

February 24, 2009

How to Secure Your PBX in a Flash System

By Allan Levene
Network Consultants, Inc.
Kennesaw, GA 30144
<http://www.networkconsultantsinc.com>
sales@networkconsultantsinc.com

About 3 months ago, I found that my PIAF system had been hacked. I still don't know how it was done, but before then I hadn't done anything but use complex passwords thinking that that was enough. It wasn't. Here's what I discovered and what I did about it to stop another attack. I have since found that my PIAF system is attacked four times a day, on average from all over the world.

The first thing was to change all of the passwords where possible; the second to secure root (the Linux Super-User/Administrator) as if a hacker gets root access it's all over; the third to secure Webmin (which is how the hacker got in I think); the fourth to disable or uninstall Samba, and the fifth to stop multiple brute force attacks.

After changing the root and other passwords to more complex ones, I focused on Webmin. Webmin is a wonderful tool to graphically access any part of your system and make changes to your system. If installed after PIAF you would access it using a browser at <yourPIAFserver IP address:10000) If installed with PIAF it's :9001. I concluded that allowing root to operate in Webmin was a huge mistake. Webmin has a section called configuration. In this section you can -

- Add a new user and give them root permissions
- Delete the root user
- Change the port number for accessing Webmin, from 10000 to something else
- Add a personal security certificate so that only users with that installed in their browser can access Webmin
- Force secure sockets (https) access if you want, obscuring your web access.
- Only allow specific IP addresses to access the Apache PIAF user/admin web pages.

In addition, by working in the Servers section, you can modify the SSH (secure shell) connection, which is the most common form of attack, to completely block an attacker.

First, the Webmin configuration using my version, 1.450 -

How to Secure Your PBX in a Flash System



Click on Webmin, and then Webmin Configuration. You'll see (if you have the latest version) a page full of icons. Click on the IP Access Control button.

Module Index

IP Access Control

The Webmin server can be configured to deny or allow access only from certain IP addresses using this form. Hostnames (like foo.bar.com) and IP net can also be entered. You should limit access to your server to trusted addresses, especially if it is accessible from the Internet. Otherwise, anyone wh your system.

The screenshot shows the 'Access control options' form. It has three radio buttons: 'Allow from all addresses' (unselected), 'Only allow from listed addresses' (selected), and 'Deny from listed addresses' (unselected). Below the radio buttons is a text input field containing '192.168.1.5' and 'mypbx.dyndns.com'. A yellow callout box with an arrow pointing to the input field contains the text 'Addresses to left ARE permitted'. At the bottom of the form, there is a checkbox for 'Resolve hostnames on every request?' which is checked, and a 'Save' button. A blue arrow points to a link that says 'Return to Webmin configuration'.

You can enter only the specific IP addresses or dynamic domain names that will be allowed to access Webmin. If you want your laptop to have access, setup a free account at dyndns.org, install a small free software product to ping the dyndns.org with your current IP address whenever you use your laptop and then connect to Webmin from it. When you access Webmin from the road, PIAF will recognize the temporary IP address as valid and

How to Secure Your PBX in a Flash System

open the first software door.

[Module Index](#)

Ports and Addressse

IP addresses and ports

Listen on IPs and ports

Bind to IP address

Any address

Listen on port

Specific port 54125

Same as first

Listen for broadcasts on UDP port

Don't listen 9001

Web server hostname

Work out from browser

Reverse-resolve connected IP address?

Yes No

Save

[Return to Webmin configuration](#)

This number is entered after the :

Next, you'll need to change the port that Webmin uses. Click on the Ports and Addresses icon and enter a random port number (54125, for example) that isn't used by another software service, such as 21, 22, 25, 80, etc., in the Listen on Ports section so that when you want to connect to Webmin, you'll have to use xxx.xxx.xxx.xxx (or a domain name using a dyndns.org account) with a : and 54125 after it such as 123.123.123.33:54125. As an aside if your PIAF box does not have a fixed IP address, you can use a dyndns account with a Linux software program, DDclient which will periodically report its current number to your account at dyndns.org so you can get to it via the web by just using its dyndns.org name.

