

SAGE Advice

The Newsletter of The System Administrators Guild of Australia

SAGE-AU'99



The Panel Session



Conference Dinner



Hard at work at the Conference



The Terminal Room

September 1999
Volume 5 Number 3

Table of Contents

Executive

- President's Report 2
- Secretary's Report 2
- General Information 3

Articles

- Tweaking Your Infrastructure 4
Andrew van der Stock
- Preparation is Better than Cure 6
Catherine Allen
- SAGE-AU'99 Tutorial Review 7
Geoffrey Day
- Book Review : Mastering
Regular Expressions 8
Karl Hanmore
- DEFCON 7 10
Brian Meilak
- Quick, Dirty and Useful Perl 12
Karl Hanmore

Regional Groups

- NSW Chapter report 14
- WA Chapter report 14
- Victorian Chapter report 14
- Regional group details 16

- Items for sale 9
- Mailing lists 9
- SAGE-AU'99 Conference CDROM 11

Print Post Approved:
PP 310009/00100



Executive

President's Report

Welcome to my first SAGE-AU President's Report. I hope it meets with your approval and that I am able to fill the large shoes of all the previous SAGE-AU Presidents.

Most of my duties as President so far have been handing over my old role to both Anthony Vialle (elected as Secretary at the AGM) and to Leanne Monette, our Administration Manager. This thankfully is now done and I can begin to concentrate on "Presidential" things.

SAGE-AU is running along quite nicely and at over 500 members, we are most definitely not a small organisation anymore. With this growth comes some pain and some new challenges. The current National Executive (and Regional ones) are no longer able to cope on our own to provide the sole effort and work to keep SAGE-AU going, let alone moving forward. Hence, Leanne has been taking on more of the previously volunteer day-to-day work.

SAGE-AU's spirit is all about helping one another and we have reached the point where we need more input and more time and effort from members in order to achieve some of SAGE-AU's loftier goals.

We are now beginning to enter political spheres. It is best to be prepared for it rather than let government legislation affect us without our input.

To that end, we have established some channels of communication at the Annual Conference, which I might add was an outstanding success. Yet again, we have out done ourselves while still providing one of the cheapest and best computer conferences in Australia and the only one totally focused on System Administration issues.

My views for where SAGE-AU will be by the next conference are that we need to dramatically increase our membership. We need to clean up some of our own internal practices and revisit our "Code of Ethics" to ensure it has kept up-to date with our industry and practices. We need to start down the road towards a "Code of Practice" to provide some guidance to members and protection in terms of new legislation. Finally we need to invest some serious time and resources at both the industry and government levels to ensure that System Administrators in Australia are recognised and consulted on important issues that affect us.

I feel it is now time to not just ask, "What can SAGE-AU do for you?" (which has been and still is quite a lot ;-)) but "What can I do for SAGE-AU?" and thus improve your lot and that of your fellow System Administrators.

David Conran, President

Secretary's Report

Welcome to my first report as Secretary of SAGE-AU. Well, the shuffling of the deck chairs was completed at the AGM. David (El Presidente) Conran, Leanne Monette and myself are still trying to come to grips with the changeover of positions and the devolution of some Secretary duties to the Administrative Manager. Hopefully nothing will fall through the cracks over the next couple of months.

As the incoming Secretary I certainly have a tough act to follow as David has done a sterling job, efficiently managing his Secretary duties as well as getting a number of new member services off the ground during his tenure. I am sure he will help me provide a similar level of service to you all.

I have become Secretary at a time when our membership is reaching a level that we can start looking at more new services for members, and the committee will certainly be investigating what else SAGE-AU may be able to do for you.

It is certainly in the interests of all members for us to continue our exceptional growth as the more members we have, the more services that may become viable to provide. If you have any suggestions of other services you would like SAGE-AU to provide for members, let myself or one of the other committee members know about it. We will certainly investigate all reasonable suggestions.

I would also ask that you help us grow. If you know of anyone who works as a Systems Administrator but isn't a member, hassle them to join. If each of us found a person to join we would be over 1000 strong at a stroke.

By the time this newsletter reaches you, the committee will have held a face-to-face meeting to plan and prioritise our activities for the coming year. Whilst we will generate a number of ideas and a whole lot of work for the committee from this meeting, we will always be open to issues raised by members. So, if



Tweaking Your Infrastructure

by Andrew van der Stock (ajv@greebo.net)

This month, I'm going to talk about getting the most out of the hardware and software that your organisation has paid for. For those of you who don't use NT, you may find the first bit of my column useful. It contains a few suggestions for performance tweaking networks, and this stuff works regardless of platform.

Many of you will have noticed that Microsoft funded a Mindcraft white paper purporting that NT is considerably faster than Linux on the same hardware for file (2.5x) and web (3.7x) serving purposes. I'm not going to defend that white paper, as I feel that it is massively flawed.

However, I am going to point out that Mindcraft have not only done a favour to the Linux, Apache and Samba developer communities (by pointing out easily rectified flaws), they've done a massive favour to NT administrators as well. How? By documenting in the one place exactly what settings you need to tune NT for the fastest possible speed. This information is spread over TechNet and the resource kits, and to a certain extent third party publications like Windows NT Magazine.

