ADANAC SOFTWARE

More ssh ideas

A friend recently got 'rooted'. He was using ssh (not ssh2). He was getting pages on his phone and processes were dying and such, so he installed "chkrootkit" which is a program that checks your system to see if there is any of a number of root kits installed. He had SuckIt installed on his machine and now has a server to rebuild

Unfortunately he used ssh to login and check his other server, so now he has 2 servers to rebuild.

Since I noticed my /var/log/secure file getting large at the beginning of the month I've made some changes to sshd_config:

1. PermitRootLogin no Users just have to login to an unprivileged account, then su if they want root access.

2. Banner /etc/banner This file is displayed after you enter your user name. I changed the banner file as below:

password:

$

Unauthorized use of this service is strictly prohibited. Unauthorized attempts to use this service, upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

I put "password:" and "$" in the banner to trip up the automated scripts these guys appear to be using. I don't know if it works, it just seems like a good idea.

3. DenyUsers adm admin apache bin daemon dovecot ftp games gopher halt lp mail mail null mysql named news nfsnobody nobody nscd operator pcap postgres rpc rpcuser rpm shutdown simon smmsp squid sshd sync uucp vcsa webalizer

A list of all the folks who cannot login.

4. AllowUsers boopy A list of all the folks who can login, just in case I left anyone out of the previous list. Only boopy gets in.

Finally, I populated hosts.deny with the apparent IP addresses of the worst offenders:

```
ALL:
222.237.79.237\
210.68.8.169\
68.58.89.36\
200.164.92.234\
162.39.201.74\
67.172.114.3\
206.165.120.54\
222.122.60.42\
211.136.90.75\
 .
 .
 .
141.28.18.200
```

ALL services are denied to these IP addresses. Well, I guess the well trained hacker changes his IP address often, but since I made this change login attempts are down to 10% of what they were. I add them 1 per line so I don't go berserk maintaining the list. Note that the \ character 'continues' the line.

5. I enable VerifyReverseMapping, but I haven't seen this work. It doesn't deny me access from the IP address I always use. It sounds like people who fail a 'reverse IP address' test of some sort (phony IP addresses?) get rejected.

Here's a little widget I wrote this morning for summarizing my secure log. Way better than actually reading it. I take these results and update /etc/hosts.deny. I have most of South Korea and Taiwan blocked now.

```
[root@mammoth tmp]# cat test grep 'Failed password' /var/log/secure|cut -d ']' --
fields=2|cut -d ' ' --fields=9|uniq -c|sort -nr

[root@mammoth tmp]# sh test
707 209.253.78.9
600 193.178.210.35
115 217.34.37.166
107 63.107.208.110
90 81.169.137.164
9 211.184.70.140
8 208.13.106.89
1 211.90.27.133
1 211.157.102.10
```