Next click on the Webmin Users menu item to your left and create a new user johnsmith1, for example. Give johnsmith1 all rights, save and log out. Log back in as johnsmith1 and make sure that you can move around the Webmin system without any problems. Go back to the Webmin Users section and delete the root account. Hackers, who almost always try to use the root account to access Linux machines but will be blocked in accessing the Webmin's root account as it will not exist in Webmin. This root account is separate from the console root account. You can also force only SSL connections so you'll need to add an s to http:// to see the Webmin screen.

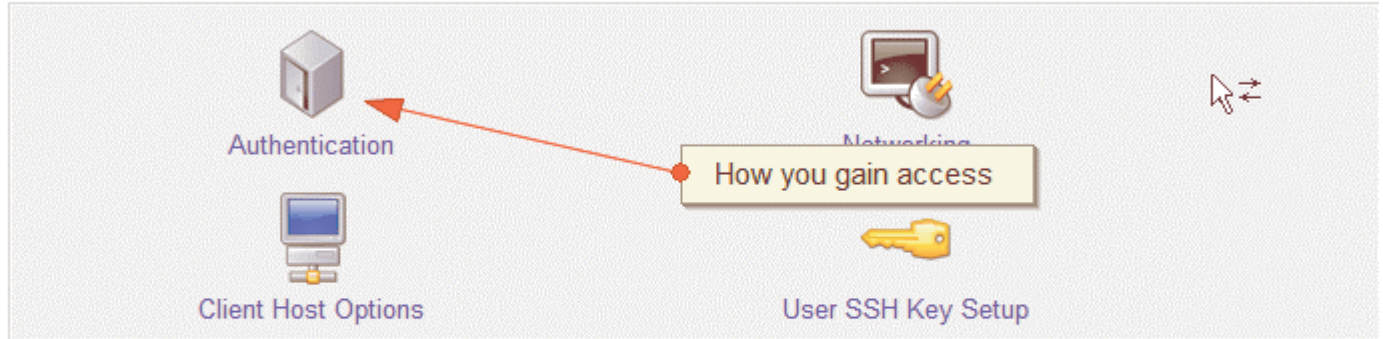
Finally, if you're feeling particularly paranoid, the section also allows you to create a security certificate which may be downloaded to your browser. You can back this browser certificate up as it's just a file and transfer it to other browsers. Without the certificate you cannot access Webmin. I have found that Webmin certificates can cause problems, especially with Java applications though so I don't use it. Your mileage may vary.

How to Secure Your PBX in a Flash System

SSH

[Help..](#)
[Module Config](#)

SSH Server
OpenSSH_4.3



[Apply Changes](#)

Click this button to apply the current configuration by sending a SIGHUP signal.

[Stop Server](#)

Click this button to stop the running SSH server. Once it is stopped, no users can connect.

Now that Webmin is hardened, let's look at SSH, THE way that hackers get root access using brute force attacks. Their computers connect to the PIAF and guess the root passwords, possibly thousands of times a minute until they guess it and log in. You can stop this with Fail2ban.

The quickest way to protect against attacks permanently (yes, the 4 attacks a day I get are from different hackers) is to use Fail2ban, a very nice tool which counts failed logins and subsequently bans access for 30 minutes and up to 99 years. I like 99 years. I'll get to Fail2ban in a minute as it doesn't have a nice point-and-click interface and you should be clicking at the moment.

Let's look at root access for a moment in the SSH module. If you click on SSH Server and then Authentication you'll see that you can set the Allow login by Root to No, Yes and use RSA, and Only for Commands which we'll ignore in this HowTo. If you select No then root access is disabled. You just save the page and then click Apply from the former page.

The problem is that once you've done this you can't get access via root in a shell either. You can avoid this problem, which involves logging into Webmin's SSH module again, allowing root access for a moment and applying the change, logging in via Putty or another SSH program, closing root access, etc. and so on by setting up a strongly encrypted certificate, illustrated below.

While the no root access, period is the strongest method of stopping attacks, especially using Fail2ban a certificate approach is almost as good and in reality, as good, although more complex to setup. But more on certificates later.

