Artikel ini dibuat untuk memonitoring kondisi box linux dari serangan **Ping Of Death, Scanning port,** maupun sekedar eksperimen saja .....
^_^

Cara kerja daemon ini adalah dengan mencatat log yang terdapat pada iptables ke file ***/var/log/ulogd.sylogemu.***

Biasanya log yang tidak menggunakan ulogd akan di memenuhi log ***"dmesg"***. Maka dengan ulogd, log-log yang anda buat pada rule iptables akan dialihkan ke log-nya ulogd. Aku menginstall ulogd ini di mesin
Slackware10
dengan kernel 2.6.8. Tidak ada copyright apapun dalam dukumen ini, anda bebas menyalin, mencetak, maupun memodifikasi (dengan menyertakanBiasanya log yang tidak menggunakan ulogd akan di memenuhi log
"dmesg"
. Maka dengan ulogd, log-log yang anda buat pada rule iptables akan dialihkan ke log-nya ulogd. Aku menginstall ulogd ini di mesin
Slackware10
dengan kernel 2.6.8. Tidak ada copyright apapun dalam dukumen ini, anda bebas menyalin, mencetak, maupun memodifikasi (dengan menyertakan nama penulis asli)

Oke .... saat nya beraksi,... sebelomnya /**me** mengucapkan terima kasih kepada **mas Hari-uh ui**
efnet.indolinux atas supportnya....
^_^

& someone special **Rahma Yurliani** atas Spiritnya ..... *wa ai lu*..... **^_^**

someone special **Rahma Yurliani** atas Spiritnya ..... *wa ai lu*..... **^_^**

Di asumsikan anda telah mengerti konsep TCP/IP dan iptables. sekedar mengulangin tentang iptables anda dapat membaca artikelnya **mas s3trum** di http://efnet.linux.or.id/docs/iptables.html

Bagi yang suka merokok ..... silahkan sambil ngisep tuh ... rokok ..... & tanggung sendiri dampak negatifnya ya. ....

Sorry agak nyindir.... soalnya aku dah berhenti merokok sejak kelas 1 SMU ..... aku mulai merokok dari kelas 5 SD ..... dah bosen ... Hmm jangan lupa makanan ringan ... &. minumnya

ala kadarnya... Juz Alpokat + Terong Belanda .... (kalo mo ikutin porsi aku)

1. Persiapan

Login dari level user biasa ke root, disarankan jangan menjalankan command *"su"*
secara langsung. Biasakan untuk selalu mengetik command tersebut langsung dari nama path-nya, yaitu
"/bin/su"
. Dengan mengetik full pathname, berarti anda menjalankan program
su
langsung dari sumbernya. Metode ini sangat penting guna memproteksi passwd Superuser dari penyadapan program2 Trojan Horse. Selanjutnya masuk ke direktory temporari tempat biasanya anda meng-install tool-tool. Saya biasanya meletakkan di ***/tmp/installer***
, lalu download dan compile tool tersebut.

Login dari level user biasa ke root, disarankan jangan menjalankan command ***"su"*** secara langsung. Biasakan untuk selalu mengetik command tersebut langsung dari nama path-nya, yaitu
"/bin/su"
. Dengan mengetik full pathname, berarti anda menjalankan program
su
langsung dari sumbernya. Metode ini sangat penting guna memproteksi passwd Superuser dari penyadapan program2 Trojan Horse. Selanjutnya masuk ke direktory temporari tempat biasanya anda meng-install tool-tool. Saya biasanya meletakkan di
/tmp/installer
, lalu download dan compile tool tersebut.

```
[sysadmin@router1]$ /bin/su root
```

```
[root@route mkdir /tmp/installer
```

```
[root@router1]# cd /tmp/installer
```

```
[root@router1]# wget -c http://freshmeat.net/redir/ulogd/10896/url_bz2/ulogd-1.02.tar.bz2
```

[root@router1]# bunzip2 ulogd-1.02.tar.bz2

[root@router1]# tar -xf ulogd-1.02.tar

[root@router1]# cd ulogd-1.02

-Disini kita akan melakukan perubahan sedikit path pada file configure karena pada configurasi default sama sekali logging iptables tidak akan ter-log.

Konfigurasi path default nya seperti ini :

/usr/local/sbin/ulogd <== file executie

/usr/local/etc/ulogd.conf <== file konfigurasi

/var/log/ulog.log <== log kondisi daemond

/var/log/ulog.syslogemu <== log laporan iptables

-

Caranya dengan mengedit file configure

```
# --- ubah menjadi seperti ini ---

            bindir='/bin'

            sbindir='/sbin'

            libexecdir='/libexec'

            datadir='/share'

            sysconfdir='/etc'

            sharedstatedir='/com'

            localstatedir='/var'
```

libdir='/lib'

includedir='/include'

oldincludedir='/usr/include'

infodir='/info'

mandir='/man'

-

Compile Source nya

[root@router1]# ./configure

[root@router1]# make

```
[root@router1]# make install
```

Setelah berhasil di install maka file2 penting ulogd akan terletak di direktori :

/sbin/ulogd <== file executie

/etc/ulogd.conf <== file konfigurasi

Lalu jalankan daemon ulogd

```
[root@router1]# /sbin/ulogd -c /etc/ulogd.conf &
```

```
Fri Sep  3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `raw'
```

```
Fri Sep  3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `oob'
```

Fri Sep 3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `ip'

Fri Sep 3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `tcp'

Fri Sep 3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `icmp'

Fri Sep 3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `udp'

Fri Sep 3 13:44:04 2004 <3> ulogd.c:300 registering interpreter `ahesp'

Fri Sep 3 13:44:04 2004 <5> ulogd.c:355 registering output `syslogemu'

Lihat apakah ulogd anda sudah berjalan

[root@router1]# ps ax|grep ulogd

5858 pts/0 S 0:00 /sbin/ulogd -c /etc/ulogd.conf

-

[root@router1]# tail -f /var/log/ulogd.log

Fri Sep 3 13:44:04 2004 <3> ulogd.c:479 ulogd Version 1.01 starting

Fri Sep 3 13:44:04 2004 <5> ulogd.c:696 initialization finished, entering main loop

Oke ..... sekarang daemon ulogd anda sudah jalan .....

