslog (syslog daemon)
- /var/log/Xorg.0.log
- /var/log/apache/*
- ...

Tool per il controllo degli accessi

- last
- W
- who
- fail2ban (user brute-force)
- ...

Controllo del traffico: NTOP

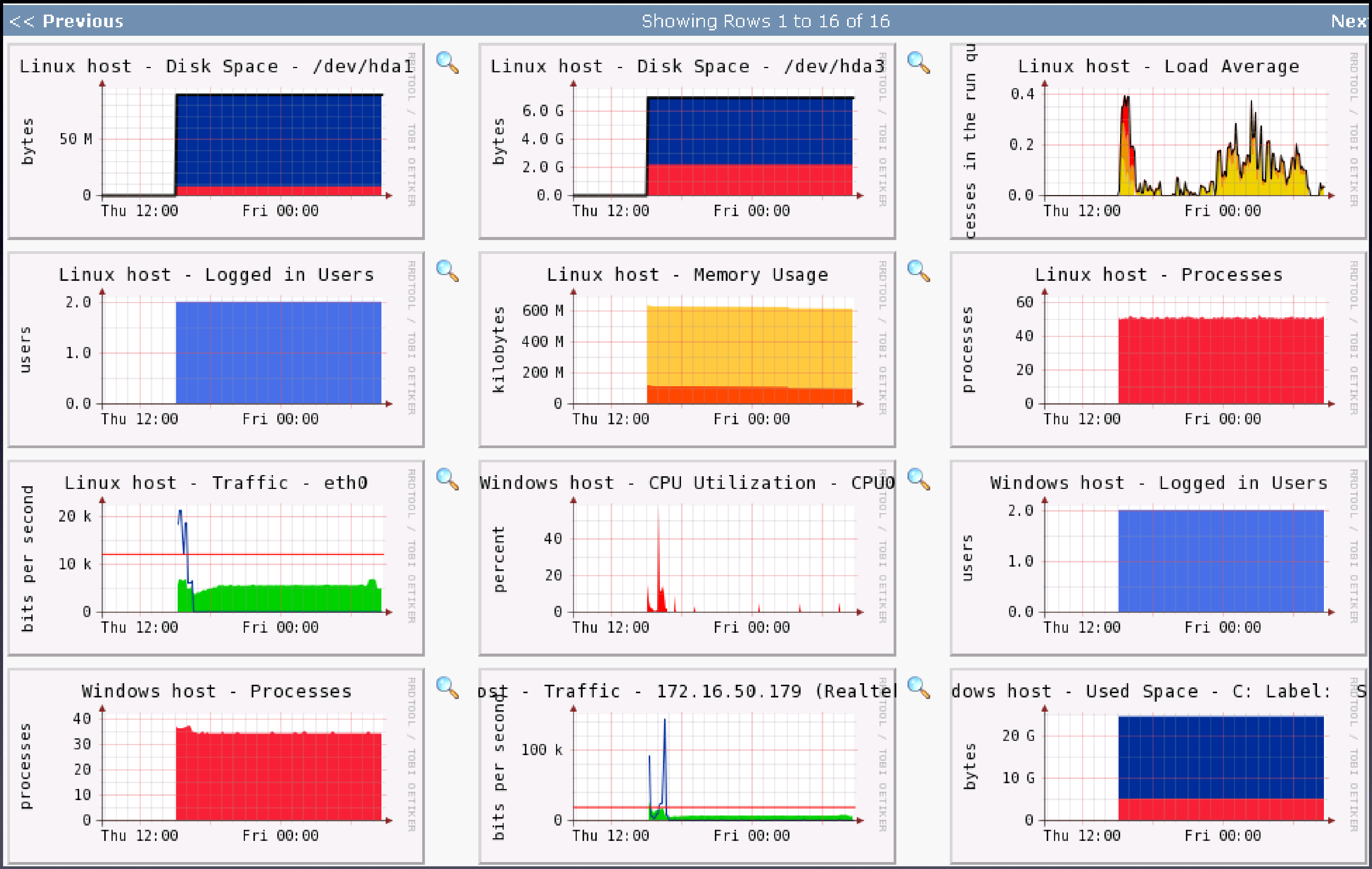


Welcome to ntop!