Infrastructure First

The tweaks contained in the Mindcraft document will not help at all if you don't have the appropriate infrastructure to support your network. There's no point in getting an extra 5% from an individual server/client combo if your network or network services sucks. In many cases, paying attention to your network will get you more of a boost than any amount of performance tweaking on your servers.

First off, try to determine overall network utilisation, particularly in server segments. 0-10% is good, 10-30% is average, 30-72% requires some thought about partitioning traffic or switching, and over 72% requires help from a professional.

Fix the low-level problems first. Use a network sniffer to see if any of your subnets are suffering from excessive jabber and other technical faults. Don't daisy chain hubs. Don't exceed Ethernet cable distances (approximately 185 m for cat 5 10/100 cable). Try to avoid putting more than 24 nodes into the same collision domain if you are still using dumb hubs. Use good punchdown patch panels (like Krone) and shortish good quality patch leads.

Subnetting is the forgotten friend of network administrators. Don't be profligate with subnetting. Just because your switch vendor says that you can have a 65,000 node subnet by using switching doesn't mean

you should. A single subnet for this many nodes would have massive broadcast and multicast packet storms, regardless of whether a switch was used or not. At a site I have worked at, they went through the entire 10.0.0.0/8 network just because they had a System™. When they wanted to connect to the outside world, they suddenly found that Telstra had already used part of this address space, and that NAT would be necessary to connection to the Internet via the Telstra managed firewall, limiting their options. Be realistic about expectations for growth. If you're setting up an outlying office and it has 3 workstations, you don't need to give the outlying office a 65,000 node network (or three, as this site did; one network for the router, one network for the three workstations, and one network for the printer. They wasted approximately 196,600 IP addresses at each of their 54 regional offices). By being parsimonious with subnetting, you can really reduce traffic and make your network management that much easier. You might need a few more router interfaces, but routers are getting cheaper, particularly routers with multiple 10/100 Mb/s interfaces.

Check that you don't have excessive broadcasts. Configured properly, using NetBIOS over TCP/IP (which can be a little bit noisy when badly configured) no more than 5% of all packets will be broadcasts. More than 5%, you need to look at your WINS configuration. Don't have WINS and have more than one subnet? Shame on you! Make sure that you set the DHCP global scope to specify WINS node type 0x8, which is Hybrid. Hybrid almost completely avoids the broadcast overhead and is far preferable to M and P types. As a bonus, hybrid is almost always faster than no WINS at all.

If you are managing more than 3 nodes, you would be crazy not to use DHCP. It's easy to configure and with the MS DNS server, you have zero maintenance DNS reverse lookups. To make DHCP work on internetworks, you need RFC1542 compliant routers. For those of you with really big networks, DHCP prior to service pack 4 scaled to about 1200 DHCP scopes per DHCP server. SP4 fixed that. I would suggest that each physical site have two DHCP servers. Configure DHCP server A to look after 50% of the subnets, and reserve 75% of each subnet. Configure DHCP server B to look after the other 50% of the subnets, similarly reserving 75% of each subnet. Then configure DHCP for fault tolerance: on server A, configure 25% of the space from server B's subnets, and vice versa. This way, if one of the servers goes down (either for maintenance or for more sinister reasons), the few clients that need a new lease during that downtime can still be serviced. I find that 3 day leases are a good compromise for

most networks. 7 days or longer is too long - if you need to renumber your network, seven days wont cut the mustard, and 1 day or less will cause a massive DHCP packet barrage around 9 AM every morning. Service Pack 4's DHCP and WINS servers can cope much better than prior NT releases with these transient loads. Get there as soon as possible if you haven't already.

If you use Exchange, always make sure both your servers and your clients have properly configured DNS. Not having DNS will slow Exchange down, in many cases make it unusable - for example the X.400 connector over TCP/IP will often fail to work. Since Windows 2000's directory is based upon DDNS, you should consider some form of DNS server today if you don't already have DNS installed at your site.

Do a traceroute from a random sampling of clients, and try to ensure that there are no more than two router hops to servers used commonly by users. For example, if user000 through user999 at site A require access to server349, make sure that all clients can talk to the server through no more than two routers, and preferably just one or none. The latency should be no more than 15 ms to provide users with seemingly fast response to their actions, particularly if they use Active Desktop or IE 4.0 or later. The pipe to their servers should be faster than 2 Mb/s to ensure that they don't bitch and moan at the server being slow. If you can't provide this sort of speed locally, figure out some way to get a file synchroniser or backup program to look after a local file server for them.

100 Mb/s EtherNet can be a minefield. Check to see that you are actually seeing an improvement in performance using the "Auto" setting when using 100 Mb/s. I've seen servers set to 100 Mb/s Full Duplex crawl - 39 minutes to copy a 72 MB file instead of 15-20 seconds. I've found that by falling back to half-duplex, the speed is almost the same as full duplex - particularly with large packets. If neither duplex settings help, fall back to 10 Mb/s and again test for maximum speed when using half/full duplex. Ensure that all devices on a switch or hub have the same duplex setting.

Finally, it's important that servers are able to talk to each other via as big a pipe as you can afford. By doing careful analysis of your network, you'll quickly come to realise that a \$2000 8 port switch, or \$4000 24 port switch will massively boost inter-server bandwidth, reduce collisions and reduce router load. With Unix servers, unless they're heavily NFS cross-mounted, there's not much point to putting servers on a switch, but putting NT servers on a switch can really help. Some common BackOffice components and poorly designed COM/COM+ objects call the security provider all the time, meaning that a good percentage of your servers will be sending a constant stream of packets to your domain controllers.

