ULOG con Iptables

Introduzione

Ulogd sostituisce il tradizionale metodo di logging bastato su syslogd, che utilizza il tradizionale TARGET LOG di iptables, con il più evoluto target ULOG/ulogd, capace di loggare direttamente in userspace e gestire i log nei modi più svariati. Le informazioni risultano più schematiche e molto simili a quelle dei tradizionali log di sistema.
In pratica i log vengono gestiti da un apposito demon che è in grado di inviarli e gestirli nei modi più disparati, da file di testo a database MySQL, il tutto in modo nativo senza usare filtri o script in perl come capitava con il target LOG.

La home del progetto:

- http://gnumonks.org/projects/ulogd

Prerequisiti

Per poter utilizzare questo metodo di log con iptables occorre applicare la ulog-patch from patch-o-matic, o comunque includerne il supporto nel kernel.
Nella sezione Netfilter Configuration occorre comunque avere selezionata l'opzione **CONFIG_IP_NF_TARGET_ULOG.**

```
Networking options  --->
        IP: Netfilter Configuration  --->
                [*]   LOG target support
```

Installazione e Configurazione

wget ftp://ftp.netfilter.org/pub/ulogd/ulogd-1.02.tar.bz2

```
bunzip2 ulogd-1.02.tar.bz2
tar xvf ulogd-1.02.tar
/ulogd-1.02# ./configure --with-mysql=/var/lib/mysql
make && make install
```

Abbiamo installato il supporto per il MySQL in modo da dirottare le registrazioni effettuate in una tabella del mysql attraverso il demone ulogd:

Configurazione

Prima di eseguire ulog occorre configurare il file **ulogd.conf** che viene copiato /usr/local/etc. Vediamo le direttive principali:

```
logfile /var/log/ulogd.log
→ file di log per i messaggi di stato

loglevel 5
→ loglevel scelto: loglevel: debug(1), info(3), notice(5), error(7) or fatal(8)

syslogfile /var/log/ulogd.syslogemu
```

→ specifica il file di testo su cui venogno dirottate le registrazioni
plugin /usr/local/lib/ulogd/ulogd_LOGEMU.so
→ è il plugin che permette di effettuare questo tipo di registrazione

ulogd_MYSQL.so: optional logging into a MySQL database
database information
mysqltable ulog
mysqlpass ulogpwd
mysqluser ulog
mysqldb ulogd
mysqlhost localhost
load the plugin (remove the '#' if you want to enable it)
plugin /usr/local/lib/ulogd/ulogd_MYSQL.so
→ parametri per la connessione al DB MySQL (dn, user e password).

Ovviamente per usare il MySQL logging occorre creare la tabella:
cd /usr/src/ulogd-1.02/doc
mysqladmin create ulogd –p'pwd'
mysqladmin ulogd –p'pwd'<mysql.table
mysql mysql -p
grant ALL PRIVILEGES on ulogd.* to ulog@localhost identified by 'ulogpwd';

Startup

A questo punto si può Avviare il demone e testatolo:

ulogd -c /usr/local/etc/ulogd.conf
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `raw'
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `oob'
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `ip'
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `tcp'
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `icmp'
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `udp'
Fri Mar 25 15:09:37 2005 <3> ulogd.c:300 registering interpreter `ahesp'
Fri Mar 25 15:09:37 2005 <1> ulogd_MYSQL.c:218 allocating 4304 bytes for statement
Fri Mar 25 15:09:37 2005 <1> ulogd_MYSQL.c:242 stmt='insert into ulog (ahesp_spi,icmp_fragmtu,icmp_gateway,icmp_echoseq,icmp_echoid,icmp_code,icmp_type,udp_len,udp_dport,udp_sport,tcp_fin,tcp_syn,tcp_rst,tcp_psh,tcp_ack,tcp_urgp,tcp_urg,tcp_window,tcp_ackseq,tcp_seq,tcp_dport,tcp_sport,ip_fragoff,ip_id,ip_csum,ip_ihl,ip_totlen,ip_ttl,ip_tos,ip_protocol,ip_daddr,ip_saddr,oob_out,oob_in,oob_mark,oob_prefix,oob_time_usec,oob_time_sec,raw_mac) values ('
Fri Mar 25 15:09:37 2005 <5> ulogd.c:355 registering output `mysql'
Fri Mar 25 15:09:37 2005 <5> ulogd.c:355 registering output `syslogemu'

