Tips Mencegah Server Linux dari IP Spoofing, Flooding dan Rootkit

Dony Ramansyah
dony_im2@yahoo.co.id
http://dony-ramansyah.bravehost.com

Pendahuluan

Anda mungkin pernah kesal dengan program mengganggu seperti spyware, malware maupun virus yang sangat menjengkelkan dan bahkan lebih parah lagi dapat merusak data2 yang ada pada komputer. Namun hal ini hanya terjadi pada keluarga Sistem Operasi (OS) Windows saja, barsyukurlah bila kita menggunakan Linux :).

Ada satu perbandingan yang sangat menarik menurut saya. Silahkan coba install OS Windows yang fresh belum di install apapun juga termasuk patch, dan Linux yang juga fresh belum tersentuh patch. Lalu anda hubungkan ke Internet..., lihat siapa duluan yang di install ulang. He..he.. Anda pasti tahu jawabannya.

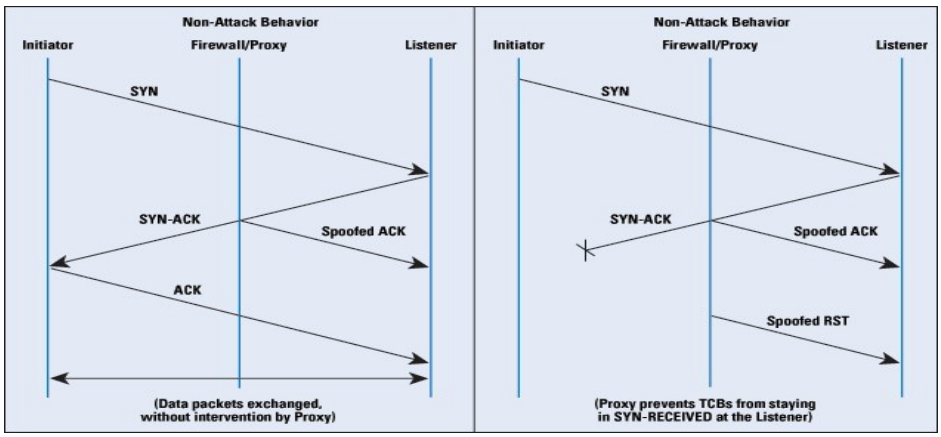
Semua yang baca ini pasti saya anggap sudah tahu bahwa setiap Sistem Operasi tidak selalu aman dari berbagai gangguan yang dapat membahayakan data-data yang ada. Seperti pada keluarga OS Windows bahwa Linux juga memerlukan perhatian yang extra dalam masalah security. Walaupun linux secara default sudah tentu lebih aman dibandingkan Windows.

