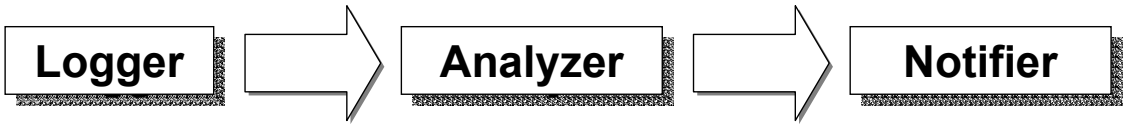
Network Security
Elements of Network Security Protocols

Elementi di logging ed auditing
I sistemi di rilevamento delle intrusioni (IDS)

- logging ed auditing
- syslog
- la catena di custodia
- log sanitization

Architettura di Auditing

- Con **logging** si intende la registrazione di eventi e statistiche che forniscono informazioni sull'uso e sulle prestazioni di un sistema
- Con **auditing** si intende l'attività di analisi dei log record per presentare informazioni sul sistema in modo chiaro e comprensibile



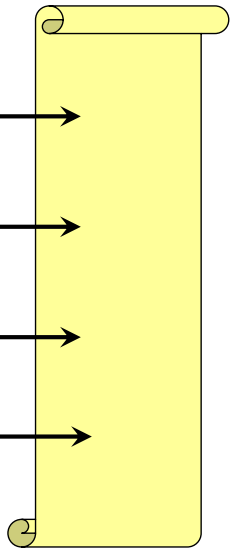
Le attività di logging & auditing servono a

- determinare se un'azione richiesta porterà il sistema in uno stato insicuro (a priori)
- determinare la sequenza di eventi che ha portato il sistema in uno stato insicuro (a posteriori)
- determinare i pattern tipici di utilizzo del sistema

Sorgenti di log

Tutto può essere sorgente di log:

- l'hw, tramite il kernel
- i demoni (sshd, httpd, inetd...)
- gli applicativi (mysql, cron, ...)
- gli utenti



Esempi di log

Esempi di log generati dall'hardware:

Jun 4 18:09:43 dhcpclient1 kernel: ide0: BM-DMA at 0xf000-0xf007, BIOS settings: hda:pio hdb:pio

Jun 6 14:45:53 dhcpclient1 kernel: eth0 : Setting promiscuous mode

Esempi di log generati dagli utenti:

yagostini pts/0 xxx-223.xxx.xxx Thu Jun 6 15:56 still logged in

trastai pts/0 xxx-21.xx.xxx Thu Jun 6 15:30 - 15:42 (00:12)

Esempi di log

Esempi di log generati da demoni:

sendmail

Jun 2 04:02:03 xxxx sendmail[24976]: g52221tb024971: to=yagostini@xxx.it, ctladdr=<root@xxx.xxx.it> (0/0), delay=00:00:02, xdelay=00:00:01, mailer=esmtp, pri=270564, relay=mail.xxx.it. [xxx.xx.xxx.xx], dsn=2.0.0, stat=Sent (<200206020202.g52221OJ024969@mail.xxx.it> Queued mail for delivery)

Apache

xx.xxx.xx.xx - - [19/Dec/2001:16:22:33 +0100] "GET /apache_pb.gif HTTP/1.1" 200 2326

Cron

Jun 2 04:32:00 hostname CROND[29556]: (root) CMD (/usr/local/bin/CheckDefang.sh > /dev/null 2>&1)

Esempi di log

Esempi di log generati da applicativi:

Un generico script di backup

Finished backup at Fri Apr 19 00:00:00 CEST 2002

Starting backup at Sat Apr 20 00:00:00 CEST 2002

Squirrelmail (webmail)

xxx.xx.xx.xxx - - [18/Feb/2002:15:07:30 +0100] "GET /squirrelmail/ HTTP/1.0" 302

0 "-" "Lynx/2.8.4rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6b"

Esempi di log

Tracce (fingerprint) di attacchi e probe:

