Hotline Admin Access

Jambo regurgitates a bunch of stuff that other people wro...
sorry, that should read 'Jambo shows you how to get admin access to a Hotline server'. (Phew!)

First of all, I'd like to say that nothing in this file is original - It's all been done before (plagiorism? Moi?). The reason I did this was to put together an easy-to-read guide that gives you (hopefully) all the information you need in one place. Now, on with the show...

Anonymity

Before you start raking through a server's HD, downloading files right, left and centre, you should make sure that the attack is not traced back to you. The best way to do this is through a wingate, using the famous bounce-attack. First things first, I suggest you get a good port scanner. The two best bets are AGNetTools, or IPorts (included with this issue). Now you want to do a Service scan over a range of IP addresses for port 1080. Once you have a working firewall, enter it into the 'SOCKS firewall' option in your Hotline client. Voila! Now the Wingate's IP will be logged instead of yours! Of course, working from a different IP is all very well but if you use your regular nick and icon, you will probably still be caught, so my advice is to also change your nickname and icon in the options menu.

Reconnaissance

At this point, you should try to find out a little more about the server you wish to attack. If it's a fairly big server, I suggest you idle on it and note how many admins there are, how frequently they enter the server, and how clued-up about Hotline security they are (this last one may prove a tad tricky to find out - just put on your smoothest public chat voice and hope they are in a sociable mood)

The next thing you should find out, and this is very important, is what machine they are running the server on. The tricks I am about to describe to you will only work on specific platforms.

The Attack
•Mac HL servers

There are a couple of decent ways to get admin access to a server. The first, but most likely to blow up in your face, is the trojan. I'm sure you've heard of it, it's the 'program within a program' that comes disguised as something else (on hotline this often means an account request). Hotline trojans have traditionally done one of two things: Either it will make a superuser account in your HL server's 'Users' folder (example - 'Pamela Slides'), or it will make an alias to your HD and put it in the files folder (example - PimpBot). The more sophisticated trojans make use of both these techniques (example - Fuct Kiwi's excellent sea trojan). To save space, I have not included any of these trojans here - see the links page for information on where to obtain them.

Now, a meatier trick. This one has actually been reported in Happle before (Happle #04, 'Hacking Hotline' by Sir Talonz) however my man Talonz forgot to mention one thing - you need to upload the alias with a PC. In case you didn't read that issue, here it is again:

1)

Find a Mac with System 7.1 or earlier
2)
Rename the computer's Hard Disk to whatever the server's HD is called
6)
Sorry, maths was never my strong point...
3)
Make an alias to the Hard Disk, put it on a floppy, then lock it
4)
Now you have to get a PC with a hotline client (you could also probably do this from a Unix box but not from a remote shell, as in order to upload from the shell to the server, you would have to have uploaded the alias to your shell. The mac automatically resolves aliases so you cannot upload them from the MacOS. Make sense of that :P)
5)
Put the disk in the PC and upload the alias from the hotline client.

Of course, you probably spotted there are a few problems with this technique. First of all, you need to know the name of the victim's Hard Disk (or be extremely good at guessing). Secondly, it has some pretty steep hardware requirements - A mac with system 7.1 or earlier and a PC with hotline.

•Win32/HX servers

This bug just surfaced the week before we went to press (not that we need a printing press, but it sounds cool) so there is a good chance that if you get in quickly, you will find some servers still using HX or HL server B7 for the PC. Please note that fixes for both platforms have since been made available and if you run a server on a PC or through HX, go to the links at the back of the zine to find out where to get a patch.

Now, rather than babble on in my idiotic way, I'm sure you'll be glad to hear that the fine folks at The Hotline Conspiracy (http://www.hotlineswsucks.com) have allowed me to reprint their advisory.

[You can read the original advisory at
http://www.hotlineswsucks.com/security/serv01.shtml]

"/.." Server Security Hole

The Win32 Hotline Server, produced by Hotline Communications, Ltd. and hxd have a security hole which allows anyone with access to hx or MacsBug to gain entry to the entire server hard drive. The glitch is merely a matter of taking advantage of the file systems directory structure, and accessing "/..", which leads to a higher directory.

THC was able to gain access to several servers, and on those which had download privileges enabled for guests we were able to download user data files, Hotline bookmarks and various other files which some would consider to contain sensitive information. If you feel your server is at risk with this security hole we recommend you move your server to a MacOS alternative immediately.

HX

With hx, the intruder need only to change the directory character to something besides "/". The command to change it to ":" is:

```
/dirchar :
```

After that, simply changeing directories to "/.." over and over will let them reach higher levels of the directory tree. ie -

```
/cd "/.."
```

Note: THC was only able to complete the hack with hx 0.7.9. The only other version which we have access to (0.5.28) does not have the dirchar command.

MacsBug

With MacsBug, the intruder will have to open a folder, then search for that name in memory, then modify it.

The search command is:

```
f address numberOfBytes 'text'
```

Where "address" is the address displayed by the "hz" command, and "numberOfBytes" is just a large number (like a couple of megabytes).

When it finds it, it displays what it found and the address. The intruder can then change it using "sb".

Obviously the intruder will need to change the name to "/..", but they also need to set the byte immediately preceding to 3.

Fix:

Win32 - Upgrade to b8 or higher.

hxd - http://krazynet.com/hx/

See that URL up there? Go to it! The Hotline Conspiracy were kind enough to let me reprint their work, so *please* justify their generosity by checking them out.

If there are any mistakes, or problems with this file please mail me at Jambo@Yewclark.demon.co.uk