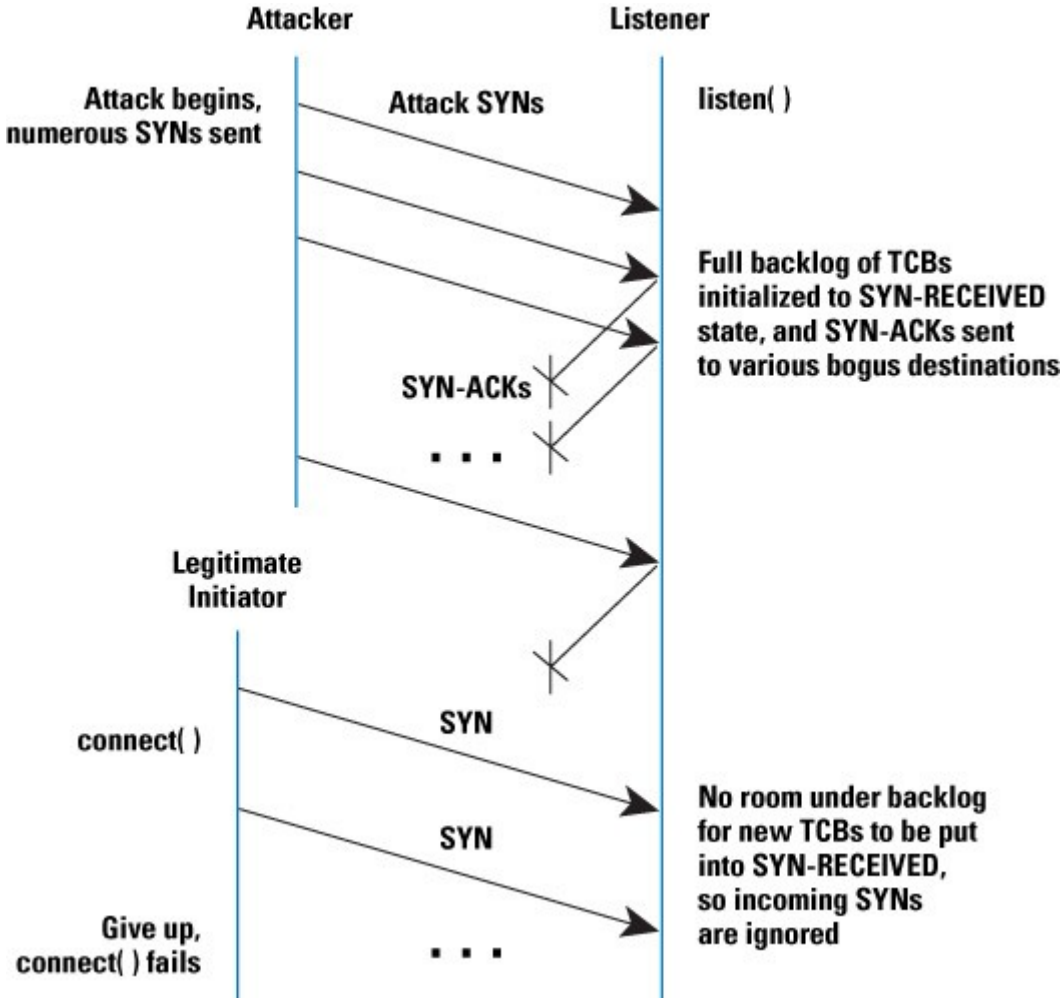
Di Linux juga tidak menutup kemungkinan memiliki celah keamanan yang cukup membahayakan. seperti virus (namun jumlahnya sangat minim), rootkit (semacam program untuk mengambil alih root kita). flooding (pengiriman traffic besar diluar batas atau dikenal DDoS), Spoofing (menduplikat IP), dll

Untuk itu disini saya akan menjelaskan sedikit trik untuk mengamankan Linux kita dari serangan flooding dan IP spoffing serta bagaimana mengaudit Linux kita dari hal-hal yang membahayakan seperti rootkit yang ada.

Isi

Linux by default pada kernelnya sudah memiliki fasilitas untuk memblokir Flood karena TCP/IP SYN cookies dan IP spoofing.





Gambar diatas menjelaskan bagaimana proses terjadinya Flood karena TCP/IP SYN cookies.

Untuk menjegahnya kita hanya perlu mengkatifkan option TCP/IP SYN cookies dan Spoof protection (rp_filter).

File tersebut berada di "/etc/sysctl.conf"

```
# cat /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com
#net/ipv4/icmp_echo_ignore_broadcasts=1

# the following stops low-level messages on console
kernel.printk = 4 4 1 7
```

 # enable /proc/$pid/maps privacy so that memory relocations are not
 # visible to other users.
kernel.maps_protect = 1

###3
 # Functions previously found in netbase
#

 # Uncomment the next line to enable Spoof protection (reverse-path filter)
#net.ipv4.conf.default.rp_filter=1

 # Uncomment the next line to enable TCP/IP SYN cookies
#net.ipv4.tcp_syncookies=1

 # Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.conf.default.forwarding=1

 # Uncomment the next line to enable packet forwarding for IPv6
#net.ipv6.conf.default.forwarding=1

Secara default pertama kali instalasi pada baris net.ipv4.tcp_syncookies=1 dan net.ipv4.conf.default.rp_filter=1 masih dalam keadaan tidak aktif. Untuk mengaktifkannya tinggal membuang tanda # di depannya dan kemudian simpan.