Apache

[Tue Jun 11 04:09:11 2002] [error] [client xxx.xx.xxx.x] File does not exist: /www/virtualhosts/www.nomesito.com/MSADC/root.exe

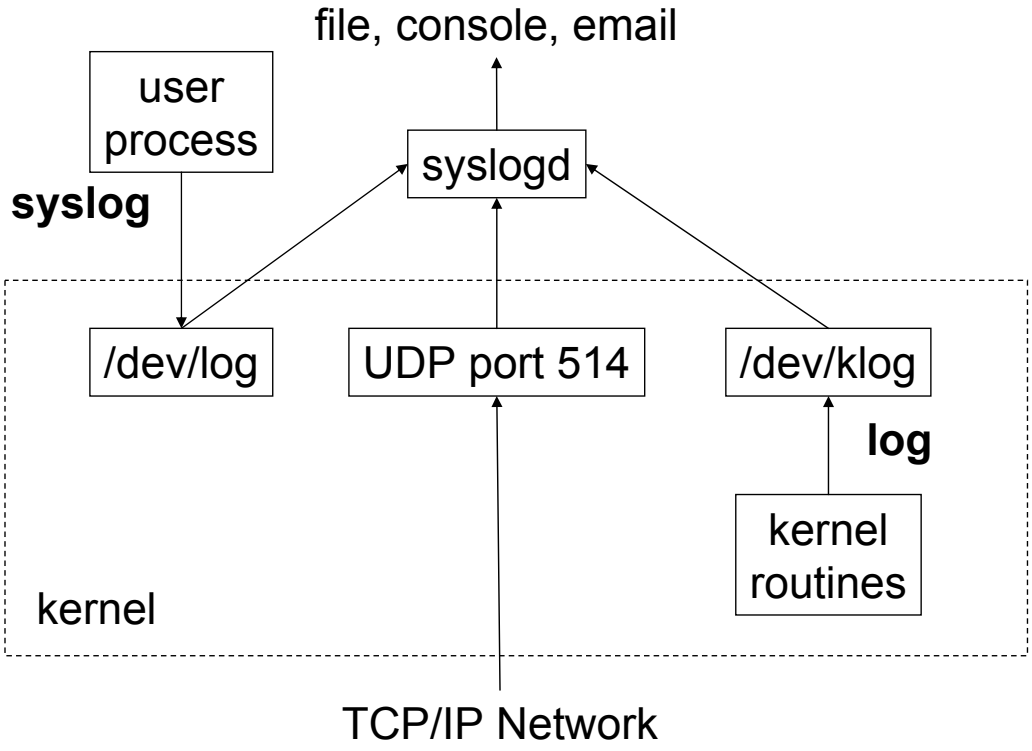
(error_log di apache che segnala un attacco NIMDA)

Ssh

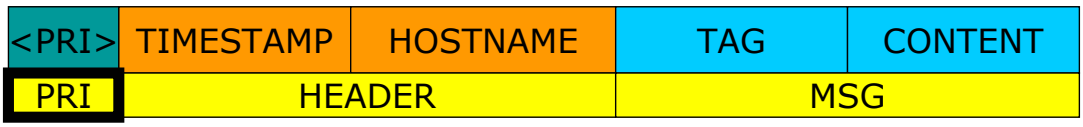
Jun 9 09:39:25 sshd[17060]: scanned from xxx.xx.xxx.xx with SSH-1.0-SSH_Version_Mapper. Don't panic.