Info about interface Consiag

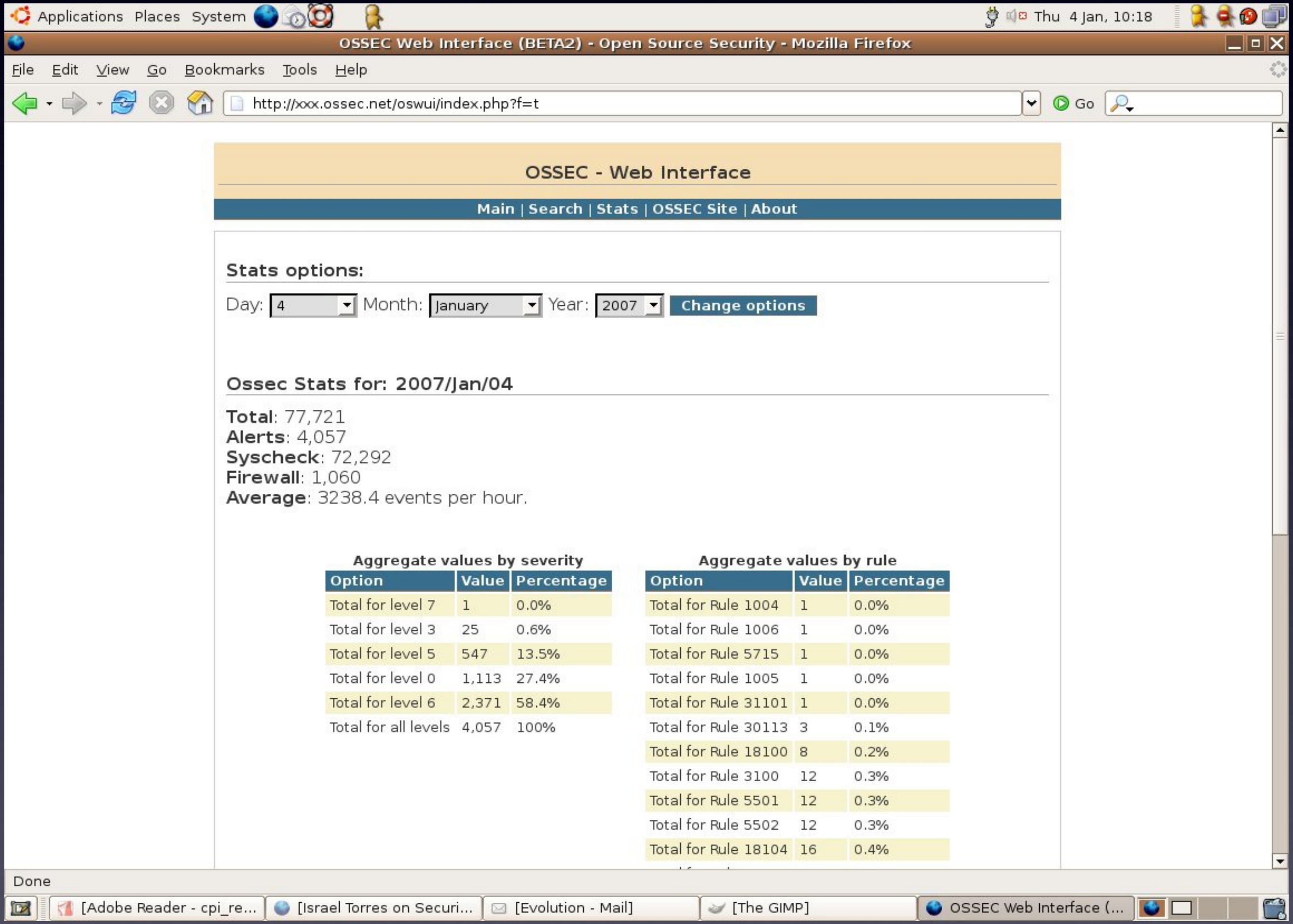
Traffic Summary

SNMP : Cacti


<< Previous
Showing Rows 1 to 16 of 16
Nex
Linux host - Disk Space - /dev/hda1
bytes
50 M
0
Thu 12:00
Fri 00:00
Linux host - Disk Space - /dev/hda3
bytes
6.0 G
4.0 G
2.0 G
0.0
Linux host - Load Average
cesses in the run qu
0.4
0.2
0.0
Linux host - Logged in Users
users
2.0
1.0
0.0
Linux host - Memory Usage
kilobytes
600 M
400 M
200 M
0
Linux host - Processes
processes
60
40
20
0
Linux host - Traffic - eth0
bits per second
20 k
10 k
0
Windows host - CPU Utilization - CPU0
percent
40
20
0
Windows host - Logged in Users
users
2.0
1.0
0.0
Windows host - Processes
processes
40
30
20
10
0
ost - Traffic - 172.16.50.179 (Realtel
bits per second
100 k
0
dows host - Used Space - C: Label: S
bytes
20 G
10 G
0
RRDTOOL / TOBI OETIKER

Ossec