How to Secure Your PBX in a Flash System

[Module Index](#)
[Help..](#)

Authentication

Login and authentication options		
Allow authentication by password?	<input type="radio"/> Yes <input checked="" type="radio"/> No	Permit logins with empty passwords?
Allow login by root?	Only with RSA auth	Allow RSA (SSH 1) authentication?
Allow DSA (SSH 2) authentication?	<input checked="" type="radio"/> Yes <input type="radio"/> No	Check permissions on key files?
Display <code>/etc/motd</code> at login?	<input checked="" type="radio"/> Yes <input type="radio"/> No	Ignore users' <code>known_hosts</code> files?
Pre-login message file	<input type="radio"/> None <input checked="" type="radio"/> <input type="text" value="/root/hacker.txt"/>	
User authorized keys file	<input checked="" type="radio"/> Default (<code>~/.ssh/authorized_keys</code>) <input type="radio"/> <input type="text"/>	
Ignore <code>.rhosts</code> files?	<input checked="" type="radio"/> Yes <input type="radio"/> No	

[Return to module index](#)

Now, we can harden web access to the many web screens used to configure PIAF, access voice mail and generally browse around the PBX from the outside world. This can be simply done in the Apache Server interface using Webmin.



The quickest way to do this is to click on Edit Conf Files and change the "Allow from" line using IP addresses and/or domain names of machines allowed to contact it -

```
# Controls who can get stuff from this server.
```

```
#
```

```
Order allow,deny
```

```
Allow from mypc.dyndns.com 222.225.22.222 mylaptop.dyndns.com 192.168.0.15
```

Save and apply and only those IPs can get to the PIAF screens.

Let's uninstall Samba. Samba is a package that allows SMB access to your PIAF server. In

How to Secure Your PBX in a Flash System

other words you can create Windows shares and access them from your PC. The problem is that so can a hacker, and if your PIAF is directly on the Internet (not behind a hardware firewall) it is not difficult to find those shares and attack them.

The quickest way to uninstall Samba is to use Webmin's uninstall utility. Navigate to System, and then Software Packages. Search for Samba and uninstall. At the very least, if you don't want to uninstall it, just stop it from running. Use System; Bootup and Shutdown. Just stop the SMB service and disable the automatic restarting at boot.

Let's go back to Fail2ban. If you use File Manager under the Others section, you'll be able to navigate your PIAF server and edit certain files. If you have the latest version of Fail2ban, navigate to the /etc/fail2ban folder and edit the jail.conf text file. There are lots of notes, so I won't detail each feature, but I set the nominal 30 minute bantime = to -1 which means longer than any of us will be alive. I then add the never ban IP addresses as either IP numbers or dyndns.org domain names as I've illustrated before so if you screw up, you won't ever be banned and have to manually unban yourself from the console or via Webmin.

When hacked, the Fail2ban log file adds the IP address and that address is banned. It's in the permanent /var/log/fail2ban.log file.

Here are some real examples -

```
2009-01-30 13:17:00,488 fail2ban.actions: WARNING [ssh-iptables] Ban 99.171.68.11
2009-01-30 13:17:40,779 fail2ban.actions: WARNING [ssh-iptables] 99.171.68.11 already
banned
2009-01-30 16:04:55,551 fail2ban.actions: WARNING [ssh-iptables] Ban 202.6.107.195
2009-01-30 16:51:38,558 fail2ban.actions: WARNING [ssh-iptables] Ban 122.41.175.118
2009-01-31 00:29:52,648 fail2ban.actions: WARNING [ssh-iptables] 202.6.107.195 already
banned
2009-01-31 09:25:15,646 fail2ban.actions: WARNING [ssh-iptables] Ban 41.204.92.94
2009-01-31 11:48:42,087 fail2ban.actions: WARNING [ssh-iptables] Ban 66.238.27.105
2009-01-31 11:49:22,566 fail2ban.actions: WARNING [ssh-iptables] 66.238.27.105 already
banned
```

