POPing for whores

I haven't seen a howto qpop or shit like that, so I've decided to tell you whores the do's, the don'ts and the "wtf do i do now?"'s.

So it begins.....

The first thing you need is a scanner (and a linux shell to exploit the server from), so we go shopping at your favourite sploit place and pick one up. I recommend bpscan for macOS and sscan (mscan's son, a lot easier to setup as well, though the logging leaves much to be desired) for linux. The good thing about these scanners are that they are easy to setup and do the job (bpscan, mscan and sscan are all available from Happle's hotline server).

Now you need some IP's to scan, bpscan can be configured to take IP's from a file like sscan does, bpscan also can do a whole domain or 50 ie. 195.45.65.1<>195.45.200.1 which will scan 195.45.65.1 to 195.45.200.1. If you have access to a linux box you can use "host -l <domain>" to
gather IP's from a whole country, sort them out using gawk (text accessory for linux) so there are only IP's or only hostnames on one line each. Now you can download this and scan from your mac (i've noticed that bpscan freezes if you use a large IP file, maybe this is fixed in bpscan2.1r1) or scan from your linux box.

You've been scanning for a while, jump up and down in excitement when your scan has finished and decide to look at your logs. First we'll look at bpscan. What i like about bpscan's logs is that it tells your that this IP is exploitble, however it only tells you that the IP is exploitable if it has qpop 2.2 or 2.41beta1, not 2.2-b5 or 2.4 (as they are also exploitable using the qpop exploit), so you can lose roots :/ . Now sscan (or mscan, as they both do the same type of logging), it connects to a server and logs the data that comes from the connection, so you have to spend your time going through it and pulling out the qpop exploitable's and deleting the others ie.pop3, zpop (or ofcourse you could use gawk and get it done in a couple of seconds ;P). This is what a qpopable server will look like in your logs: +OK QPOP (version 2.2) at x starting. Where x can be anything ;). As far to my knowlage these are the exploitable qpop versions for linux servers: 2.2-b5, 2.4, 2.2, 2.41beta1. Unless you find a BSD server running qpop than the exploitable qpop versions are 2.3 and 2.5, you'll need a different qpop exploit to exploit it, as it is

based for BSD not linux.

Now we come to the fun part, hacking the bitch. This is how an exploitable server will/should react to the qpop exploit. You do: qpop <ip> . Then wait for it to connect and do it's work, usually (if not everytime) if it works, it will give you some garbage characters, about a line or two, sometimes it may take a while to give you those characters. You may come across a server or two that don't look like they work (don't give you characters), the way to see if they have worked is do a *nix command ie.ls , if it works that means the server is exploitable, if it doesn't work, that means well.... it doesn't work :P.

Once you're in you want to cover your tracks up, if you don't some servers will send your ISP a nice little letter with their logs of you exploiting them, then you get your ass removed from your ISP/get cops knocking at your door. The way to cover your tracks when you have just qpop'ed a host is by typing:

killall -9 syslogd ; rm -f /var/log/mail* ; rm -f /var/log/news* ; rm -f /var/log/messages

This removes the system log, the pop log (mail) and the news (just for a bit more protection), some servers run klogd, so kill that aswell. Also for all you daft people, don't remove the mail if you use a different exploit, that command line contents is just for the qpop exploit, you have to remove other logs if you use a different exploit.

That's about it on that front. My advice is don't add new users, that's like
waving a fluro green flag saying "YOUR SERVER IS HAX0RED BITCH!", just add a nice udp backdoor, if you can chuck it on the boot so when the server reboots the backdoor will be operational. Some nice backdoors are b4b0's, they're purdy cool ;) Until next time, unf.

Ferrocyanide

"I am a computer. I am dumber than any human and smarter than any administrator."