(messages log file, evidenzia la signature di un version scanner per sshd)

syslog (RFC 3164)



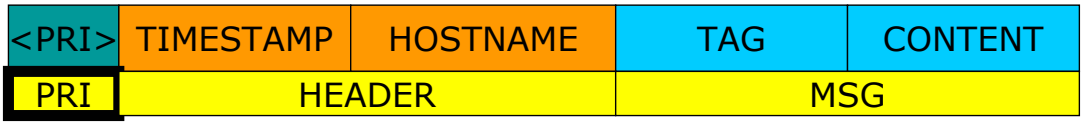
Formato del messaggio syslog



PRIORITY = FACILITY * 8 + SEVERITY

Ci sono 24 facilities e 8 severities, quindi il valore di PRI può andare da 0 a 191

Formato del messaggio syslog



PRI - LE FACILITIES (0-23)

0 kern, 1 user, 2 mail, 3 daemon, 4 auth, 5 syslog,

6 lpr, 7 news, 8 uucp, 9 cron, 10 authpriv, 11 ftp,

16-23 local 0-7

PRI - LE SEVERITIES (0-7)

0 emerg/panic, 1 alert, 2 crit, 3 error/err,

4 warning/warn, 5 notice, 6 info, 7 debug

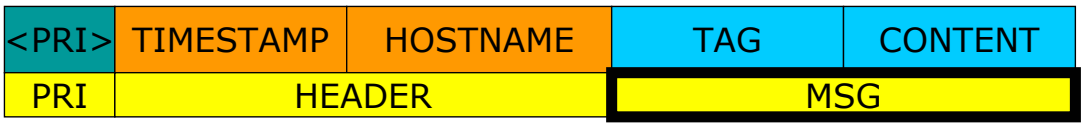
Formato del messaggio syslog

HEADER

Il **TIMESTAMP** contiene la data locale nel formato Mmm dd hh:mm:ss

L'**HOSTNAME** contiene il nome dell'host che ha generato il messaggio (senza il dominio)

Formato del messaggio syslog



MSG

Il **TAG** contiene il nome del programma o processo che ha generato il messaggio

Il campo **CONTENT** contiene l'effettivo messaggio

Il file di configurazione di syslogd

/etc/syslog.conf

Ogni riga è formata da due campi :

un campo selettore

un campo di azione

separati da uno o più spazi (o tab) che definiscono rispettivamente **COSA** loggare e **DOVE** loggare

FACILITY.SEVERITY<spazio/tab>AZIONE

Il campo selettore

facility.severity

*	tutte le facilities o tutte le severities
none	nessuna severity
,	multiple facilities e severities
;	multiple statement con stessa azione
=	esattamente una severity
!	negazione severity
\	separazione multiline

Il campo azione

E' possibile specificare diverse azioni

File normali : /

Named Pipe - FIFO : |

Terminali virtuali e console

Macchine remote : @

Lista di utenti : ,

Tutti gli utenti : *

Il file di configurazione di syslogd

Esempio

```
*.=info;*.=notice;*.=warning;\
auth,authpriv.none;\
cron,daemon.none;\
mail,news.none                    /var/log/messages
```

Tutti i messaggi con severity info, notice e warning, eccetto quelli provenienti dalle facilities auth, authpriv, cron, daemon, mail e news devono essere registrati sul file /var/log/messages

Il file di configurazione di syslogd

Esempio

```
*.alert    *
```

Tutti i messaggi con severity alert o maggiore devono essere inviati a tutti gli utenti collegati

```
kern.!alert; \
*.=debug;*.=info;\
*.=notice;*.=warn          /dev/tty8
```

Tutti i messaggi con severity debug, info, notice e warn vengono visualizzati su /dev/tty8 tranne quelli provenienti da kern con severity uguale o maggiore ad alert

Come inviare messaggi a syslogd

Rendere i propri script e programmi più 'loquaci'

SHELL SCRIPT

E' possibile utilizzare il programma **logger**, con il quale si può inviare a syslogd un messaggio con una priorità e un tag definibile.

logger -p facility.severity -t tag message

Es: logger –p local0.notice –t HOSTIDM

La priorità può essere specificata numericamente o con una coppia facility.severity

Di default logga con priorità user.notice

Come inviare messaggi a syslogd

Rendere i propri script e programmi più 'loquaci'