- Monitoring e alerting sullo stato del sistema


Applications Places System
Thu 4 Jan, 10:18
OSSEC Web Interface (BETA2) - Open Source Security - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://xxx.ossec.net/oswui/index.php?f=t
Go
Done
[Adobe Reader - cpi_re...
[Israel Torres on Securi...
[Evolution - Mail]
[The GIMP]
OSSEC Web Interface (...

OSSEC - Web Interface

Main | Search | Stats | OSSEC Site | About

Stats options:

Day: 4 Month: January Year: 2007 Change options

Ossec Stats for: 2007/Jan/04

Total: 77,721
Alerts: 4,057
Syscheck: 72,292
Firewall: 1,060
Average: 3238.4 events per hour.

Aggregate values by severity

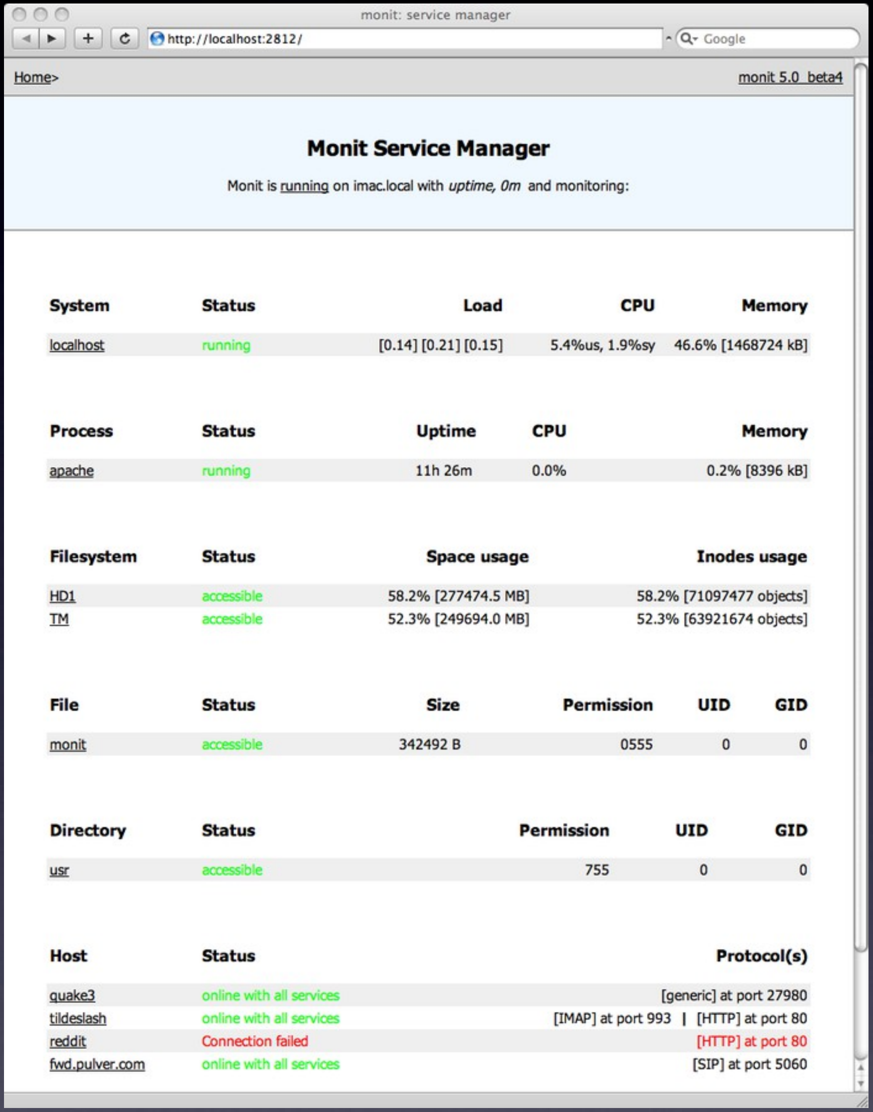
Option	Value	Percentage
Total for level 7	1	0.0%
Total for level 3	25	0.6%
Total for level 5	547	13.5%
Total for level 0	1,113	27.4%
Total for level 6	2,371	58.4%
Total for all levels	4,057	100%