Untuk mengeditnya di ubuntu dengan :

$ sudo gedit /etc/sysctl.conf
lalu edit dan simpan kembali

Untuk melalui konsole yang lain dapat menggunakan text editor lewat konsole seperti mc, vi, maupun joe, dll.

Sekarang isi dari sysctl.conf anda jadi seperti ini :

 # /etc/sysctl.conf - Configuration file for setting system variables
 # See sysctl.conf (5) for information.
#

#kernel.domainname = example.com
#net/ipv4/icmp_echo_ignore_broadcasts=1

 # the following stops low-level messages on console

kernel.printk = 4 4 1 7

 # enable /proc/$pid/maps privacy so that memory relocations are not
 # visible to other users.
kernel.maps_protect = 1

###3
 # Functions previously found in netbase
#

 # Uncomment the next line to enable Spoof protection (reverse-path filter)
net.ipv4.conf.default.rp_filter=1

 # Uncomment the next line to enable TCP/IP SYN cookies
net.ipv4.tcp_syncookies=1

 # Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.conf.default.forwarding=1

 # Uncomment the next line to enable packet forwarding for IPv6
#net.ipv6.conf.default.forwarding=1

Cukup mudah bukan... :)
tinggal anda restart PC anda dan kemudian modul tersebut akan otomatis jalan pada kernel anda.

Audit Linux Anda...

Rootkit pada Linux cukup banyak jenisnya dan beragam, biasanya digunakan oleh pada cracker untuk mengambil alih login root anda.

Didalam OS Windows untuk mengaudit security yang ada di PC kita dapat menggunakan software GFI LanGuard, tapi sayang software ini berbayar dan harganya pun cukup mahal. (www.gfi.com/languard/).

Di Linux anda dapat menggunakan rkhunter, Ada beberapa program yang bisa dipakai untuk mendeteksi adanya rootkit pada system. Rootkit detector kit, chkrootkit dan Rkhunter adalah contoh yang bisa digunakan.

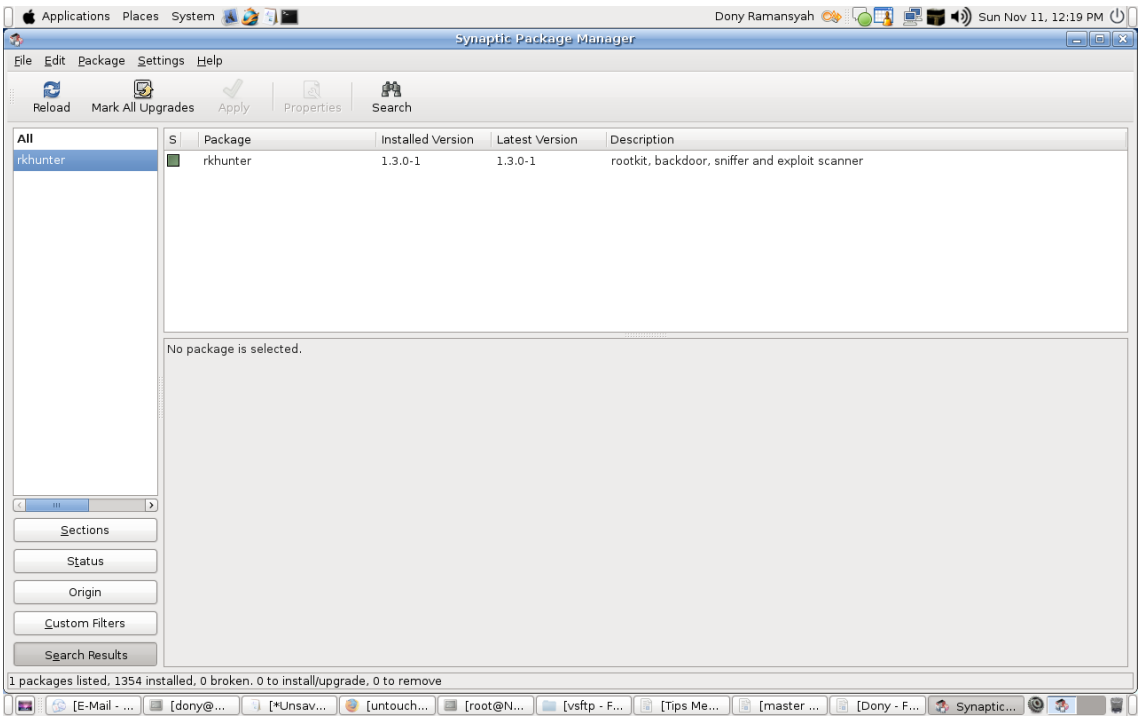
"rkhunter" ini gratis anda dapatkan di : www.rootkit.nl/projects/rootkit_hunter.html.