Linguaggio C

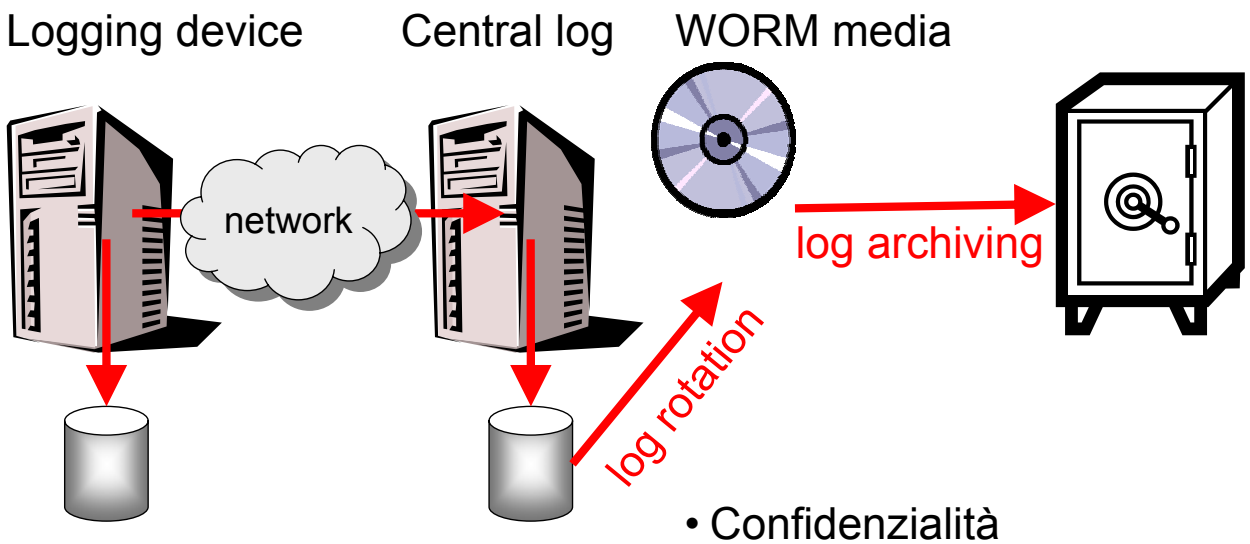
Includere **syslog.h** e utilizzare le funzioni di Standard C library:

void openlog(char *ident, int option, int facility)
void syslog(int priority, char *format)
void closelog(void)

Linguaggio PERL

E' possibile usare il modulo **Sys::Syslog**

La catena di custodia



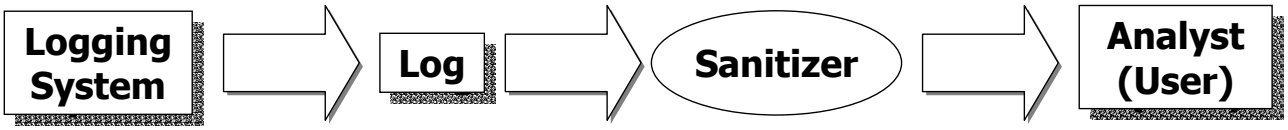
- Confidenzialità
- Integrità
- Disponibilità

Sicurezza di syslog

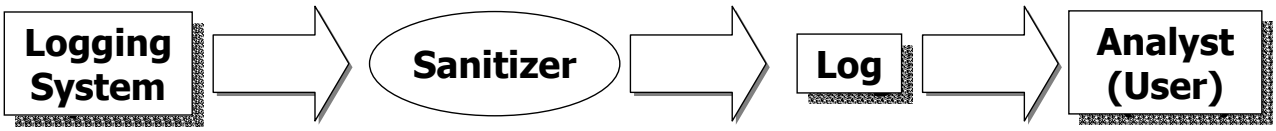
- Confidenzialità
  - Tunnel SSL o SSH
  - IPSec
- Integrità ed autenticità
  - "Reliable delivery for syslog" (RFC 3195)
  - Syslog-Sign Protocol (draft RFC)
  - Tunnel SSL o SSH
- Disponibilità
  - clustering
  - indirizzi privati