Aggregate values by rule

Option	Value	Percentage
Total for Rule 1004	1	0.0%
Total for Rule 1006	1	0.0%
Total for Rule 5715	1	0.0%
Total for Rule 1005	1	0.0%
Total for Rule 31101	1	0.0%
Total for Rule 30113	3	0.1%
Total for Rule 18100	8	0.2%
Total for Rule 3100	12	0.3%
Total for Rule 5501	12	0.3%
Total for Rule 5502	12	0.3%
Total for Rule 18104	16	0.4%

Monit

- managing and monitoring:
  - Processes
  - Files
  - Directories
  - filesystems



Home>

monit 5.0 beta4

Monit Service Manager

Monit is running on imac.local with *uptime, 0m* and monitoring:

System	Status	Load	CPU	Memory
localhost	running	[0.14] [0.21] [0.15]	5.4%us, 1.9%sy	46.6% [1468724 kB]

Process	Status	Uptime	CPU	Memory
apache	running	11h 26m	0.0%	0.2% [8396 kB]

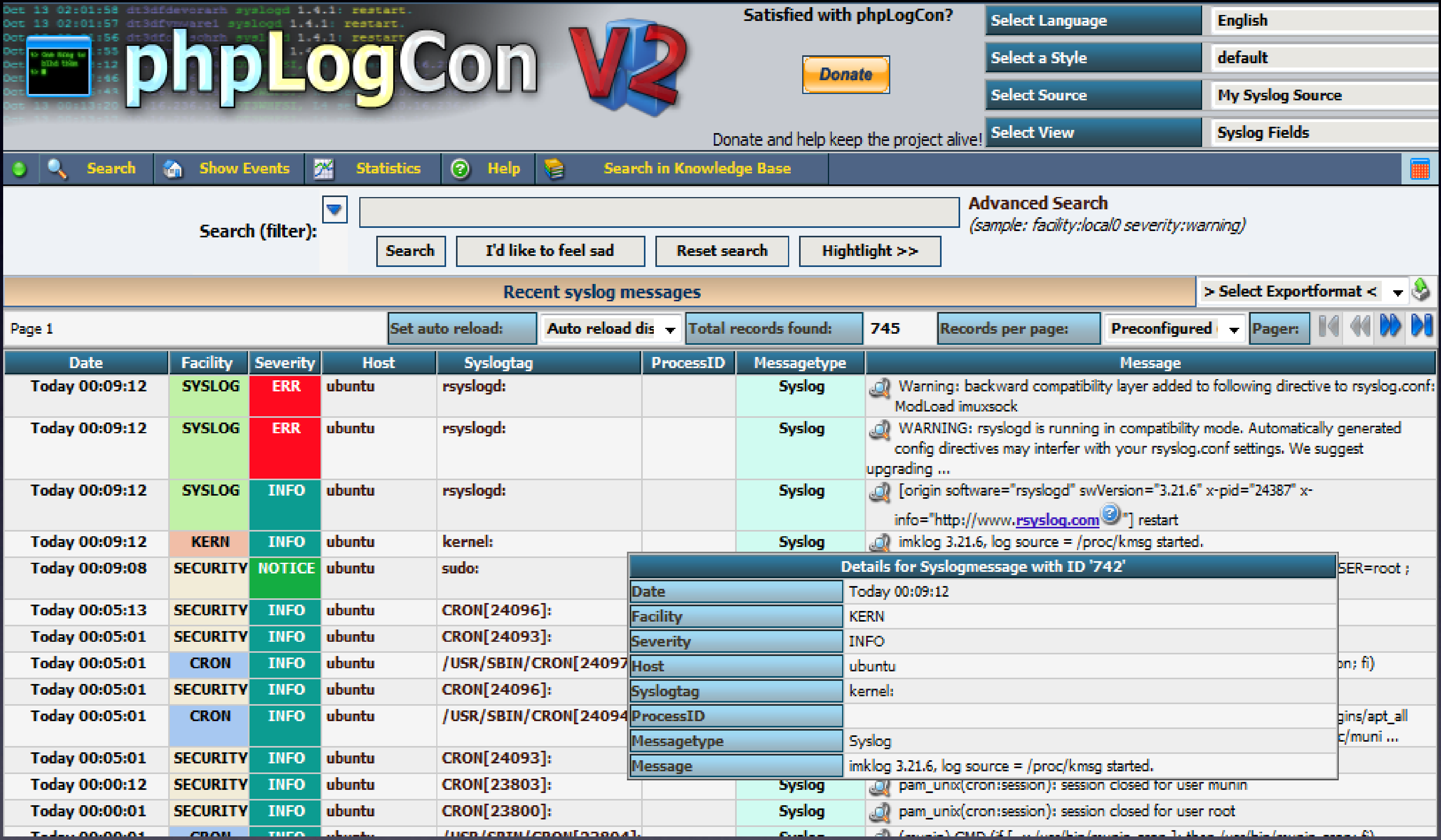
Filesystem	Status	Space usage	Inodes usage
HD1	accessible	58.2% [277474.5 MB]	58.2% [71097477 objects]
TM	accessible	52.3% [249694.0 MB]	52.3% [63921674 objects]

File	Status	Size	Permission	UID	GID
monit	accessible	342492 B	0555	0	0

Directory	Status	Permission	UID	GID
usr	accessible	755	0	0

Host	Status	Protocol(s)
quake3	online with all services	[generic] at port 27980
tildeslash	online with all services	[IMAP] at port 993 | [HTTP] at port 80
reddit	Connection failed	[HTTP] at port 80
fwd.pulver.com	online with all services	[SIP] at port 5060

phpLogCon



Satisfied with phpLogCon?

Donate and help keep the project alive!

Select Language	English
Select a Style	default
Select Source	My Syslog Source
Select View	Syslog Fields

Search (filter):

Advanced Search
(sample: facility:local0 severity:warning)