Untuk keluarga debian dan ubuntu, dll dapat langsung mengunduh langsung dari repositori yang ada :

ubuntu :
$ sudo apt-get install rkhunter

atau melalui synaptic :

Menu System – Administration – Synaptics Package Manager



Gambar tampilan synaptics pada ubuntu

Jika menginstall manual dapat mengikuti langkah berikut :

 # tar -xvzf rkhunter.tgz
 # cd rkhunter
 # # ls
files installer.sh
#

jalankan installer nya :

#./installer.sh

Tunggu sampai proses instalasi selesai.

Setalah selesai dengan install maka pertama kali kita harus mengupdate rkhunter tersebut terlebih dahulu agar dapat mengenali rootkit terbaru yang ada.

 # rkhunter --update
(Untuk mengupdate database rootkit terbaru)

Untuk menjalankannya dapat melihat file help yang ada :

 # rkhunter --help

Usage: rkhunter {--check | --update | --propupd | --versioncheck |
--list [tests | languages | rootkits] |
--version | --help} [options]

Current options are:

--append-log	*Append to the logfile, do not overwrite*
--bindir <directory>...	*Use the specified command directories*
-c, --check	*Check the local system*
--cs2, --color-set2	*Use the second color set for output*
--configfile <file>	*Use the specified configuration file*
--cronjob	*Run as a cron job*
	(implies -c, --sk and --nocolors options)
--dbdir <directory>	*Use the specified database directory*
--debug	*Debug mode*
	(Do not use unless asked to do so)
--disable <test>[,<test>...]	*Disable specific tests*
	(Default is to disable no tests)
--display-logfile	*Display the logfile at the end*
--enable <test>[,<test>...]	*Enable specific tests*

	(Default is to enable all tests)
--hash {MD5 | SHA1 | NONE | <command>}	*Use the specified file hash function (Default is SHA1)*
-h, --help	*Display this help menu, then exit*
--lang, --language <language>	*Specify the language to use (Default is English)*
--list [tests | languages | rootkits]	*List the available test names, languages, or checked for rootkits, then exit*
-l, --logfile [file]	*Write to a logfile (Default is /var/log/rkhunter.log)*
--noappend-log	*Do not append to the logfile, overwrite it*
--nocolors	*Use black and white output*
--nolog	*Do not write to a logfile*
--nomow, --no-mail-on-warning	*Do not send a message if warnings occur*
--ns, --nosummary	*Do not show the summary of check results*
--novl, --no-verbose-logging	*No verbose logging*
--pkgmgr {RPM | DPKG | BSD | NONE}	*Use the specified package manager to obtain or verify file hash values. (Default is NONE)*
--propupd	*Update the file properties database*
-q, --quiet	*Quiet mode (no output at all)*
--rwo, --report-warnings-only	*Show only warning messages*
-r, --rootdir <directory>	*Use the specified root directory*
--sk, --skip-keypress	*Don't wait for a keypress after each test*
--summary	*Show the summary of system check results (This is the default)*
--syslog [facility.priority]	*Log the check start and finish times to syslog (Default level is authpriv.notice)*
--tmpdir <directory>	*Use the specified temporary directory*
--update	*Check for updates to database files*
--vl, --verbose-logging	*Use verbose logging (on by default)*
-V, --version	*Display the version number, then exit*
--versioncheck	*Check for latest version of program*
-x, --autox	*Automatically detect if X is in use*
-X, --no-autox	*Do not automatically detect if X is in use*

dari option diatas untuk menjalankannya ketik perintah :