Win32 programs, almost without exception, print to the GDI print model. The NT print processor then en-

sure that the printer driver is capable of delivering results close to the original intentions using the native PDL, and if not, it fakes it by rasterizing the necessary areas. If you have non-PostScript printers, you'd be surprised at the size of even modest business documents. PostScript is one of the highest forms of PDL, and thus has the smallest need to rasterize a GDI call. In the field, the difference can be quite staggering: a simple PowerPoint job will take 100 kb instead of 5 MB on a PCL printer. If you care about network bandwidth, do not buy non-PostScript printers. If you have printers that can do both PCL and PostScript, you can do your network a favour by choosing the PostScript version of the driver. Your users will get more options, all jobs will print quicker, and the network will not be bogged down so often. It's extremely worthwhile to place printers and the printer server on the same switch. This will do more for speeding your network up than almost every other trick here as printer traffic (which can get quite intense) will not traverse user segments, switches and routers.

Last printing tip: Don't use any form of AppleTalk print server. They all suck and they all at least double your network traffic. If you need Macs to print, buy EtherTalk capable printers, such as the HP 4000N, and let the printer do the talking.

Tweaks

Now that I've saved a good percentage of the network traffic, you need to look at getting the most out of your hardware that you've already purchased.

Windows NT and all the BackOffice components supply a rich set of performance counters, which make it easy to work out what your servers are doing and if they're coping. It's a good idea to take PerfMon logs on every major counter for a week or so and work out baseline performance for your servers. Then about once every three months or during known busy times, do it again and compare against previous baselines. By looking at the results of the comparisons, you can determine if your servers are coping with the load, or if they need upgrading. There are heaps of performance tuning references, including the resource kits from Microsoft, so I'm not going to go into much detail here. These baselines make it easy to justify purchasing upgrades or new servers. Without them, you may as well wet your finger, stick it in the air and see which way the wind is blowing.

Conclusion

It's important to set up your environment to best cope with the operating system you're going to use most. If that happens to be Windows NT, then a few small tweaks and some generic good advice will make the difference between a marginal existence and a trouble free, fast environment.

Preparation is Better than Cure

by Catherine Allen (catherine.allen@eserv.com.au)

Preparing for an external security audit, particularly over machines which have not been audited before, can be a lot of fun. It's a great time to test your security procedures, particularly installation guides if you have any, and to jot down all the things you've fixed, so that you know what to check for next time.

Use the policy and procedure documents available to you to create a checklist for the security of the machines. Any areas of non-compliance should be documented as they are fixed.

If the machines in question have been audited previously, then the audit report is another good resource. The audit report should include areas where the machines failed to comply with security policy or procedures. Obviously, these should be checked to ensure that the non-compliance is fixed for the next audit. Be aware that the audit might have sparked a change in policy statements or procedures, which may mean that the recommended changes are not to be undertaken on particular machines.

If there is no computer security policy or if the policy and procedure statements do not cover specific installation and configuration issues, then the next port of call for many systems administrators is the AusCERT Unix Security Checklist [CHKLST]. Although it's getting a little old, the checklist includes a good basic set of configuration vulnerabilities to look for.

If the AusCERT checklist looks daunting, don't panic. There are tools which can help you to run the suggested checks automatically. Most people will have heard of COPS before but a surprising number appear not to have heard of Tiger [TIGER], which does a similar job. It's valuable to use both tools because neither tests a superset of the other.

More recent tools are available [TOOLS], so hunt around for a tool that suits you.

Back to the topic of policy documents. If you don't have any, now is a good time to start the push for writing some and getting them ratified by management [POLICY].

Reviewing procedures can be a very important aspect of an external audit. If the external auditor plans to go through the procedures and policy documents, then it's a good idea to be sure that they're in good order. Ensure that the stated procedures comply with the policy statements and that all policy is supported by procedures.

A detailed network diagram including IP addresses, subnet masks and information flow for all incoming protocols should also be available to the auditor.

Some "rules of thumb" for preparing machines for an audit are included in the Appendix.

To obtain a good report from an external security audit, ensure that all devices are configured according to the policies and procedures in place. Internal audits may be carried out to ensure continuing compliance with policies and procedures. Systems administrators can leverage off reports from previous external and internal audits.

References

- [ADVISY] http://www.auscert.org.au/Information/Advisories/aus_advisories.html
or <ftp://ftp.auscert.org.au/pub/auscert/advisory>
- [CHKLST] ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist
- [POLICY] Geer (Ed.), Oppenheimer, Wagner and Crabb, System Security: A Management Perspective, USENIX Association for SAGE, 1997
- [TIGER] <ftp://net.tamu.edu/pub/security/TAMU/tiger-2.2.4p1.tar.gz>
and <ftp://net.tamu.edu/pub/security/TAMU/tiger-2.2.4p1-patch>
- [TOOLS] http://www.auscert.org.au/Information/Tools/other_tools.html

Appendix 1 Preparing Routers and Hosts for Audit

To prepare routers for an external audit:

- * ensure the most recent non-vulnerable version of the operating system (or IOS) is in use;
- * ensure that an encrypted password has been enabled for telnet connections to the router;
- * if there is more than one level of access to a router, ensure that the privileged access is protected by an encrypted password;
- * ensure that the router filters comply with the organisation's security policy;
- * ensure that security procedures are being carried out, particularly that logs are monitored and acted on.