Esempi di utilizzo

Per poter verificare il reale funzionamento del sistema si può provare a specificare qualche regola con il target ULOG al posto del canonico target LOG:

iptables -A OUTPUT -j ULOG --ulog-nlgroup 1

Il valore di ulog-nlgroup deve essere lo stesso che è stato specificato nelle GLOBAL OPTIONS del file di configurazione:

netlink multicast group (the same as the iptables --ulog-nlgroup param)
nlgroup 1

```
# iptables -A INPUT -j ULOG -p tcp --dport 80 --ulog-nlgroup 1
```

Sintassi di ULOG

Il meccanismo di funzionamento di ULOG prevede di registrare un messaggio di log con programmi eseguiti in user-space.
Il messaggio stesso viene inviato in multicast tramite un netlink socket. Le applicazioni che intendono gestire il log devono essere agganciate ai netlink group relativi all'indirizzo multicast utilizzato, per poter ricevere il pacchetto.

Usando -j ULOG si possono utilizzare le seguenti opzioni:

--ulog-nlgroup nogroup → specifica il netlink group al quale il pacchetto viene inviato. Può avere un valore è compreso tra 1 e 32 (default è 1);
--ulog-prefix prefix → indica la stringa da anteporre al messaggio da inserire nel log (per un massimo 32 caratteri);
--ulog-cprange size → specifica il numero di byte da copiare nello userspace, in base a quanto indicato da size (con il valore 0 si indica di copiare l'intero pacchetto - valore di default);
--ulog-qthreshold size → specifica il numero di pacchetti da accodare in kernelspace prima di inviarli come messaggio multipart del netlink, in base a quanto specificato da size (per default è 1);

Esempi di utilizzo con Shorewall

Shorewall semplifica di molto l'uso di ULOG, basta specificarlo nelle policy o nel file delle rules, in questo modo:

```
#POLICY
#SOURCE        DEST          POLICY        LOG LEVEL      LIMIT:BURST
#-->LOC
loc            net           ACCEPT
loc            dmz           DROP          ULOG
loc            fw            DROP          ULOG
loc            all           DROP          ULOG
#--> DMZ
dmz            fw            DROP          ULOG
dmz            net           DROP          ULOG
dmz            loc           DROP          ULOG
dmz            all           DROP          ULOG
#--> NET
net            fw            DROP          ULOG
net            dmz           DROP          ULOG
net            loc           DROP          ULOG
net            all           DROP          ULOG
#sempre per ultima
all            all           REJECT        ULOG
#LAST LINE -- ADD YOUR ENTRIES ABOVE THIS LINE -- DO NOT REMOVE
```

Test del Sistema

Se avete scelto di usare ULOG per registrare tutti i pacchetti droppati, basta fare un Portscan per osservare il file di testo popolarsi di dati:

tail -f /var/log/ulogd.syslogemu

```
Mar 25 14:44:23 fire Shorewall:loc2fw:DROP: IN=eth0 OUT= MAC=00:40:95:30:84:73:00:e0:4c:39:7b:95:08:00
SRC=192.168.0.9 DST=192.168.0.156 LEN=40 TOS=00 PREC=0x00 TTL=56 ID=28092 PROTO=TCP SPT=57850
DPT=929 SEQ=1127813671 ACK=0 WINDOW=1024 SYN URGP=0
Mar 25 14:44:23 fire Shorewall:loc2fw:DROP: IN=eth0 OUT= MAC=00:40:95:30:84:73:00:e0:4c:39:7b:95:08:00
SRC=192.168.0.9 DST=192.168.0.156 LEN=40 TOS=00 PREC=0x00 TTL=43 ID=24079 PROTO=TCP SPT=57850
DPT=202 SEQ=1127813671 ACK=0 WINDOW=4096 SYN URGP=0
Mar 25 14:44:23 fire Shorewall:loc2fw:DROP: IN=eth0 OUT= MAC=00:40:95:30:84:73:00:e0:4c:39:7b:95:08:00
SRC=192.168.0.9 DST=192.168.0.156 LEN=40 TOS=00 PREC=0x00 TTL=59 ID=64118 CE PROTO=TCP SPT=57850
DPT=1430 SEQ=1127813671 ACK=0 WINDOW=4096 SYN URGP=0
```