Recent syslog messages

> Select Exportformat <

Page 1 | Set auto reload: Auto reload dis | Total records found: 745 | Records per page: Preconfigured | Pager:

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 00:09:12	SYSLOG	ERR	ubuntu	rsyslogd:		Syslog	Warning: backward compatibility layer added to following directive to rsyslog.conf: ModLoad imuxsock
Today 00:09:12	SYSLOG	ERR	ubuntu	rsyslogd:		Syslog	WARNING: rsyslogd is running in compatibility mode. Automatically generated config directives may interfer with your rsyslog.conf settings. We suggest upgrading ...
Today 00:09:12	SYSLOG	INFO	ubuntu	rsyslogd:		Syslog	[origin software="rsyslogd" swVersion="3.21.6" x-pid="24387" x-info="http://www.rsyslog.com"] restart
Today 00:09:12	KERN	INFO	ubuntu	kernel:		Syslog	imklog 3.21.6, log source = /proc/kmsg started.
Today 00:09:08	SECURITY	NOTICE	ubuntu	sudo:			SER=root ;
Today 00:05:13	SECURITY	INFO	ubuntu	CRON[24096]:			
Today 00:05:01	SECURITY	INFO	ubuntu	CRON[24093]:			
Today 00:05:01	CRON	INFO	ubuntu	/USR/SBIN/CRON[24097			on; fi)
Today 00:05:01	SECURITY	INFO	ubuntu	CRON[24096]:			
Today 00:05:01	CRON	INFO	ubuntu	/USR/SBIN/CRON[24094			gins/apt_all c/muni ...
Today 00:05:01	SECURITY	INFO	ubuntu	CRON[24093]:			
Today 00:00:12	SECURITY	INFO	ubuntu	CRON[23803]:		Syslog	pam_unix(cron:session): session closed for user munin
Today 00:00:01	SECURITY	INFO	ubuntu	CRON[23800]:		Syslog	pam_unix(cron:session): session closed for user root
Today 00:00:01	CRON	INFO	ubuntu	/USR/SBIN/CRON[23804]:		Syslog	(munin) CMD (if [-x /usr/bin/munin-cron]; then /usr/bin/munin-cron; fi)