To prepare a firewall or bastion host for an external audit:

- * ensure that the host has the latest version of the operating system and that the appropriate patches or service packs have been applied;
- * ensure that the operating system on that host has been pared down to only the required utilities;

- * ensure that the files relating to all services which run with administrator or superuser privileges are owned by the administrator or superuser and have restrictive permissions;
- * ensure that the filters on the routers and the firewall host comply with the organisation's security policy;
- * ensure that security procedures are being carried out, particularly that logs are read and acted on.

SAGE-AU'99 - A Tutorial Review

Evaluating a Site's System Administration Maturity

reviewed by Geoffrey Day (gday@arcbs.redcross.org.au)

For the first time during a SAGE-AU conference I somehow managed to choose mostly non-technical tutorials to attend. This came as a surprise to me as I am not inclined towards management at all and after being back at work for only two days my attitude was confirmed - I do not want to manage a group of people yet.

Elizabeth Zwicky's tutorial however was pitched at exactly the right level for me, with the tutorial being focused largely on managing technical issues rather than people issues.

Elizabeth took an interesting approach by first giving an overview and touching briefly on statistics before heading into a look at some of the key areas of site administration. After defining the goals of the tutorial and site administration Elizabeth proceeded to show us how to "cook" any statistic we like to show what we wanted. One of the statistics given as an example is the Staff-to- User Ratio. Tricks for manipulating this included redefining positions i.e. a database administrator is NOT a system administrator and noting that a user does not need to know you exist before you can count them. Since these types of numbers are so easily manipulated they were completely avoided for the remainder of the tutorial.

The remainder of the tutorial covered : backups, security, networks, user support, application support, data sharing, maintainability and long term viability, and lastly human resources issues. For each of these topics a summary was given, followed by examples of what happens at an Average, Good and Excellent site. Accom-

panying many of the "gradings" for topic were examples from Elizabeth's consulting experience.

As an example from the tutorial notes:

Backups : Average - There is some sort of backup system in place, Coverage is spotty, backups are only done by one person

Backups : Good - There is a known backup system in place, People know what is backed up and what is not, more than one person knows about the backup system

Backups : Excellent - There is a good quality, supported backup system in place, backups are available on every platform, Backups and restores can be done by juniors

This was the most interesting part of the tutorial as I sat looking at the examples and thinking to myself "yeah my site would mostly fit into the Good category for backups". However in most categories I found that my site did not neatly fit into Average, Good or Excellent but spanned two or even three of the gradings. At that point I asked Elizabeth what she thought of this fact. She noted that at every site some areas are excellent, some are average and some are not so good, it all depends on the strengths and weaknesses of the staff you have.

In all the tutorial was perfectly pitched for myself, not totally technical nor completely management based, a neat blend of the two. The ratings for each topic, along with the concrete examples, provide a way for those present to return to their sites and do an informal audit of how mature their site really is.

Book Review

Mastering Regular Expressions

Reviewed by Karl Hanmore (avatar@ultra.ultra.net.au)

If you are unlucky enough to be like me, your understanding of regular expressions is probably not as good as it could be. I had the dubious pleasure of meeting them when first learning perl. They were complex and so, after picking up the basics, I left them for the greener pastures of writing interesting (and not so interesting) perl scripts, sans regex. This however, was probably one of my poorer decisions in my perl life, as pretty soon I found I needed to deal with these unwieldy beasts.

When it comes to checking that people are not trying to input invalid characters into your database or file name, you really just cant go past regular epressions. For over a year I have scraped together the barest chunks of regular expressions, spent hours trying to find why case X slipped through the loop and generally suffered much heartache over it all.

Finally, I ordered a copy of Jeffrey E F Friedl's Mastering Regular Expressions and it was indeed money well spent.

Unlike many O'Reilly books, which tend to read like a man page, Mastering Regular Expressions is written in an easy to read style. Friedl makes extensive use of analogies (perhaps too extensive) and examples to get his point across. The majority of the examples presented are in perl (I presume because its easy to understand and clearly the best programming language there is :), however he also presents examples from egrep, awk, sed, tcl and python.

The first chapter gives a rapid introduction to regular expressions, giving the reader enough of the basics in order to allow them to start using regex in their day to day lives. One thing which I personally found good was that Friedl makes no assumption of previous regex use. Even from the first chapter there were some subtleties which I gleaned which previously I had missed. One section I found of particular interest was regarding the effects of unicode characters and regular expressions. It suggested to me that the author has a good deal of experience with the less common (and more problematic) tasks for which one may use a regular expression.

Chapter Two extends the solid introduction from Chapter One, giving a 10 second introduction to perl (which would be useful for those who don't know the language) and then proceeds with some "real world" examples. Many examples are presented in a format where the answer is on the overleaf from the question. I personally find this quite good as it encourages the reader to attempt to solve the problem as opposed to blindly reading the answer. Several examples include common pitfalls, so in solving the question the reader gains a good understanding of some of the practical problems in day to day regular expression use.