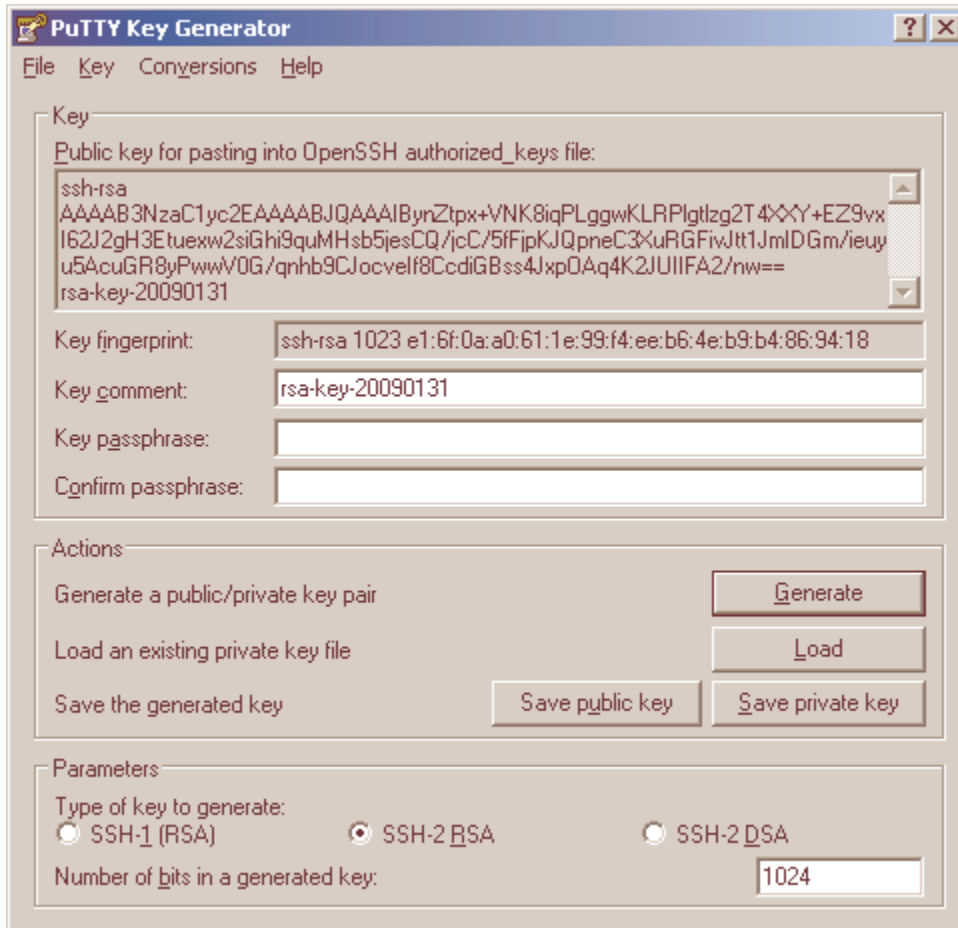
Now back to creating and using certificates. In this instance I'll use puTTY a common free secure shell program. I'll illustrate using the latest build, released on January 30, 2009.

First download the following program here -

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>. Under the heading - The latest development snapshot download "Windows installer for everything except PuTTYtel" and install on your Windows PC.

After the install, click on PuTTY Key Generator, then generate a key as in the example -