Details for Syslogmessage with ID '742'

Date	Today 00:09:12
Facility	KERN
Severity	INFO
Host	ubuntu
Syslogtag	kernel:
ProcessID	
Messagetype	Syslog
Message	imklog 3.21.6, log source = /proc/kmsg started.

Cron

- possiamo automatizzare i controlli
- Avviare qualsiasi script personalizzato
  - Tipo rkhunter o chkrootkit e farsi mandare una mail nel caso di problemi
- ...

Logging centralizzato

- Storage unico dei log
- Sicurezza
- Log non esposti all'alterzione (sul client)
- client/server architecture required
- Maggior controllo
- Minor carico sui server
- Collector e

rsyslog

- La soluzione sicura alla centralizzazione
- Supporta ssl/tls (syslog-ng e' a pagamento)
- ....

Problemi della correlazione

- flusso logico delle azioni …
- cosa e come correlare
- fonti da cui recuperare i log (sonde)
- problema dei pattern predefiniti
- protocolli di comunicazioni (IDMEF example)

Sistemi SIM

- Security Information Management
- Monitor events in real time.
- Display a real-time view of activity.
- Translate event data into XML format
- Aggregate data.
- Correlate data from multiple sources.
- Cross-correlate to help administrators discern between real threats and false positives.
- Provide automated incidence response.
- Send alerts and generate reports.