The following chapters start to get into the "nitty gritty" of using and constructing regular expressions. Chapter Three discusses many of the different "flavours" of regex and is peppered with examples and perhaps a couple more analogies than are really required. Chapter Four delves into the way in which the different regular expression engines handle the somewhat daunting task of actually processing the regular expressions that the previous chapters have inspired us to dream up. For those of you with a love of the theoretical aspects of computer science and mathematics, this chapter touches on DFA's and NFA's and explains the difference with reference to regular expression processing.

Chapter Four also explains (with reference to the underlying engine structure) the reasons for such concepts as "greediness" (.*) and how different ways expressions are structured can make a large difference in the processing time with certain engines.

Chapter Five continues on from Chapter Four (as one might imagine) delving deeply into backtracking issues and the time complexity of different queries under different regex implementations.

Chapter Six, "Tool Specific Information" would probably have to be one of the most useful references when faced with a flavour of regex you are unfamiliar with. It has a number of friendly tables which provide a quick look up of the features and syntax of the various engines. And no book on regular expressions would be complete with-

out a chapter on perl. A point of note is that the perl chapter takes up about one third of the book!

Overall I found this book most worthwhile. Just as described in the books preface it can be used as a reference book, but is best read as a story. The author's use of examples and interesting side-tracks turn what could have been one of the most dull and boring topics ever to reach press into an enlightening journey into the world of regular expressions. The obvious depth of experience of the author leads one to believe that there is not a problem which regular expressions cannot solve (or at least play a part) My only negative comment regarding this book would be that a few of the analogies (as much as I love them) do get a little long winded.

All things considered it was probably the best book purchase I have made this year. If you ever use perl, sed, awk or one of the various incarnations of grep, get this book.

Table of Contents

1. *Introduction to Regular Expressions*
2. *Extended Introductory Examples*
3. *Overview of Regular Expression Features and Flavors*

4. *The Mechanics of Expression Processing*
5. *Crafting a Regular Expression*
6. *Tool-Specific Information*
7. *Perl Regular Expressions*
- A. *Online Information*
- B. *Email Regex Program*

Book Information:

ISBN 1-56592-257-3

Pages 368

1st Printed January 1997

Publisher O'Reilly and Associates (Sebastopol, CA)

Current Reprint December 1998, 7th printing (minor corrections)

Hotline Books (<http://www.hotline.com.au>) (\$69.95AU)

Dymocks (<http://www.dymocks.com.au>)

O'Reilly (<http://www.ora.com>)

I personally purchased my copy through Hotline. I was impressed by the speed of the service. I ordered the book late Sunday night, and it was delivered by lunch time on the Wednesday.

Items for Sale

<u>Item</u>	<u>Member Price (\$)</u>	
SAGE Job Description Booklet	15.00	
SAGE Computing Policy Booklet	15.00	
SAGE System Security Booklet	15.00	
SAGE Educating & Training Booklet	15.00	
SAGE-AU'94 Proceedings	15.00	
SAGE-AU'95 Proceedings	15.00	
SAGE-AU'96 Proceedings	25.00	
SAGE-AU'97 Proceedings	25.00	
SAGE-AU'98 Proceedings	25.00	
SAGE-AU'99 Proceedings	25.00	<i>New!</i>
SAGE-AU'98 Conference Video CDROM	50.00	
SAGE-AU'99 Conference Video CDROM	60.00	<i>New!</i>
SAGE-AU Polo Shirts (Navy & Black)	25.00	<i>New!</i>
SAGE-AU Coffee Mugs	5.00	

Note:

Postage & handling is charged at \$3 for the first item, and \$2 for each additional item (for Aust residents - overseas postage charged at cost).

Many of these items are in short supply, so "first in, best dressed". To order any of these items please complete an order form which you can find at:

<ftp://ftp.sage-au.org.au/pub/SAGE-AU/Forms>

Mailing Lists

sage-au	sage-au-exec
sage-au-announce	sage-au-membership
sage-au-chairs	sage-au-jobs
sage-au-conf	sage-au-skills
sage-au-pubs	sage-au-standards
sage-rg-exec	sage-rg-tres
sage-nsw-exec	sage-nsw
sage-qld-exec	sage-qld
sage-vic-exec	sage-vic
sage-wa-exec	sage-wa
sage-bris	sage-rocky
sage-tas	sage-act

Most of the mailing lists are available for members to subscribe to.

Please see the page on the website, at: **<http://www.sage-au.org.au/resource/maillist.html>** for information about joining the various lists.

DEFCON 7 9-11 July, 1999

by Brian Meilak (brian@gremlin.com.au)

This was an interesting conference and an interesting experience. It was an opportunity to meet and see a lot of faces and personalities behind the names that I have seen on the Internet ie: IRC, news, bugtraq, ntbugtraq etc.. There was always something going on somewhere at the conference venue.

The conference was on at the Alexis Park Resort, www.alexispark.com. Approximately 2500-3500 people attended on any day and the place was packed. There were three streams: a newbie and two technical types. Each stream was generally packed. On the first day, the presentations ran on time and with the right speakers. Things tended to go astray after that - presenters/talk times were changed due to people flying in/out, being too drunk/sick to talk or being at the Defcon Shootout out in the Nevada Desert instead of doing their talk.

