差出人: **Naruaki TOMA** tnal@ie.u-ryukyu.ac.jp
件名: (shark) sshdへのアタック
日付: 2014年4月16日 12:58
宛先: ML Lab. nal-lab@eva.ie.u-ryukyu.ac.jp nal-lab@eva.ie.u-ryukyu.ac.jp
CC: 當間愛晃 tnal@ie.u-ryukyu.ac.jp

當間です。

何故か shark への ssh ログインができない／しづらくなっていたのですが、
/var/log/secure を眺めた結果以下のような root ログイン試行が大量に届いてました。

==========
Apr 16 12:47:39 shark sshd[10966]: PAM service(sshd) ignoring max retries; 7 > 3
Apr 16 12:47:39 shark sshd[10972]: Failed password for root from 59.63.167.182 port 40683 ssh2
Apr 16 12:47:40 shark sshd[10974]: Failed password for root from 59.63.167.182 port 40782 ssh2
Apr 16 12:47:40 shark sshd[10982]: Failed password for root from 59.63.167.182 port 41102 ssh2
Apr 16 12:47:40 shark sshd[10975]: Failed password for root from 59.63.167.182 port 40787 ssh2
Apr 16 12:47:40 shark sshd[10976]: Failed password for root from 59.63.167.182 port 40791 ssh2
Apr 16 12:47:40 shark sshd[10977]: Failed password for root from 59.63.167.182 port 40792 ssh2
Apr 16 12:47:40 shark sshd[10983]: Failed password for root from 59.63.167.182 port 41120 ssh2
Apr 16 12:47:41 shark sshd[10970]: Failed password for root from 59.63.167.182 port 40245 ssh2
Apr 16 12:47:41 shark sshd[10968]: Failed password for root from 59.63.167.182 port 39537 ssh2
Apr 16 12:47:41 shark sshd[10969]: Disconnecting: Too many authentication failures for root
==========

上記だと 59.63.167.182 からの攻撃ですね。
で、sshd にはデフォルト設定で「ログイン失敗しすぎると怪しい」ということで
　　Disconnecting: Too many authentication failures for root
　　PAM service(sshd) ignoring max retries; 7 > 3
が短時間に繰り返されまくる（上記のログだと2秒で上限に達している）ことになってました。
暫く待つと sshd がまた通常モードに戻るので、再度上記を繰り返すと。

ということで、試しに /etc/hosts.deny にて 59.63.167.182 からのアクセスを
弾くように
　　sshd : 59.63.167.182
と記述を加え、sshd をリロードしました。
この結果、現時点では /var/log/secure では

Apr 16 12:52:05 shark sshd[11334]: refused connect from ::ffff:59.63.167.182 (::ffff:59.63.167.182)

のように refused に変化しています。
また、ssh通常通りにログインできるはずです。

これで暫く様子を見てみます。

Naruaki Toma
E-mail: tnal@ie.u-ryukyu.ac.jp, Tel: 098-895-8830
http://www.eva.ie.u-ryukyu.ac.jp/~tnal/
working: http://ie.u-ryukyu.ac.jp/~tnal/