Idem il da base MySQL:
mysql> select * from ulog;

```
+------+-----------------------------------------+-------------+--------------+-----------------------+----------+--------+---------+------
------+------------+------------+--------+--------+----------+--------+---------+-------+-----------+----------+----------+-----------
+------------+------------+---------+----------+---------+---------+---------+---------+---------+----------+----------+---------+---------
--+------------+-------------+-------------+-------------+-------------+-------------+-------------+----------+------------+-------------
--+
| id   | raw_mac                                 | oob_time_sec | oob_time_usec | oob_prefix            | oob_mark | oob_in | oob_out |
ip_saddr   | ip_daddr   | ip_protocol | ip_tos | ip_ttl | ip_totlen | ip_ihl | ip_csum | ip_id | ip_fragoff | tcp_sport | tcp_dport | tcp_seq
| tcp_ackseq | tcp_window | tcp_urg | tcp_urgp | tcp_ack | tcp_psh | tcp_rst | tcp_syn | tcp_fin | udp_sport | udp_dport | udp_len |
icmp_type | icmp_code | icmp_echoid | icmp_echoseq | icmp_gateway | icmp_fragmtu | pwsniff_user | pwsniff_pass | ahesp_spi |
local_time | local_hostname |
+------+-----------------------------------------+-------------+--------------+-----------------------+----------+--------+---------+------
------+------------+------------+--------+--------+----------+--------+---------+-------+-----------+----------+----------+-----------
+------------+------------+---------+----------+---------+---------+---------+---------+---------+----------+----------+---------+---------
--+------------+-------------+-------------+-------------+-------------+-------------+-------------+----------+------------+-------------
--+
|    1 | 00:40:95:30:84:73:00:0c:6e:e3:85:78:08:00 |   1111756610 |       625321 | Shorewall:loc2fw:DROP: |        0 | eth0   |
| 3232240110 | 3232240028 |          6 |      0 |     64 |       60 |      5 |   33809 |  4544 |      16384 |    34503 |       23 |
2777837977 |        0 |      5840 |      0 |    NULL |      0 |      0 |      0 |      1 |      0 |     NULL |     NULL |    NULL |     NULL |
NULL |       NULL |       NULL |       NULL |       NULL | NULL       | NULL       |     NULL |     NULL | NULL         |
|    2 | 00:40:95:30:84:73:00:0c:6e:e3:85:78:08:00 |   1111756613 |       623746 | Shorewall:loc2fw:DROP: |        0 | eth0   |
| 3232240110 | 3232240028 |          6 |      0 |     64 |       60 |      5 |   33807 |  4546 |      16384 |    34503 |       23 |
2777837977 |        0 |      5840 |      0 |    NULL |      0 |      0 |      0 |      1 |      0 |     NULL |     NULL |    NULL |     NULL |
NULL |       NULL |       NULL |       NULL |       NULL | NULL       | NULL       |     NULL |     NULL | NULL         |
|    3 | 00:40:95:30:84:73:00:0c:6e:e3:85:78:08:00 |   1111756619 |       623772 | Shorewall:loc2fw:DROP: |        0 | eth0   |
| 3232240110 | 3232240028 |          6 |      0 |     64 |       60 |      5 |   33805 |  4548 |      16384 |    34503 |       23 |
2777837977 |        0 |      5840 |      0 |    NULL |      0 |      0 |      0 |      1 |      0 |     NULL |     NULL |    NULL |     NULL |
NULL |       NULL |       NULL |       NULL |       NULL | NULL       | NULL       |     NULL |     NULL | NULL         |
|    4 | 00:40:95:30:84:73:00:0c:6e:e3:85:78:08:00 |   1111756631 |       622826 | Shorewall:loc2fw:DROP: |        0 | eth0   |
| 3232240110 | 3232240028 |          6 |      0 |     64 |       60 |      5 |   33803 |  4550 |      16384 |    34503 |       23 |
2777837977 |        0 |      5840 |      0 |    NULL |      0 |      0 |      0 |      1 |      0 |     NULL |     NULL |    NULL |     NULL |
NULL |       NULL |       NULL |       NULL |       NULL | NULL       | NULL       |     NULL |     NULL | NULL         |
|    5 | 00:40:95:30:84:73:00:0c:6e:e3:85:78:08:00 |   1111756655 |       619937 | Shorewall:loc2fw:DROP: |        0 | eth0   |
| 3232240110 | 3232240028 |          6 |      0 |     64 |       60 |      5 |   33801 |  4552 |      16384 |    34503
```