Agar dapat dijalankan setiap mesin anda booting maka dapat ditambahkan di rc.local

[root@router1] echo "/sbin/ulogd -c /etc/ulogd.conf &" >> /etc/rc.d.rc.local

2. Konfigurasi Kernel dan Module

Agar kernel anda support dengan iptables maka terlebih dahulu harus mengaktifkan config option CONFIG_IP_NF_TARGET_ULOG pada netfilter dengan me-recompile kernel atau hanya me-recompile module netfilter

[root@router1] cd /usr/src/linux-2.6.7/

[root@router1] make modules SUBDIRS=net/ipv4/netfilter

[root@router1] make modules_install

3. Membuat rule log iptables

Berhubung saya menggunakan distro Slackware, maka rule iptables-nya diletakkin pada /etc/rc.d/rc.firewall
sedangkan untuk distro RedHat dapat diketikkan langsung pada console dan akan tersimpan otomatis pada
/etc/sysconfig/iptables

/usr/sbin/ip '< Ping Scan PUT -p icmp --icmp-type "echo-request" -m limit --limit 5/minu

/usr/sbin/iptables -A in_tcp -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-bu

--ul '< Stealth Scan >'

/usr/sbin/iptables -A in_tcp -p tcp --tcp-flags ALL FIN,URG,PSH -m limit --limit 5/m -j ULOG --ul

'< XMAS Scan >'

/usr/sbin/iptables -A in_tcp -p tcp --tcp-flags SYN,RST SYN,RST -m limit --limit 5/m -j ULOG --u

'< SYN/RST Scan>'

/usr/sbin/iptables -A in_tcp -p tcp --tcp-flags SYN,FIN SYN,FIN -m limit --limit 5/m -j ULOG --ulo

'< SYN/FIN Scan>'

Restart iptables anda, untuk mesin Slackware

[root@router1]# /etc/rc.d/rc.inet2 restart

Untuk mesin Redhat

[root@router1]# /etc/inet.d/iptables save

[root@router1]# /etc/inet.d/iptables restart

4. Mengetes logging iptables

Setelah ulogd di running kan dan iptables direstart ..... saat nya anda mengetest loging tersebut .....

Skenario yang saya buat adalah dimana mesin router1 (192.168.0.2) di Ping oleh Win2003 server
(192.168.0.1)

dan port scanner dari Notebook (192.168.3.37)

Ping yang dilakukan oleh Win2003 Server

***=======================================**

Welcome to Microsoft Telnet Server.

***=======================================**

C:\Documents and Settings\Administrator>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time<1ms TTL=64

Reply from 192.168.0.2: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

-

Kemudian lihat hasil logging iptablesnya :

[root@router1]# tail -f /var/log/ulogd.syslogemu

Sep 3 13: < Ping Scan IN=eth0 OUT= MAC=00:80:48:11:c2:d7:00:c1:28:01:ce:2f:08:00 SRC=1

DST=192.168.0.2 LEN=60 TOS=00 PREC=0x00 TTL=128 ID=433 PROTO=ICMP TYPE=8 CODE=0

Sep 3 13: < Ping Scan IN=eth0 OUT= MAC=00:80:48:11:c2:d7:00:c1:28:01:ce:2f:08:00 SRC=1

DST=192.168.0.2 LEN=60 TOS=00 PREC=0x00 TTL=128 ID=435 PROTO=ICMP TYPE=8 CODE=0

Port Scanning dari IP 192.168.3.37

[root@iman]# nmap -v www.imanibbi.ac.id

Starting nmap 3.50 (http://www.insecure.org/nmap/) at 2004-09-03 13:51 WIT

Host ns1.imanibbi.ac.id (192.168.2.1) appears to be up ... good.

Initiating SYN Stealth Scan against ns1.imanibbi.ac.id (192.168.2.1) at 13:51

Kemudian lihat lagi hasil logging iptablesnya :

[root@router1]# tail -f /var/log/ulogd.syslogemu

Sep 3 14: < Stealth Sc IN=eth2 OUT= MAC=00:80:48:17:0d:57:00:80:48:17:0d:4a:08:00

SRC=192.168.3.37 DST=192.168.2.1 LEN=40 TOS=00 PREC=0x00 TTL=63 ID=230 DF PROTO=T

SEQ=138215714 ACK=0 WINDOW=0 RST URGP=0

Dari hasil logging diatas kelihatan bahwa ip 192.168.0.1 dan 192.168.3.37 masing-masing telah melakukan ping dan port scanning.

Untuk contoh-contoh rule logging yang lain, anda dapat mencarinya di !google ..... ^_^

Selamat Mencoba, Salam dari Medan City

5. Referensi

1. http://freshmeat.net/redir/ulogd/10896/url_homepage/ulogd

2. www.netfilter.org

3. Manual page iptables

4. file README pada paket ulogd

5. MailingList http://freshmeat.net/redir/ulogd/10896/url_list/ulogd

==========

<<-I.R-Harahap-Medan -->>

Aku bukanlah orang yang merasa pandai :-(

Aku selalu menganggap diriku orang yg kekurangan :-(

Dgn kekurangan itulah aku mau belajar agar bisa pandai :-)

sangat menarik