Bagi yang memiliki server yang selalu terhubung dengan intenet, tentunya pernah melihat di dalam log filenya bahwa telah terjadi usaha membobol server kita oleh cracker, baik secara langsung ataupun melalui script seperti d
ictionary attack
ataupun
brute force attack
. Di dalam log file biasanya kita menemukan entry seperti ini /var/log/messages banyak sekali:

Mar 20 19:28:17 serverku sshd(pam_unix)[14456]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.178.20.170
Mar 20 19:28:24 serverku sshd(pam_unix)[14458]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.178.20.170
Mar 20 19:28:30 serverku sshd(pam_unix)[14460]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.178.20.170 user=root
Mar 20 19:28:37 serverku sshd(pam_unix)[14462]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.178.20.170 user=root
Mar 20 19:28:44 serverku sshd(pam_unix)[14464]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.178.20.170 user=root
Mar 20 19:28:51 serverku sshd(pam_unix)[14466]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.178.20.170
Mar 20 22:15:13 serverku sshd(pam_unix)[15883]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=220.73.231.29
Mar 20 22:15:17 serverku sshd(pam_unix)[15885]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=220.73.231.29
Mar 20 22:15:22 serverku sshd(pam_unix)[15887]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=220.73.231.29
Mar 20 22:15:26 serverku sshd(pam_unix)[15889]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=220.73.231.29
Mar 20 22:15:30 serverku sshd(pam_unix)[15891]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=220.73.231.29
Mar 21 00:22:03 serverku sshd(pam_unix)[16944]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.73.4.119 user=root
Mar 21 00:22:10 serverku sshd(pam_unix)[16946]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.73.4.119 user=root
Mar 21 00:22:17 serverku sshd(pam_unix)[16948]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.73.4.119 user=root

Hal ini kadang2 terjadi dalam jumlah yang sering sekali, seperti dapat kita lihat di dalam notifikasi LogWatch kita:

sshd:
Authentication Failures:

unknown (210.72.201.10): 232 Time(s)
root (host-ip167-189.crowley.pl): 89 Time(s)
unknown (220.117.240.34): 35 Time(s)
root (220.117.240.34): 16 Time(s)
apache (210.72.201.10): 1 Time(s)
apache (220.117.240.34): 1 Time(s)
bin (210.72.201.10): 1 Time(s)
ftp (220.117.240.34): 1 Time(s)
mail (210.72.201.10): 1 Time(s)
mysql (210.72.201.10): 1 Time(s)
mysql (220.117.240.34): 1 Time(s)
nobody (210.72.201.10): 1 Time(s)
postgres (210.72.201.10): 1 Time(s)
root (210.72.201.10): 1 Time(s)
xfs (210.72.201.10): 1 Time(s)
Invalid Users:
Unknown Account: 267 Time(s)

Memang sih biasanya hal ini sebenarnya relatif tidak berbahaya asalkan kita telah mengamankan server kita, minimal menggunakan password yang sulit ditebak dan rutin melakukan update.

Namun alangkah baiknya jika kita dapat lebih mengamankan server kita dengan cara memblok IP para cracker itu agar mereka tidak leluasa di dalam usahanya membobol server kita.

Untuk hal ini kita dapat menggunakan script yang namanya denyhosts.
Dari keterangan yum:

DenyHosts is a script intended to help Linux system administrators thwart
ssh server attacks. DenyHosts scans an ssh server log, updates
/etc/hosts.deny after a configurable number of failed attempts from a
rogue host is determined, and alerts the administrator of any suspicious
logins. http://denyhosts.sourceforge.net/

Cara menginstall denyhosts:
yum install denyhosts

Setelah terinstall, kita tinggal mensetupnya. File contoh konfigurasi telah tersedia di dalam direktori:
/usr/share/doc/denyhosts-2.2/

Langkah2nya:
1. Copy file denyhosts.conf-dist ke dalam /etc/denyhosts/denyhosts.cfg

Edit file /etc/denyhosts/denyhosts.cfg itu, dan sesuaikan dengan kebutuhan kita. Biasanya pakai yang standar pun sudah cukup, tapi kita bisa mengubahnya sesuai kebutuhan kita, misalnya option:
DENY_THRESHOLD_INVALID = 5 <-- sampai berapa kali gagal login utk user yg TIDAK ADA kita memblok IP tersebut.
DENY_THRESHOLD_VALID = 10 <-- sampai berapa kali gagal login utk user yg ADA kita memblok IP tersebut.
DENY_THRESHOLD_ROOT = 1 <-- bila kita mengatur sshd kita tidak dapat login root, maka begitu ada yang mencoba login sebagai root, kita dapat langsung membloknya.
ADMIN_EMAIL = emailkamu@domainkamu.com <-- kita bisa mengatur agar kita dinotifikasi lewat email setiap ada yang telah terblok oleh denyhosts.

Silahkan di explore deh option2 yang ada, keterangannya cukup jelas kok.

2. Selanjutnya, kita mengcopy startup script denyhosts ke dalam direktori /etc/init.d/
cp /usr/share/doc/denyhosts-2.2/daemon-control /etc/init.d/denyhosts

Jangan lupa untuk menyesuaikannya sedikit. Edit file tersebut:
DENYHOSTS_CFG = "/etc/denyhosts/denyhosts.cfg"

3. Trus kita masukkan service denyhosts ini ke dalam startup Linux kita:
chkconfig --add denyhosts
chkconfig --level 345 denyhosts on

4. Kita jalankan servicenya:
service denyhosts start

Tunggulah sehari dua hari, maka kita akan mulai menerima report dari server kita bahwa telah "tertangkap dan terblok" beberapa buah IP:

Email message follows:
From: DenyHosts <nobody@localhost>
To: emailkamu@domainkamu.com
Subject: DenyHosts Report
Date: Mon, 27 Mar 2006 19:44:15 +0700

Added the following hosts to /etc/hosts.deny:

148.245.12.101 (na-12-101.na.avantel.net.mx)
202.181.213.162 (unknown)
61.218.185.123 (61-218-185-123.HINET-IP.hinet.net)
141.24.205.224 (ktxeon.theoinf.tu-ilmenau.de)
61.153.4.55 (unknown)
59.120.13.130 (59-120-13-130.HINET-IP.hinet.net)
200.243.33.5 (unknown)
220.95.230.169 (unknown)

Kesimpulan dan penutup
Nah, dengan terbloknya IP-IP tersebut, maka setidaknya para cracker akan cukup kesulitan sebab peluangnya untuk membobol server kita menjadi lebih sempit. Semoga tulisan ini dapat membantu kamu di dalam mengamankan servermu.

v.0.1 by ari_stress a.k.a tiger74 a.k.a Fajar Priyanto Bukit Sentul, 30 March 2006. Email: fajarpri at arinet dot org. He is a Microsoft Certified Professional who falls in love with Linux. Working at an automotive dealer in Jakarta