 # rkhunter -c

tunggu sampai dia selesai mengecek system kita, jika ada konfirmasi untuk melanjutkan tekan tombol “ENTER”

Berikut capture nya :

```
# rkhunter -c
[ Rootkit Hunter version 1.3.0 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                 [ None found ]
    Checking for preload file                 [ Not found ]
    Checking LD_LIBRARY_PATH variable         [ Not found ]

  Performing file properties checks
    Checking for prerequisites                [ OK ]
    /bin/bash                                 [ OK ]
    /bin/cat                                  [ OK ]
    /bin/chmod                                [ OK ]
    /bin/chown                                [ OK ]
    /bin/cp                                   [ OK ]
    /bin/date                                 [ OK ]
    /bin/df                                   [ OK ]
    /bin/dmesg                                [ OK ]
    /usr/bin/ldd                              [ Warning ]
    /usr/bin/less                             [ OK ]
    /usr/bin/locate                           [ OK ]
    /usr/bin/logger                           [ OK ]
    /usr/bin/lsattr                           [ OK ]
    /usr/bin/lsof                             [ OK ]
    /usr/bin/md5sum                           [ OK ]
    /usr/bin/newgrp                           [ OK ]
    /usr/bin/passwd                           [ OK ]
    /usr/bin/perl                             [ OK ]
    /usr/bin/pstree                           [ OK ]
    /usr/bin/rkhunter                         [ OK ]
    /usr/bin/rpm                              [ Warning ]
    /usr/bin/runcon                           [ OK ]
    /usr/bin/sha1sum                          [ OK ]
    ..... (cut)
    .....
    /usr/sbin/usermod                         [ OK ]
    /usr/sbin/vipw                            [ OK ]
```

[Press <ENTER> to continue]

Checking for rootkits...

Performing check of known rootkit files and directories

55808 Trojan - Variant A	*[Not found]*
ADM Worm	*[Not found]*
AjaKit Rootkit	*[Not found]*
aPa Kit	*[Not found]*
Apache Worm	*[Not found]*
Ambient (ark) Rootkit	*[Not found]*

..... (cut)

System checks summary
==========

File properties checks...
Files checked: 123
Suspect files: 2

Rootkit checks...
Rootkits checked : 109
Possible rootkits: 0

Applications checks...
Applications checked: 3
Suspect applications: 0

The system checks took: 1 minute and 18 seconds

All results have been written to the logfile (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

---------- eof ----------

Dari hasil resume yang diberikan kita dapat melihat apakah System Linux kita sudah aman, hasil resume ini juga memberitahukan rootkit yang terdeteksi dan suspect file yang ada.

Penutup

So.. jangan lupa untuk selalu mengaudit sistem anda, jangan sampai terlena bahwa sistem yang anda miliki sudah pasti aman karena bukan dari keluarga Windows, namun hal tersebut pun tidaklah salah :)

"rkhunter" pun akan menampilkan hasil akhir sehingga kita bisa tahu dimana sistem kita memiliki hole / bugs yang mungkin saja itu merupakan jalan masuk bagi intruder / aksi hacker yang tidak bertanggung jawab.

Tunggu apalagi segera audit sistem operasi anda.

Referensi

http://www.rootkit.nl
http://www.debian.org/doc/manuals/securing-debian-howto/

Biografi Penulis

Dony Ramansyah. Sedang Menyelesaikan S1 di STMIK Nusa Mandiri. Lulus dari STM Pembangunan Jakarta tahun 2003 dengan lama pendidikan 4 Tahun (3 tahun + 1 tahun magang). Pernah bekerja di PT. Limawira Wisesa sebagai Internal Web Develomment, IT Support, Sales Enginer. Dan pernah juga bekerja di PT. Sisindokom sebagai IT Support dan Network Enginer. Sekarang bekerja di divisi NOC di PT. Indosat Mega Media (IM2) dan.

Dony Ramansyah
site : http://dony-ramansyah.bravehost.com
blog : dony-ramansyah.blogspot.com
Registered linux user : ID 400171