Interfacce per Ulogd

Ovviamente per migliorare la consultazione delle registrazioni si può ricorrere al file **ulog_query.php**, contenuto nella directory contrib dei sorgenti, basta specificare al suo interno i parametri per l'accesso al db MySQL:

vi ulog_query.php

```
$link = mysql_connect("localhost", "ulog", "ulogpwd")
or die("No database connection possible!");
mysql_select_db("ulogd")
or die("Database selection failed!");
$select{strlen($select)-1}=" ";
$query = "SELECT ".$select." FROM ulog";
```

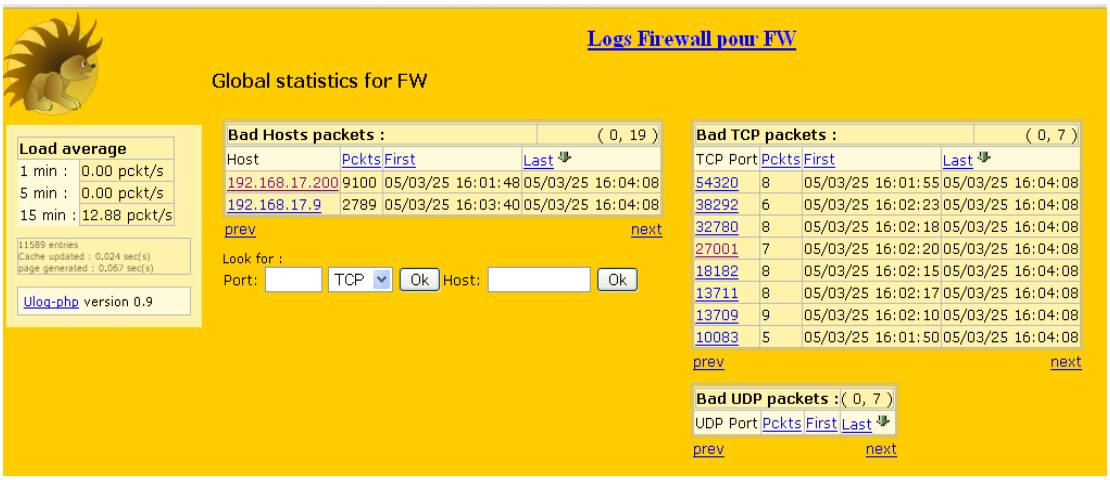
Ulogd-php

Questa interfaccia permette il Controllo via web in modo integrato delle registrazioni.

wget http://www.inl.fr/download/ulog-php-0.9.tar.gz

Il db di ulog va eliminato e ricreato utilizzando il file di dump di questa interfaccia che aggiunge delle tabelle necessarie al suo funzionamento,

mysql ulogd <ulogd.mysqldump -p'pwd'



Altri progetti sono:

Ulogipac
wget http://freshmeat.net/redir/ulogipac/46887/url_tgz/ulogipac_0.04-1.tar.gz

ulog-monitor
wget http://freshmeat.net/redir/ulogmonitor/49026/url_bz2/ulog-monitor_0.3.tar.bz2

Risorse

- http://gnumonks.org/projects/ulogd
- http://www.napolifirewall.com/ptables.htm

Doc: ***ulogd.pdf***

Dott. Paolo PAVAN [Netlink Sas]– pavan@netlink.it
Data*: Marzo 2005*

Note finali

- Il presente documento è a semplice scopo divulgativo
- L'autore non si assume la responsabilità di eventuali danni diretti o indiretti derivanti dall'uso dei programmi, o dall'applicazione delle configurazioni menzionate nel seguente articolo
- I marchi citati sono di proprietà dei rispettivi proprietari e sono stati utilizzati solo a scopo didattico o divulgativo.
- L'uso o il riutilizzo del presente articolo è liberamente consentito per scopi didattici o informativi previa citazione della fonte
- Sono possibili errori o imprecisioni, segnalatemele a pavan@netlink.it
- Chi volesse integrare il presente documento, può scrivere a pavan@netlink.it.