Friday, July 29. 2011

550 Access Denied

The biggest problems with getting your Email to someone is getting through the receiving ends mail servers defences.

Sadly, long gone are the days of the early 90's where spam was really only something that was heard of in a supermarket, although it had been around for years, even on ARPANET, it was not of plague proportions like it reached in the mid-late 90's through to the problem it is today. Long gone also are the days where you can trust strangers to use your mail server, where it was common two decades ago for most mail servers to be open relays, but, as with anything that's available, it soon became abused, so to combat the problem of spammers abusing this privilege, MTA's like Sendmail soon released versions that no more by default permitted open relaying capabilities, like the 'ol saying... if you abuse it, you loose it!

Defence comes in many forms, most common is the well known method of DNSBL's (DNS based Real-time Block Lists), often also referred to as RBL's, PBL's, Blacklists, or even Blackhole Lists, these are DNS based lists of domain names and IP numbers of trouble makers, people who have given others grief in some form or another (spam, phishing, compromised, abuse, etc...), they become submitted to these lists by trusted persons, also through automated processes, including hidden addresses to trap spambots when they harvest websites looking for addresses to add to their spam-out lists.

Today there are more than 30 such public lists, each with their own listing criteria, however, there are only a handful of what are considered reputable lists that the vast majority of administrators use, not to mention many private lists (like the one we run), and in-house DNSBL's used amongst a group of ISP's, occasionally even sharing data between them. You can test a blacklist entry here

But DNSBL's are just one obstacle, before you get that far, you often go through several other checks like local access lists, hostname and DNS compliance testing, and so on, this is where greater than 90% of the rubbish is filtered out.

One of the best ways to help get your mail received is to ensure your DNS is properly configured. In your domains DNS zone file you should have an A record entry, and in your in-addr.arpa or ip6.arpa zone files for your IP allocations, a matching (rDNS) PTR record entry - for every machine, and in particular, for every server. RFC 1912, Section 2.1, para 1 and 2 clearly states "Every Internet-reachable host should have a name" and "Make sure your PTR and A records match" and "For every IP address, there should be a matching PTR record".

With IPv6 starting to get off the ground, it is going to be far more of an issue given that most people will end up with so many addresses. So it will be more important than ever to set correct DNS for your IPv6 and IPv4 addresses for any server that should be sending mail, be it a mail server, or a web server that might for example, run a forum or blog, and needs to send mail for confirmations, updates, password resets etc.

Another well used trick involves rejecting dynamic users, these are connections that have good forward and reverse DNS, but include things like a dotted or dashed version of their IP number, ppp, dial, xdsl, pool, cpe-, ip- , dyn, cable, and res, to name only some, in their hostname, this normally indicates a residential host, with likely no dedicated mail server or a genuine need to be directly sending mail. So in selecting a service, ensure your rDNS can be changed to a suitable name, if not, find a provider that does offer it, even if only by request to support. The recipients ISP's wont tolerate constant whitelist me please requests because you or your network provider can't get their act together, remember it's you/your host that are non compliant. So, in your naming conventions, don't use the IP number or parts of it in your DNS/rDNS entry for servers, but it is of course fine to do so for general PC's, laptops and mobiles that should have no reason to directly send Email to anyone, and make sure that your server hostname settings match, if they present a HELO/EHLO with rubbish, you can be sure you'll get blocked for that as well. Make life easy, give your servers a server-like name, eg: falcon.your.domain, and configure it and DNS for that name only, if you run a dedicated mail server, call it mail.your.domain, or some othername that resembles a servername, and ensure your DNS zone has that name listed in the MX record field.

If running a mail server, and you block a host because of policy, ie: access lists, milters, RBL's, etc, you must do this at the initial smtp connection, where your server can reject the message with a 55x error code so the sender knows they have been blocked, and why, the only time you are not required to do this, is if using an anti-spam set like spamassassin

and you silently drop high scored spam messages, low/medium scored should still be delivered, most anti spam mail server software has the ability to send a warning message and attach the original spammy message to it, I personally use a cutoff of around 15, that's high scored and silently discarded anything less and amavisd will warn the recipient and include the spam as an attachment, please do not ever use software that bounces spam or notifies the sender of the spam message, if you have accepted the message, you must either deliver it, or discard it, never bounce it (chances are the addresses will be forged anyway).

Speaking of forgeries, I also suggest you use SPF, you should not only publish your SPF record for your domain (and any domains you host), but enforce SPF checks on your mail servers too. There would be so much less phishing attacks, especially for financially related incidents, if only those organisations would use SPF.