Confidenzialità dei log: log sanitization

Log sanitization for external use



Log sanitization for user privacy



Confidenzialità dei log

Modalità di bonifica (sanitization)

- Senza ricostruzione (log anonimo)

  Le informazioni sensibili sono bonificate in modo che neanche l'originatore del log può ricostruirle

- Con ricostruzione

  L'originatore del log può ricostruire le informazioni sensibili

Bonifica con ricostruzione

Bonifica basata su pseudonimi

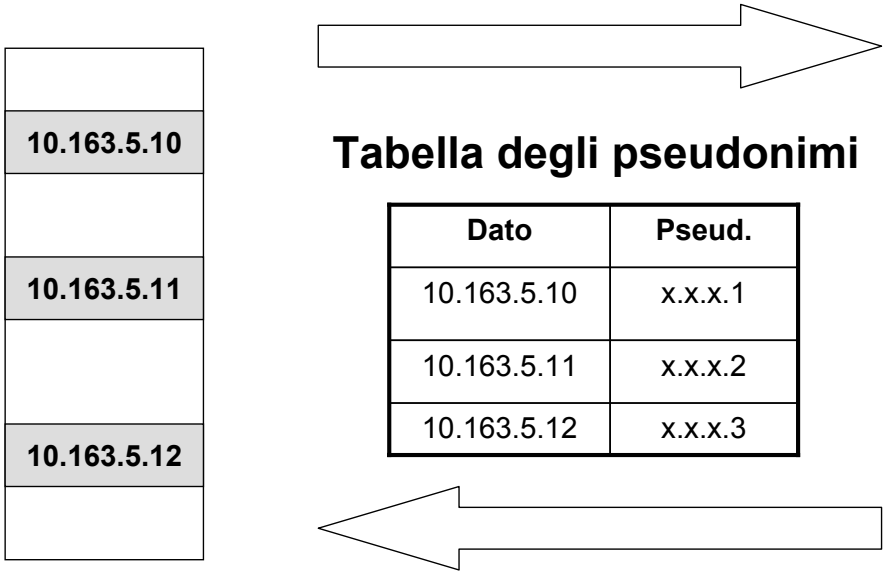


Tabella degli pseudonimi

Dato	Pseud.
10.163.5.10	x.x.x.1
10.163.5.11	x.x.x.2
10.163.5.12	x.x.x.3

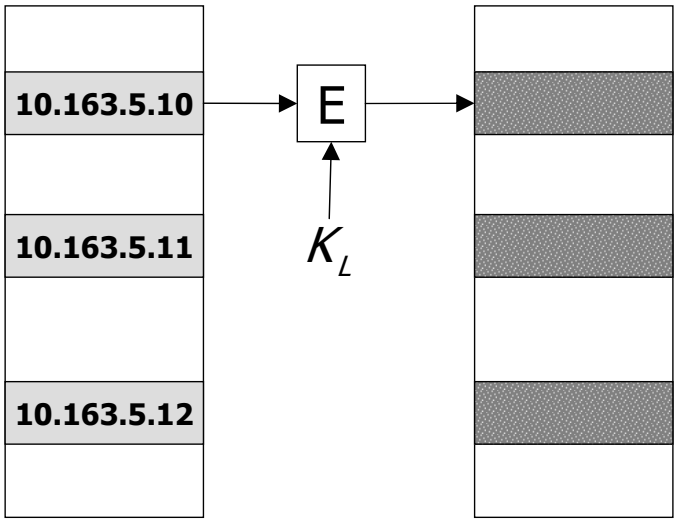
Log originale

La Tabella è accessibile al system administrator

Log bonificato

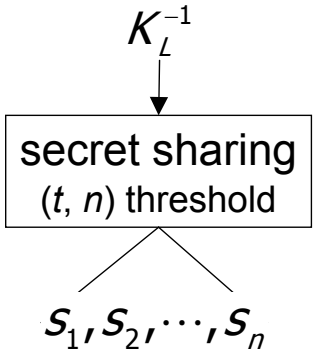
Bonifica con ricostruzione

Bonifica basata sulla crittografia



Log originale

Log bonificato



- *t* share su *n* permettono di ricostruire la chiave privata
- ciascuna share è distribuita ad un diverso utente
- la chiave privata viene distrutta