The subject matter for talks was wide. Simple Nomad spoke about hacking Novell Netware. This session was followed by Hacking Oracle 101 by Vic Vandal. The session on HERF guns, EMP bombs and weapons of mass disruption by Winn Schwartau was also very enlightening. Its seems amazing what an electrician can do with \$750 of stuff from the local hardware/electronics shop. From the lock picking demo by V1RU5, I now know how to get out of handcuffs and to pick my front door lock. The Las Vegas Spy shop sold out of \$30 lock picking sets

on the first day of the conference.

Deanna Peugeot (Electronic/Electrical engineer background) gave a talk titled "Embedded systems hacking". It was about designing/building 'simple devices' ie: network/keyboard monitors etc. that could be attached to the network. Devices would include a small processor and say a PCMCIA card for storage. Basically, small spy type stuff. Wish I knew a diode from a capacitor.

Daremo's presentation, 'The Firewall Appliance: Friend or Foe?', covered the results of his evaluation of 23 firewalls (he had approached 32 or 34 vendors) out on the market at the moment. Things he examined: setup/install, documentation, support, response time to fixes for new vulnerabilities released on the net, management, performance under various loads, did it actually do what the doco said? etc.. At the time of the conference, he could not release his findings as lawyers - his company's and various vendor company's were working out the 'small stuff' ie: so he doesn't get sued into oblivion!"

The Cult of the Dead Cow's release of BO2K! was... interesting. It was like a Micro\$oft launch except I think I preferred this one. Lots of noise, lights, etc. A live demo was given. It was good. CDC have put a lot into BO2K. I especially like how it could be controlled via TCP or UDP or ICMP. At the end, more loud noise, computers were smashed on stage, Mudge played his guitar then proceeded

to smash that on stage as well. When CDC people started throwing out CD's of BO2K, mmmm people went a bit wild to get them. A person (a manager from ISS I was told later) was seen diving through the air to get one! Man can fly.

Between sessions "Spot the Fed" was played where if you think you saw someone was a Fed, you'd drag that guy/girl out on stage for questioning by the crowd ie: do you carry a gun? can you carry a gun on an airplane? If you were right and they were a Fed, you both got a t-shirt :). This was always very funny and well received. Several Feds were successfully identified this way.

All manner of junk could be purchased ie: t-shirts, stickers, books, 2600 was there, Sun IPC's, sparc 1, 2's, SGI machines, a battle field radar unit, mobile phones, network hubs, switches, routers...

Media reports, pics, pre, during, post information is all at www.defcon.org

General

One of the underlying tones that came from both conferences (I attended Blackhat 99 as well) was the security professionals out there who are not really security professionals ie: the fakes. Fakes who are installing insecure systems in your company. People selling security products or services who don't really understand the product or underlying concepts. Or just plain liars. These people are making deci-

sions in organisations that are wrong, ie. you don't need to put filtering on your router, your firewall can handle it all.

Mudge (LOpht Industries and LOpht-crack author) during his presentation at Blackhat99 spoke about being called up by one of the big companies and asked to technically interview an applicant for a senior security position. The applicant had already been through several interviews and had passed with

flying colours. Mudge agreed and within a couple of minutes of interviewing the candidate was told by the candidate that he wrote lOpht crack.. big mistake, he didn't get the job!

Another tone was the usual distrust and/or hatred of Microsoft (all comments /dev/null - just my observation only!).

The colour black was in. The majority of gurus wore black and had long hair. (Our very own Lucifer comes to mind here :)).

And if you didn't have a mobile phone, a palm pilot, and a short wave radio/talkies with a groovy ear/mouth piece (so you could keep in touch with your buddies at the conference), then you're not with it.

I found both conferences to be worth while and intend to visit again next year. They gave me a different perspective on what is happening in the computing industry and with the Internet overseas. cheers!

SAGE-AU'99 Conference CDROM - On Sale Now!!!

Contains:

- * Videos of all conference talks and sessions (inc. panel session on the "Online Censorship Bill" which included the ABA, IIA, Sen. Kate Lundy (Labour), EFA, Australian Democrats, eServ, etc.
- * Approximately 11¹/₂ hours of high-quality video.
- * Video presented in 384x288 full colour at ~5-6fps.
- * All conference slides and papers.
- * Full notes for two of the half-day tutorials.
- * AGM slides and minutes.
- * All materials supplied in a OS-neutral format. ie. text/html/pdf/RealPlayer.
- * A browser friendly WWW interface.
- * Links to other relevant information.
- * Conference flyers and call for participants announcements.
- * A full 650 Meg of data!
- * Runs completely off CD-ROM.
- * Membership application forms and How to Join SAGE-AU.
- * An amazingly low price - \$AUD60 for members, \$AUD160 for non-members.

Complete an order form (see <ftp://ftp.sage-au.org.au/pub/SAGE-AU/Forms>) and return with payment to SAGE-AU, GPO Box 2974, Sydney 2001 or fax the form with credit card payment to 0500 5444 88.



Quick, Dirty and Useful Perl

by Karl Hanmore (avatar@ultra.ultra.net.au)

One of the most frustrating things that I used to find in my day to day life working for a small ISP was, "Can you please forward my mail to x@y.com while I am away?"

"No worries", I would reply, and then they would ask, "Oh can you also forward the mail that's still in my inbox? Thanks ... bye." *click*

The joy of forwarding several hundred messages from pine with the bounce command is not great but what were my options?