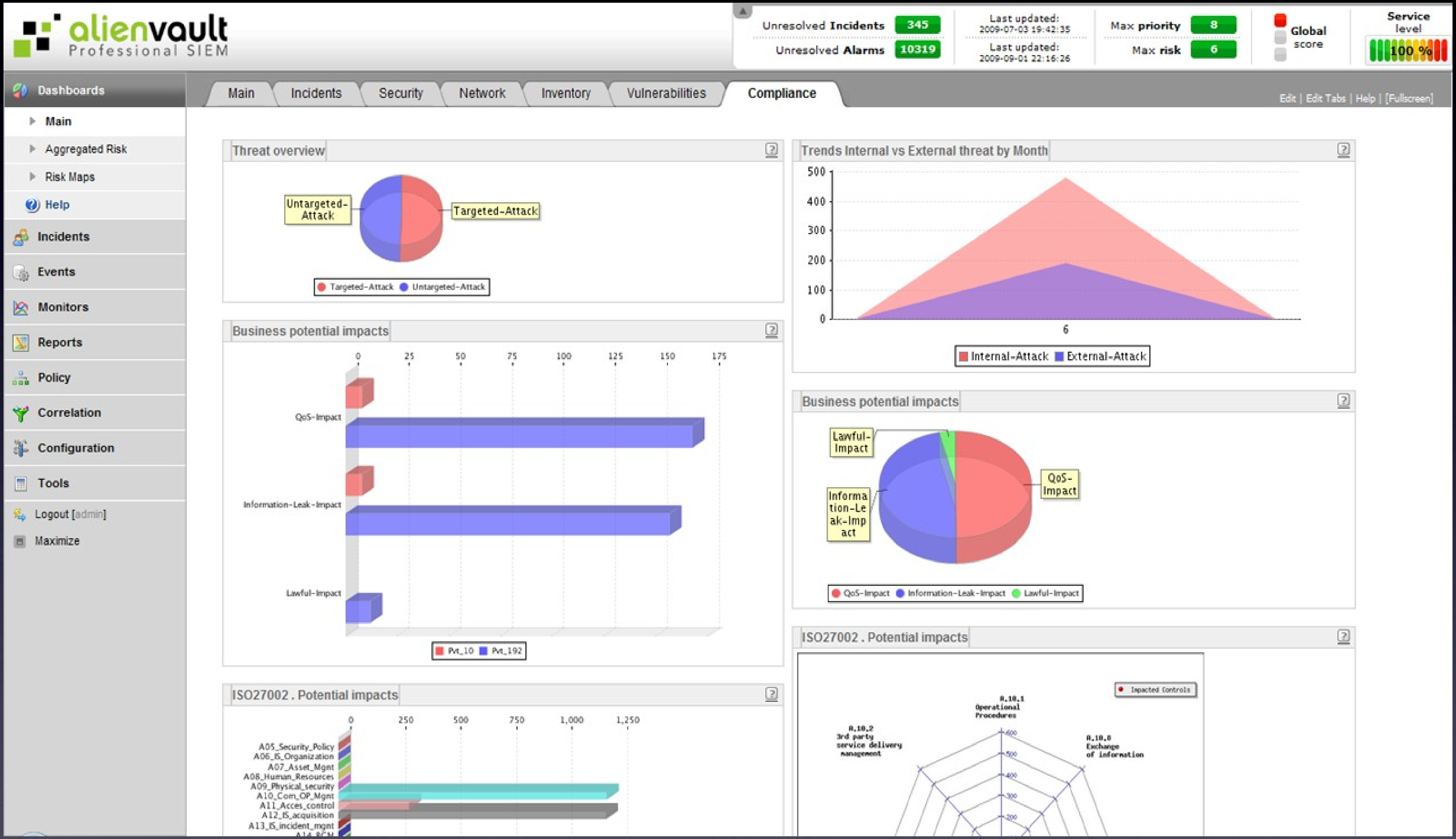
OSSIM - 1

- *Arpwatch* – used for MAC anomaly detection.
- *P0f* – used for passive OS detection and OS change analysis.
- *Pads* – used for service anomaly detection.
- *Nessus* – used for vulnerability assessment and for cross correlation (IDS vs Security Scanner).
- *Snort* – the IDS, also used for cross correlation with nessus.
- *Spade* – the statistical packet anomaly detection engine. Used to gain knowledge about attacks without signatures.

OSSIM - 2

- *Arpwatch* – used for MAC anomaly detection.
- *Tcptrack* – used for session data information which can prove useful for attack correlation.
- *Ntop*
- *Nagios* – fed from the host asset database, it monitors host and service availability information.
- *Osiris* – a great HIDS.
- *OCS-NG* – cross-platform inventory solution.
- *OSSEC* – integrity, rootkit, registry detection, and more.