When implementing SPF, I recommend testing thoroughly first by publishing a softfail condition, and once you're sure it works right, change your DNS SPF resource record (RR) to a hardfail, that's from ~all to -all. The modern way of using SPF in DNS is with the Type SPF, but, because there are a lot of lazy admins out there who have not updated their daemons or scripts, you should also publish your SPF data in the deprecated TXT method as well for the time being. In its simplest form, all you need is the IP address numbers of the servers you want to allow to send mail on your domains behalf, for instance this domain, ausics.net has the following SPF and TXT records:

v=spf1 ip4:27.33.160.23 ip4:62.113.243.167 ip6:2a00:f48:1029::1:a05d:e257 ip6:2001:470:67:524::0/64 -all"

This means only those addresses can send mail for any email address at ausics.net (based on envelope sender) (I do not recommend using name types or mx's, use IP address or ranges only, SPF is of course very powerful and can be extended to include other zones, and even use regex's, if you're new to this, stick to the basics only, don't over complicate things.) You must always remember, like everything DNS, you need to keep things up to date at all times, so if you change mail server IP's change your SPF too!

Another advantage of publishing SPF records is if sending to Live.com (Hotmail), or Gmail, under their scoring systems, you get a higher rating, meaning greater probability of inbox delivery.

Some people are anti-SPF claiming it messes up your mailing list posts, I've published SPF records for a great many years now, and have never seen any collateral damage like this, most modern list servers re-write the envelope sender address, so although a mailing list post might reflect From deletethis@ausics.net, the envelope sender which SPF uses, will be different, it will be from the domain of the sending list server, eg: cisco-nsp-bounces@puck.nether.net, so SPF receivers, would be testing if puck.nether.net is allowed to send for cisco-nsp-bounces@puck.nether.net, and not testing for deletethis@ausics.net. You can learn more about SPF at openspf.net.

The most popular used anti spam program, SpamAssassin, is used on a very large number of servers and proprietary hardware devices, it looks for keywords and styles and is based on a score system, so don't send Emails that are obviously spammy and it wont positive score you, SpamAssassin, like everything else, is not foolproof, nothing is, and anyone trying to convince you their solution is, is full of crap, but SpamAssassin works, and works really well. Some sites rely on outsourced services (or rules), meaning they pay a ridiculous amount of money for some re-badged server from one of the mobs selling these hardware devices and relying on their rules, their decisions, and don't custom configure the devices at all. I've seen and heard countless admins cursing those things, but, you got to expect that if you're prepared to let someone else decide what your network gets. Personally, I don't believe in those things, if I'm providing a mail service, that's for me and my colleagues to decide.

Note: SpamAssassin has an internal whitelist when it comes to URIBL's (which check links inside emails), some domains on that list should never be there, like mail.ru, and a few more, so I highly recommend adding into your local.cf the keyword option: clear_uridnsbl_skip_domain

If you run a mailing list, ensure it is configured to double opt in, and don't blindly add any addresses to it under any circumstances. Configure the list to suspend delivery of mail after a very small number of bounces - Mailman and Ecartis are able to do this, and, although its been many years since I looked at it, I think ezmlm also. Make sure only subscribed members can post to your lists, moderate new members for the first few messages if at all possible, spammers love to abuse mailing lists too. Having someone on a list that doesn't want to be, is the worst thing you can do, so make sure your list server works properly for those wishing to unsubscribe, and make sure it works by email as well as any web interface, nothing worse than having to use a web login to remove ones self from a mailing list. Failing to adhere to most of these things is another great way to be placed on a blocklist.

IP numbers are finite, yes, they get re-used, and it is possible the ranges allocated to you were previously used by low

life scum who spammed and the range was listed in one or more blacklists, you will have problems convincing blacklist maintainers removing that listing, ensure all PC's with access to your LAN are virus scanned and kept patched, this is especially so for Windows users. Research your service provider well, and if you're on ISDN/xDSL/Cable etc, perhaps explain to your ISP your dilemma and ask them to change your IP range, hopefully you do this when you first get your connection up and running before you migrate and go live on your new connection.

There are some whitelists around for SpamAssassin and hardware devices using nice-lists and reputation, there are some money grabbing bastards who operate some block/reputation lists, that when you are blocked via their lists, the reject message is telling you to go to some web site and pay to be whitelisted/get a good reputation - WTF? Seriously people, save your money - Trust can only be earned, not bought! I also work under the assumption of my network, my rules.

With relation to grey-listings, don't bother, many spam bots are cluey enough to retry these days, all it serves today is to delay legitimate Email, something that could cost you or your employer in many ways. I'm also not a real fan of DKIM, since it can, and does break with mailing lists (often you'll see it with gmail users), and when you have many domains on one server it gets trickier.

One thing I need to make clear to you if you're new to setting up your own mail servers, do not ever allow it to accept messages for non existent users or blindly relay for others, backscatter is the fastest way for your mail server to get blacklisted. Ensure you only relay for your local IP ranges, better still, use the message submission port (SMTP Auth) (port 587) and only accept inbound mail on smtp (port 25) that's destined to your own network from external addresses, and block outgoing port 25 on your router (with the exception of your mail servers IP of course) if at all possible.

In conclusion, if you follow the above rules, the chances of your mail getting through to the recipient, will be pretty good, you'll have less rubbish yourself to deal with, and overall, also be a better netizen

Posted by NoelB at 19:47

Thursday, July 14. 2011

Phone Hacking - OH NO!!! No, your mobiles not actually hacked

So, in light of Murdoch's staffs criminal actions, the worlds media have been filling our airwaves with the term Phone Hacking, why, I'll never know, as it is really incorrect, no phones were actually hacked at all, no conversations were monitored in real time, no phones contacts list or stored emails or photos were ever compromised in this latest scandal.