Well, I could just mail them their mailbox file and let them deal with it. This, however appealing, is not an option. Customer service would dictate that the mail should appear as close to its original format as possible (We don't want to force people to think now do we?)

I had been playing with Perl for a little while when this problem yet again cropped up. I made a decision, I would change the world, I would write a messy little script to solve my problem. I did, and it did, and you should find it below.

A couple of things to note. 1) the code is disgusting; I wrote it when I was learning AND in a hurry and as it still works, I haven't fixed it :) 2) It doesn't really know how to cope with errors be they in the file or socket connection errors. Again, I have never had a problem with it and thus I didn't fix it.

Please forward all flames about my useless coding to /dev/null but if its going to get you out of forwarding hundreds of messages in pine, feel free to use it!

```
#!/usr/local/bin/perl
# This script is copyright Karl
# Hanmore 1999 (avatar@ultra.net.au)
# Feel free to use, abuse and
# modify it as you see fit.
# This script may well eat your
# mail, chase your cat and other
# nasties,
# there is no warranty of any sort
# with this script, use it at your
# own risk!
#
```

```
# For those of you who hate typ-
# ing, this script is available at
# ftp://ftp.scripts.pl/pub/users/
# avatar/forwardmail
use Socket;
```

```
$domain_suffix="example.com";
$smtp_server="mail.example.com";
```

```
print("\nPlease enter the path to
the folder you wish to resend:");
$mailfolder=<STDIN>;
chop($mailfolder);
print("Please enter the email ad-
dress of the recipient:");
$mailto=<STDIN>;
chop($mailto);
print("\nFolder:$mailfolder De-
liver to:$mailto\n-Enter to Con-
tinue-\n");
$dummy=<STDIN>;
```

```
$messageopen=0;
open(FOLDER,$mailfolder)||die("Could
not open $mailfolder\n");
while ($fin = <FOLDER>)
{
    if (($fin =~ /^From /
)&&!(($fin =~ / From /)))
    {
        &CloseMail if $messageopen ==
1;
        sleep 5 if $messageopen == 1;
        @array=split(/ /,$fin);
        $from=$array[1];
        &OpenMail($mailto, $from);
        $messageopen=1;
    }
    print SOCKET $fin if
$messageopen=1;
}
```

```

sub OpenMail
{
  @instuff =@_;
  $user=$instuff[0];
  $from=$instuff[1];

  $port=25;
  $iaddr = inet_aton(
"$smtp_server" );
  $paddr = sockaddr_in( 25,
$iaddr );
  $proto = getprotobyname(
"tcp" );
  if (! socket(SOCKET, PF_INET,
SOCK_STREAM, $proto ) )
  {
    print "ERROR, connection
refused\n";
    $error=2;
  }
  if (! connect( SOCKET,
$paddr ) )
  {
    print "Unable to connect
to $host!! Failing !!";
    $error=4;
  }

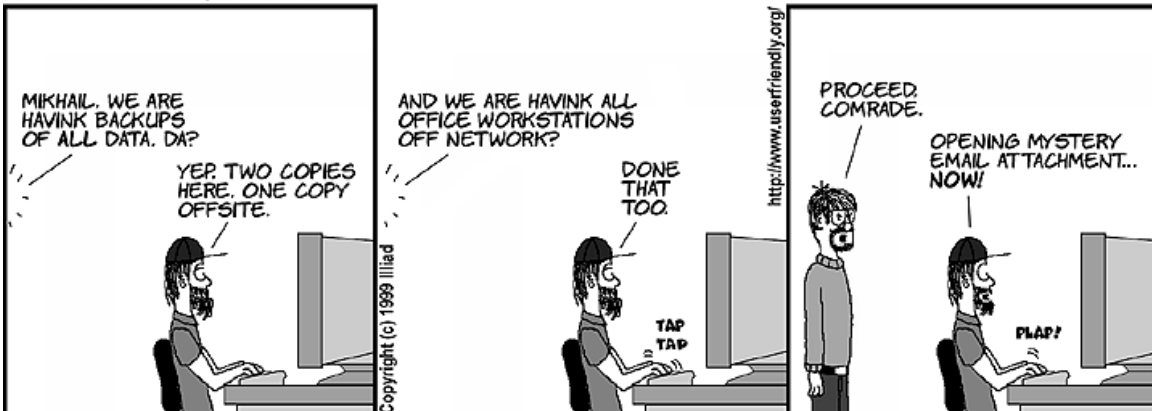
  select(SOCKET);$|=1;
  select(STDOUT);
  while (1)
  {
    $in = <SOCKET>;
    print $in;
    #print ("\nblah\n");
    if ($in =~ /220 /) {last;}

    #print ("\nwaiting \n");
  }
  #print "before mail from";
  $from="$from@$domain_suffix"
  if ($from !~ /.*\@.*/);
  print SOCKET ("Mail from:$from
\n");
  while ($in = <SOCKET>)
  {
    print $in;
    last if ($in =~ /250/);
  }
  print SOCKET ("rcpt to:
$user\n");
  while ($in = <SOCKET>)
  {
    print $in;
    last if ($in =~ /250/);
  }
  print SOCKET ("data\n");
  while ($in = <SOCKET>)
  {
    print $in;
    last if ($in =~ /354/);
  }
}
sub CloseMail
{
  print SOCKET ("\n.\n");
  while ($in = <SOCKET>)
  {
    print $in;
    last if ($in =~ /250/);
  }
  print SOCKET ("QUIT\n");
  while ($in = <SOCKET>)
  {
    print $in;
    last if ($in =~ /221/);
  }
  close(SOCKET);
}