Ossim



Unresolved Incidents 345

Unresolved Alarms 10319

Last updated: 2009-07-03 19:42:35

Last updated: 2009-09-01 22:16:26

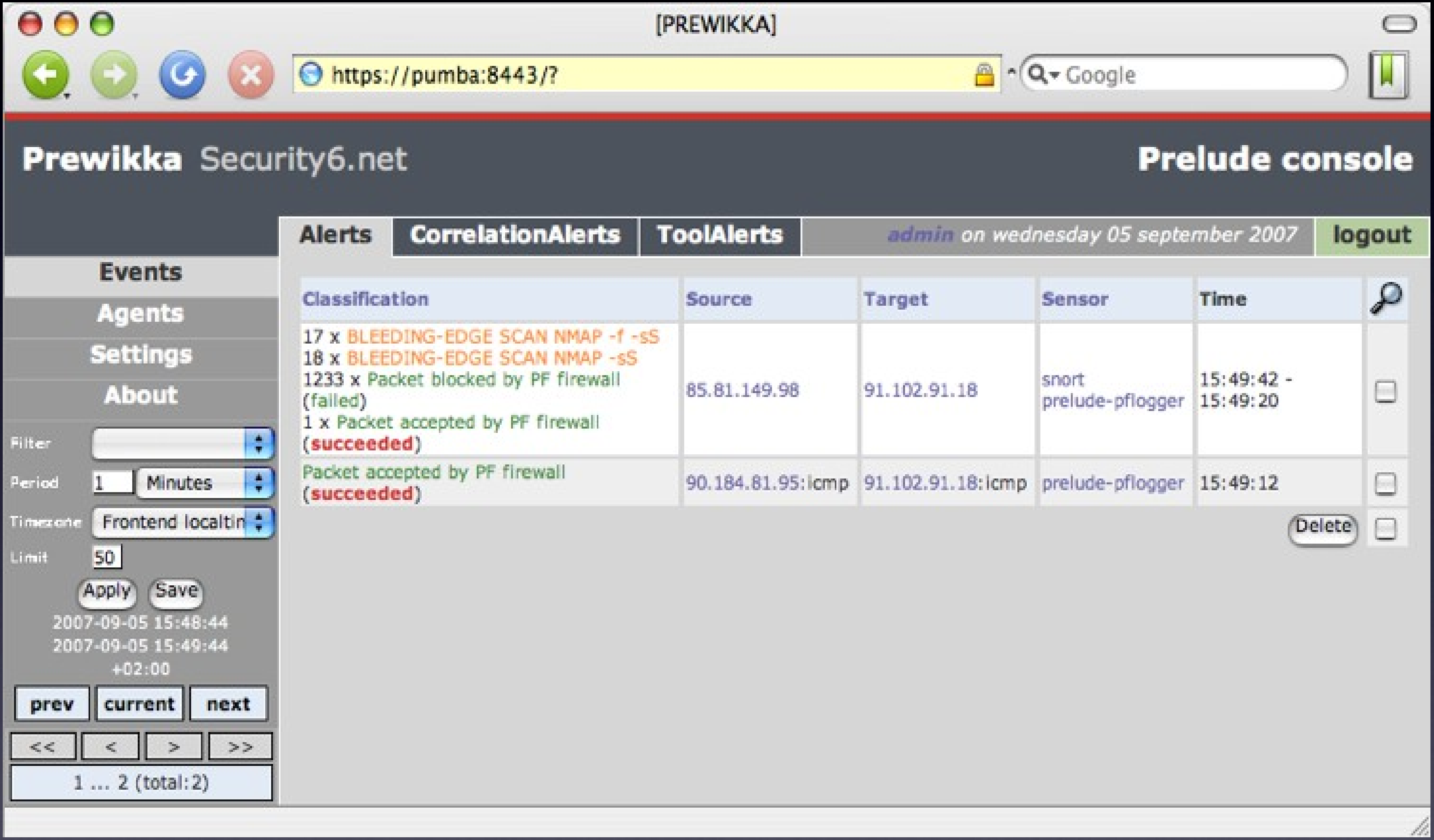
Max priority 8

Max risk 6

Global score

Service level 100 %

PreludeIDS



admin on wednesday 05 september 2007

Filter:
Period: 1 Minutes
Timezone: Frontend localtim
Limit: 50

2007-09-05 15:48:44
2007-09-05 15:49:44
+02:00

1 ... 2 (total:2)

Classification	Source	Target	Sensor	Time	
17 x BLEEDING-EDGE SCAN NMAP -f -sS 18 x BLEEDING-EDGE SCAN NMAP -sS 1233 x Packet blocked by PF firewall (failed) 1 x Packet accepted by PF firewall (**succeeded**)	85.81.149.98	91.102.91.18	snort prelude-pflogger	15:49:42 - 15:49:20	□
Packet accepted by PF firewall (**succeeded**)	90.184.81.95:icmp	91.102.91.18:icmp	prelude-pflogger	15:49:12	□
					□

References

- www.alienvault.com
- www.prelude-ids.com
- Network Security Hacks (O'Reilly)
- IETF rfc*
- man - info - papers

Contact

- vieni a trovarci su irc.freenode.net - canale #pnlug
- mail: rainbow@irh.it
- site: www.irh.it
-
- *A6U*
- mail: mail@teocolella.net
- Site: www.teocolella.net

License

END