What is actually occurring is illegal access to peoples voicemail boxes. Most of us, and yes, I bet *you*, are still using the default PIN number for voicemail. Now, most of the time we don't need to know it, since the phone networks know who we are and just give us access, but, you do know that you can access your mobiles voicemail from any phone, anywhere, at any time.

Usually when your voicemail is first activated you will or at least should be, asked for a PIN, if you did not get asked for whatever reason, your voicemail box will be using the default PIN, in 99% of the time, that is simply the last four digits of your mobile number

So, by knowing someones mobile phone number and the network they use, which wont take long to suss out either way since all networks publish voicemail access numbers for members to be able to remote retrieve their voicemail, someone can very easily illegally gain access to ones new and stored mobile messages. It is in some cases as easy as dialing your own mobile number, instead on leaving a message, hitting the star button gives you access, where you will be asked for your PIN.

The way that has been used in recent times with prominent people is, a partner of the offender will place a genuine call to the unsuspecting victim, whilst the other partner goes about accessing their voicemails.

It is imperative that everyone who is not sure, goes to their phone providers website and find the voicemail FAQ, and sets up a personal PIN, in most cases this is done via dialing your voicemail number (321) and going into setup and finding the option to setup or change your PIN.

So, although the media have got it named all wrong, the hype about its risk and dangers is very very real, and should be taken seriously by every mobile user in the world.

Now you've finished reading this and should have a better understanding of the dangers, you are now about to hop off changing your PIN, right?

Posted by NoelB at 10:22

Friday, July 1. 2011

Data Centre Cooling

For decades most Data Centre's utilised raised floors to inject cool air from underneath up to the racks in a back to back arrangement, this is called the Hot aisle Cold aisle method, but for some years now this method is considered outdated and rather inefficient for Data Centre cooling.

inefficient hot aisle - cold aisle approach

This method, as seen at left, involves hot air from hardware released from the rear door of a rack into the general Data Centre airspace, to assist with some form of hot air containment, most rows of racks will be so two rows are back to back, but, this still allows for hot air mixing with cold air as they are not truly contained for exhaust.

Many modern Data Centre builders have got it right in what makes far more sense using the all Cold aisle method, which involves an overhead plenum for the hot air to be expelled into, this means only cold air in your DC, and no mixing of cold and hot air, since the idea is to keep everything cool so your valuable hardware stays at a safe operating temperate.

The cold only method works by, as mentioned above, using an overhead return plenum to capture the hot air, and in most buildings this is already in place by means of false ceilings which can easily be sealed and used for this purpose. The racks will often have a low current fan that pulls the hot air out into the plenum by way of a type of boot, think of it as like a house chimney expelling smoke into the outside air, rather than filling up your lounge room. The cold air can be pumped in from overhead or the side so your racks can sit on that nice firm slab of concrete, and in this day and age with the world experiencing a horrific number of earthquakes, it also just might save your bacon if you are in a quake zone.

efficient all cold aisles approach

The method works best by using a grated front cage door on the racks to allow the cold air in, with the two sides and rear door fully sealed so the rear hot air rises to be expelled into the plenum. It's also more efficient if all blank RU's have blank panels attached to trap that hot air in the rear, back in 2007, I even saw pictures of some rack RU's covered and taped over with plastic, some racks even with cardboard... well... so long as it does the job I suppose

This approach has the benefit of keeping your entire Data Centre cooler, and given the CRAC units have an intake inside the plenum, they have less work to do, anything that needs to cool 27/28c into 22c must be better than something that needs to cool mid-high 30's and in Brisbane, that's more summer days than not, even days around 40, which, although not having the same humidity level, even Sydney can see a good number of days up that high. This makes your DC cooler, Greener since you'll have less of a carbon footprint, and more cost efficient.

It is also important I think to have a fresh air intake to your CRAC's for OH&S, some DC's in the U.S I've heard inject outside air for five minutes every 30 minutes, sure, that kind of contradicts the above advantage injecting some hot air, but overall it's cooler temps to be cooled and the idea of this is after all to keep the DC cool, the other is just beneficial side affects.

Sidenote
The entire idea of this is hot air containment, so if you only have a small room, with a few racks in it and use in-row CRAC units, you can take a similar approach, using sealed rack sides, sealed spare RU's and front grated doors, but with rear grated doors to expel the hot air into the small area behind, sealing above and the sides of your row of racks (even cheap perspex will do the job) forcing all hot air into that small isolated area at the rear of the racks where your in-row CRAC unit has its inlet, or, by still using duct cut outs into the plenum to allow the hot air to escape for a building CRAC, so long as that rear area is isolating the hot air from the server rooms cool air, the net effect is pretty much the same, and its much cheaper idea if you only have a few racks using in-row air cooling.

Posted by NoelB at 07:42