How to Secure Your PBX in a Flash System



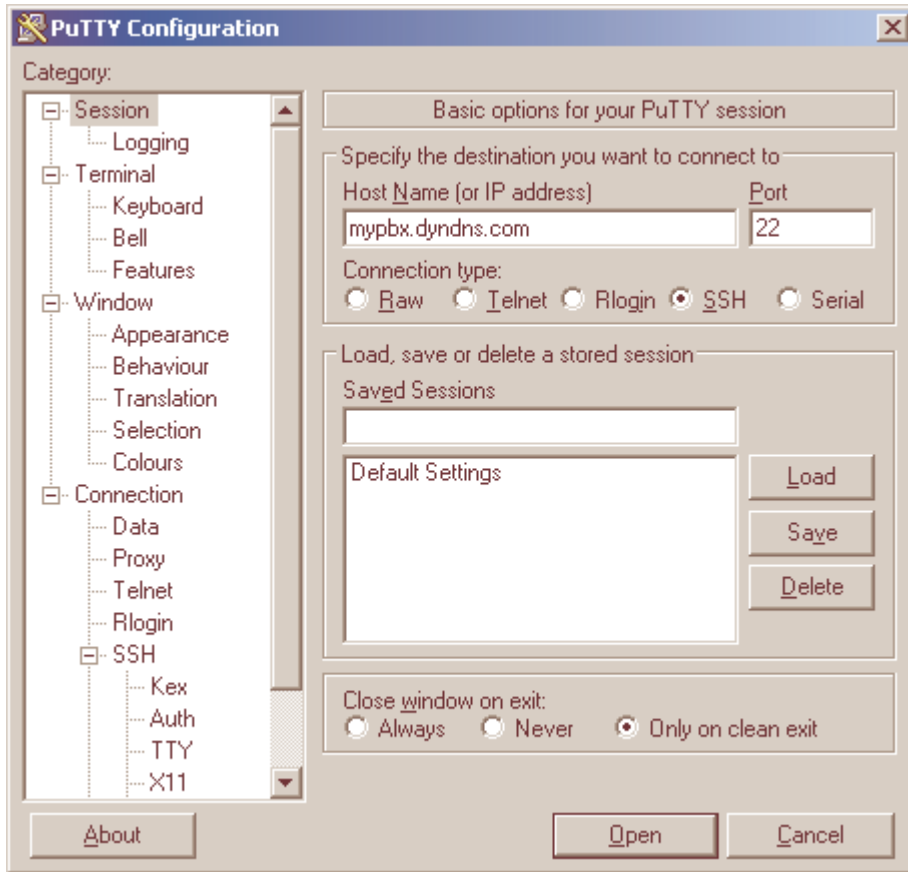
Save the private key, with a PPK extension in your My Documents folder with a name like PIAF.ppk or whatever name you want. Ignore the password request. Then copy and paste the Public key contents to a text file for manual insertion on your PIAF server using Webmin File Manager to access the corresponding text file that's used to compare your key with its. Here is the public key example in its entirety. Its like an extremely long password -

```
ssh-rsa
AAAB3NzaC1yc2EAAAABJQAAAIBynZtpx+VNK8iqPLggwKLRPlgtlg2T4XXY+EZ9vxI62J2gH3E
tuexw2siGhi9quMHsb5jesCQ/jcC/5fFjpKJQpneC3XuRGFivJtt1JmIDGm/ieuyu5AcuGR8yPwwV
0G/qnhb9CJocveIf8CcdiGBss4JxpOAq4K2JUIFA2/nw== rsa-key-20090131
```

Run Webmin again and navigate to the /etc/ssh folder. Open the authorized_keys text file (or create the text file) using the edit button and paste the entire key into it and save. The idea is that the key on the PIAF server is linked to the private key that you'll use in puTTY to authenticate with. Now open puTTY and do the following -

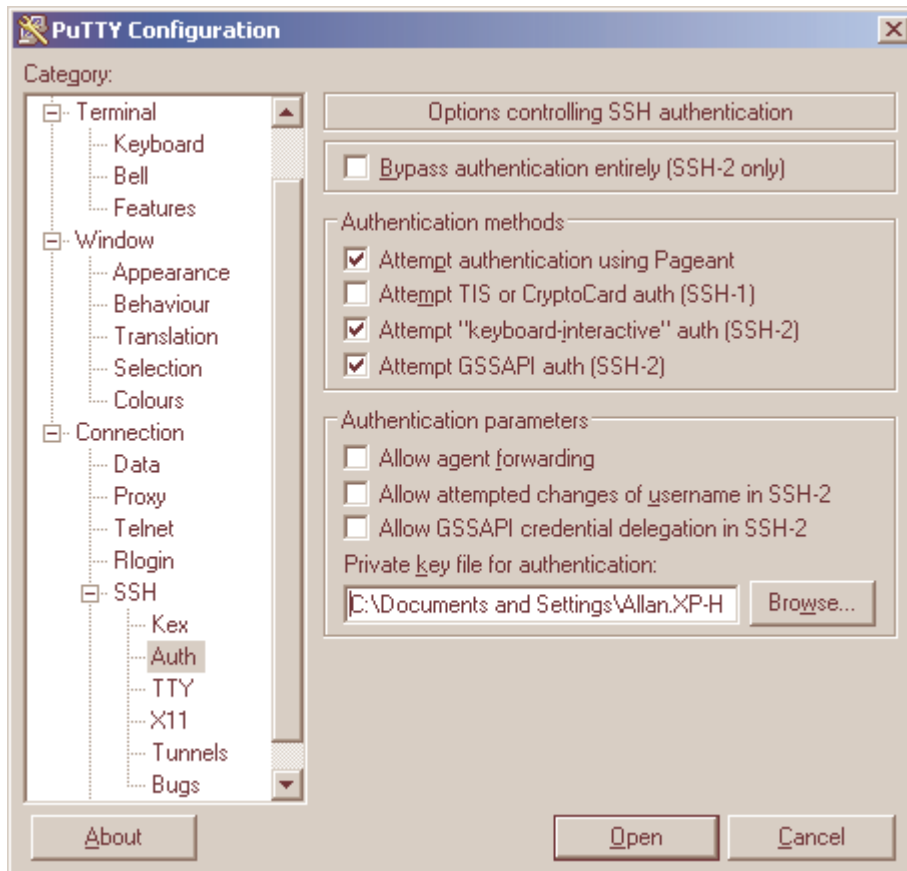
Type your PIAF IP address or it's dyndns.com domain name into the box as shown