I sistemi di rilevamento delle intrusioni (IDS)

- Modelli basati sulle anomalie e sulle firme
- Falsi positivi e falsi negativi
- HIDS & NIDS
- Dove collocare l'IDS

Modelli principali

- Nel modello **Anomaly Detection** (**basato sulle anomalie**) si rileva la presenza di un attacco come deviazione dal comportamento normale di un elaboratore o di una rete
- Nel modello **Signature Detection** (**basato sulle firme**) si rileva un attacco sulla base delle caratteristiche note, o *signature*, di un attacco

Falsi positivi e falsi negativi

- **Falsi positivi** (**falsi allarmi**): quando l'IDS rileva erroneamente un'intrusione
- **Falsi negativi**: quando l'IDS, erroneamente, non rileva un intrusione
- I falsi positivi/negativi
  - sono inevitabili,
  - minano la credibilità dell'IDS,
  - richiedono un intervento umano

Modelli & falsi

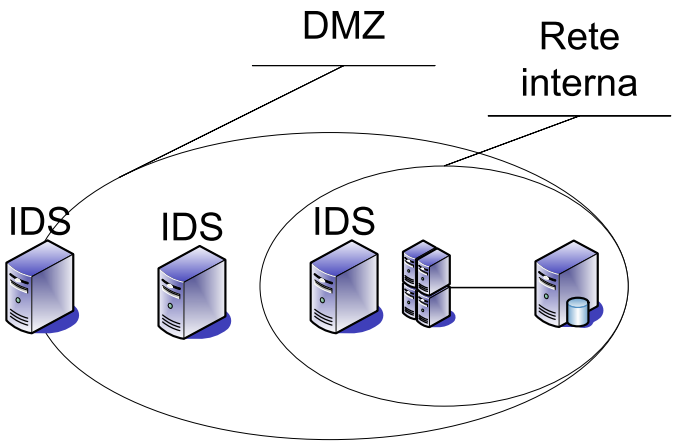
modello	falsi positivi	falsi negativi
basato sulle anomalie	si	si
basato sulle firme	no	si

- IDS basati sulle anomalie: funzionano bene laddove la definizione di "normale" è molto precisa
- IDS basati sulle firme: è difficile trovare un compromesso tra firme estese (traffico normale) e firme ridotte (facili da ingannare)

HIDS & NIDS

- **Host Intrusion Detection System**–IDS basati sugli host rilevano intrusioni su di un host
- **Network Intrusion Detection System**–IDS basati su reti rilevano intrusioni in rete
- HIDS e NIDS sono approcci complementari
  - HIDS tendono a conoscere lo stato della macchina su cui operano ma possono essere sovvertiti se l'host viene compromesso
  - NIDS sono più resistenti ad attacchi e rilevamenti ma hanno più difficoltà a conoscere lo stato della rete

Dove collocare un IDS



- Qual è lo scopo dell'IDS?
- Metafora: in una banca dove posizionereste una telecamera di videosorveglianza?
- monitorare il traffico esterno può essere inutile, è meglio registrarlo ed analizzarlo successivamente

- Un buon punto dove inserire l'IDS è nella rete interna vicino ad attività specifiche, importanti, sensibili, ad accesso limitato
- Un altro buon punto dove inserire l'IDS (*honeypot*) è in DMZ: il traffico verso questa macchina è ostile oppure è il risultato di una mal configurazione