IP-PBX Security Best Practices v.1.0

by Matt Martin and VCCS Telecom
http://www.vccs.ca

Linux and SIP hack attempts are all too common. There are dozens of stories out there including a client of mine that incurred $18,000 in losses. Here are a few tips on securing your Phone System.

1) Make sure all passwords are changed from the defaults immediately.

Root:
> passwd

Mysql:
mysql asterisk --execute="UPDATE mysql.user SET Password=PASSWORD('XXXX') WHERE User='root';"
mysql asterisk --execute="FLUSH PRIVILEGES;"

- **Don't forget the Admin passwords if any through the Admin GUI.**
- **Only login with a standard user account and use "sudo" when needed.**
- **Use Complex SIP Passwords for Extensions and Trunks!**

2) If using VoIP.

- Use IP AUTHENTICATION with your SIP Provider!! Avoid registrations with passwords at ALL costs if you can!
- Instead of using a registration string use "Qualify=yes".

3) Things to notice in your CLI: "Pinball activity".
Multiple Messages such as **"wrong password for ext xx"** or **"attempting to register but host is not dynamic"** etc. Basically random messages with IP's that you do not recognize. Don't confuse them with your remote agents though! Use IPtables to block malicious IPs.

iptables -A INPUT -s x.x.x.x -j DROP (add blocked IP)

(CentOS)

> /etc/init.d/iptables save (save settings)

(Debian)
To allow ONLY specific IPs

iptables -A INPUT -s "friendlyip.1" -j ACCEPT

iptables -A INPUT -s "friendly.ip.2" -j ACCEPT

iptables -A INPUT -s 127.0.0.1 -j ACCEPT # yes, accept connections from localhost.

Save--
iptables -A INPUT -s 0/0 -j DROP

- **Don't forget your remote IP if needed and your ISP/Router/Gateway.**

4) There are more root password hack attempts than SIP registration hacks due to linux hack attempts versus targeted SIP hack attempts. Lock down remote SSH wrong password attempts.

1. Open /etc/pam.d/sshd in a text editor.

2. Right before @include common-auth, add the following on its own line:

auth required pam_tally.so onerr=fail deny=3 unlock_time=120

3. Right before @include common-account, add the following on its own line:

account required pam_tally.so reset

- See also /var/log/auth.log

5) Disable un-needed services such as FTP, TFTP, and any other remote access services not needed.

Best of luck and happy calling!

Matthew Martin
Chief Consultant
VCCS Telecom