How to Secure Your PBX in a Flash System



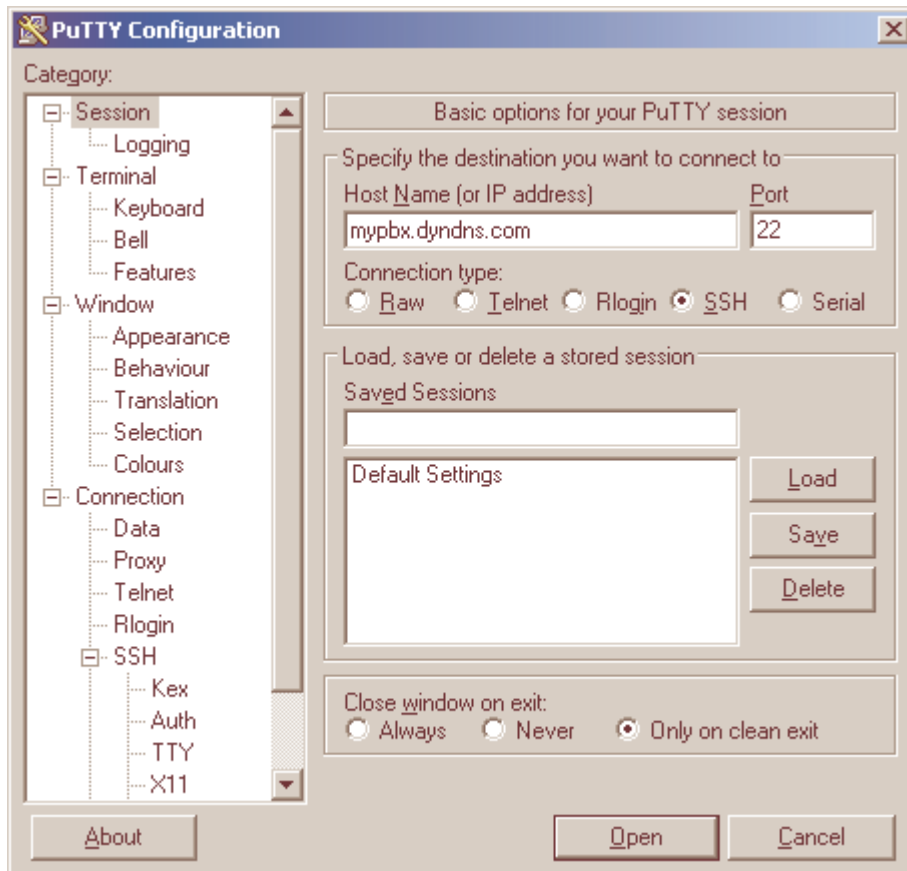
Then go the SSH, Auth and follow the illustration - browse to the PIAF.ppk (or whatever name you used) in your My Documents folder.

How to Secure Your PBX in a Flash System



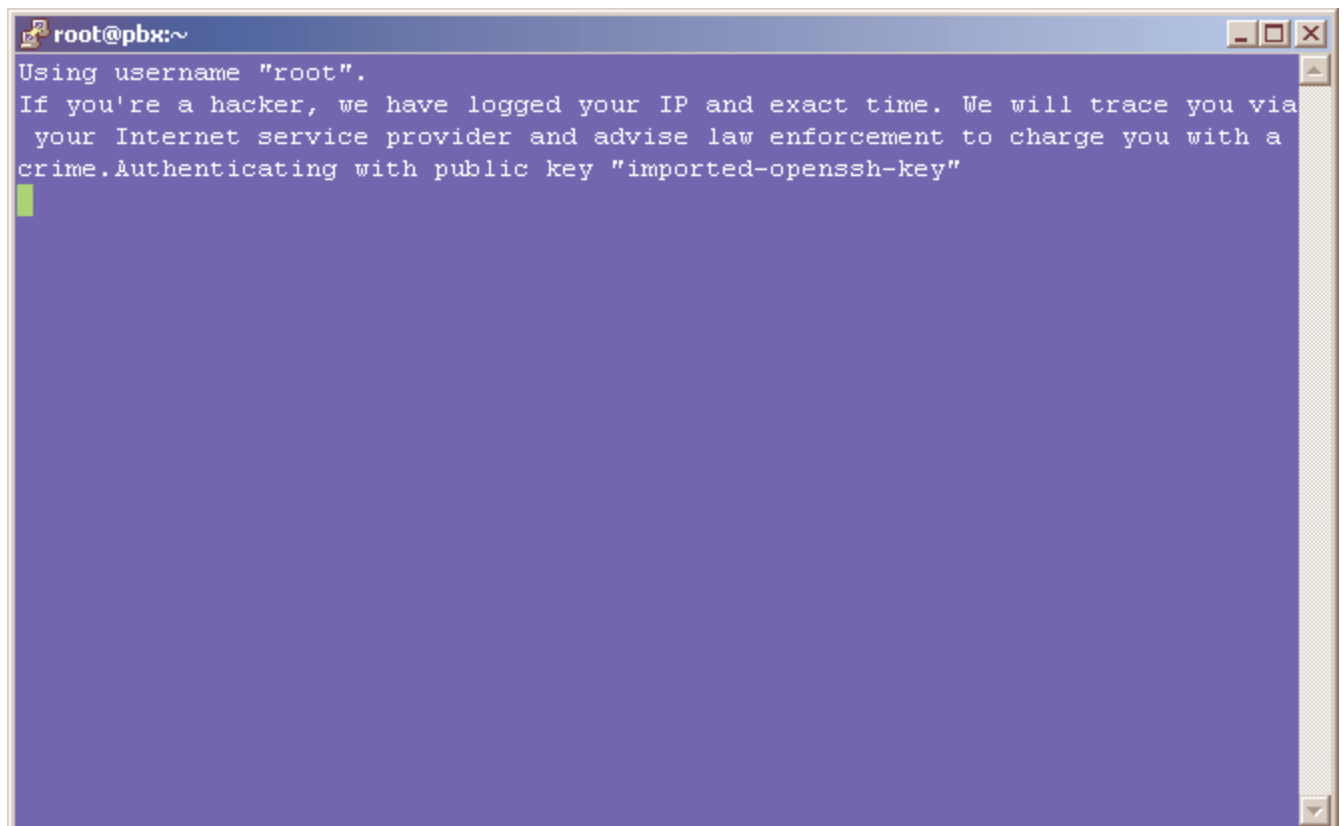
And finally, click on the Connection, Data section and enter root in the Auto-login username section. Now click on the top Session button and type in mypbx.dyndns.com name in the Saved Sessions box and Save.

How to Secure Your PBX in a Flash System



If you're really lucky this will work the first time; just clicking Open will open a session and automatically log you in. Note the scare message for good measure. Good luck.

How to Secure Your PBX in a Flash System

A terminal window with a blue background and white text. The window title is "root@pbx:~". The text inside the terminal reads: "Using username 'root'.", "If you're a hacker, we have logged your IP and exact time. We will trace you via your Internet service provider and advise law enforcement to charge you with a crime.", and "Authenticating with public key 'imported-openssh-key'". A green cursor is visible on the line following the last message.

```
root@pbx:~  
Using username "root".  
If you're a hacker, we have logged your IP and exact time. We will trace you via  
your Internet service provider and advise law enforcement to charge you with a  
crime. Authenticating with public key "imported-openssh-key"
```