```

Reproduced by kind permission of User Friendly (http://www.userfriendly.org)

USER FRIENDLY by Illiad



Regional Groups

NSW Chapter Report : Titus Chiu (titus@carbon.chem.unsw.edu.au)

The NSW Chapter has been progressing well since the last report. Regular monthly meetings have been held in Sydney (with the exception of July) with an average attendance of around 25 people. This is yet another increase from an average of around 20 in the last report. As reported at the SAGE-AU'99 conference, NSW member numbers are rising nicely and this is reflected in the local meeting attendance.

In May, Zip World (zip.com.au) gave a talk on the interesting world of ISPs.

In June, the topic was RCS. Yours truly presented a case study of practical RCS use for a system adminis-

trator. Then Igor Rosenfeld from Compaq talked about a localised version of WebRCS and how it is used by developers at Compaq.

In July, no meetings were held with the highlight obviously being the SAGE-AU'99 Conference held in Sydney's Novatel Hotel in Brighton-le-Sands.

In August, post conference excitement along with interesting talks by Peter Hughes from Sequent and Karl Veitch from Arthur Andersen attracted a most impressive rollup of around 40 people with people coming from as far as Penrith to attend.

WA Chapter Report : Tom Hallam (thallam@ee.uwa.edu.au)

Pre. meeting drinks started at 6:00. SAGE members had a private room at the back of the "Moon and Sixpence English Pub" with tables scattered though it. This was an informal atmosphere which led to lots of discussion. Members arrived from about 6pm onwards and helped themselves to their favourite drink: Newcastle Broun Ale, Guinness, lemonade whatever...

The meeting started about 6:30 and was a fairly rambling affair with lots of open discussion; although the topic was "The SAGE-AU conference" various other topics were also covered like "Would you ever use an WWW interface for administration".

The highlights, lowlights and tutorials attended by group members were discussed. General consensus was that the conference was very successful and worth going to.

Future SAGE-AU meetings ideas were discussed. There seemed to be about as many people wanting Tuesday as Wednesday. It was decided that SAGE-AU WA will:

- Meet at "Moon and Sixpence English pub" on the first Wednesday of each month. This may change to every even month (see below)

- Discuss alternating monthly meetings with AUUG-WA.

- Discuss doing combined events with AUUG-WA.

Some members thought that Perth might not have the population to support both SAGE-AU and AUUG so the alternating meetings was suggested as a possible way of keeping both groups going. There is also a large overlap in membership between the two groups. As SAGE-AU numbers have been going up Australia wide and AUUG numbers have been going down I'm not sure that this is a good idea.

There were various ideas for meeting subjects. I now have to chase these up. I see the availability of speakers for meeting subjects as being a key issue to how many meetings we can have and how many new members we attract.

Please pass any meeting subject ideas on to me (with contacts / speakers if you have them).

Victorian Chapter Report : Steven Pemberton (spember@ue.com.au)

The Victorian Chapter continues to meet on the second Tuesday of each month.

Looking back over the past couple of Victorian Chapter Reports, I notice many of the same issues and aims are current again today. That's not an indication that nothing's happened in that time, but more a sign that our needs are growing.

Meeting Venue

In 1997 we were searching for a new venue, and having found one we are now looking again. In September last year we moved from upstairs at Cafe Coco to a hired conference room in "The Public Office". Our aim now is to find an improved venue, with larger seating capacity, better A/V facilities, and possibly closer to the CBD.

If you know of a near-CBD venue that would suit our needs please contact the Victorian Executive.

Member's Meetings

We held a meeting every month except July, with the December meeting being a purely social event.

Our new meeting format, trying to present two complementary talks each evening, has worked well and we've covered a broad range of topics in the past year. We have hosted presentations from both members and non-members, and once screened a video from the '98 Conference.

Interestingly our highest attendance for the year was the June meeting which featured David Burren's "Connectivity on a Budget - Virtual Networking" and Luke Parson's non-technical "Effects of the proposed GST on IT&T Contracting". The June meeting was also hosted at RMIT, right in the CBD, so maybe that also contributed to our 40+ turnout.



David Le Blanc presenting his talk on CA-Unicenter

Speakers

The task of organising speakers has ranged from easy, where volunteers have called us, to frantic, when several "potential's" evaporated at the last moment. We've somehow always managed to find a speaker on the night and the show went on regardless.

Topics we hope to coerce^H^H^H^H convince speakers to present in the near future include:

- * How to increase your hourly rate
- * Managing IT Staff
- * Managing a large mail system
- * NNTPcache
- * Business Continuity Planning
- * High Availability
- * BSD on a palmtop computer
- * Enterprise backup

Please take a moment to think what you could present at a future meeting. Something you may be working with could be very interesting to your fellow members.

Membership Drive

With the ever present spectre of QLD Chapter to urge us on (and NSW not far behind) the need to boost membership remains pressing. :)

Something I'd like to try this year is a "membership" day, where we host a sort of SysAdmin "show-and-tell" for students and other potential SysAdmins.



As the crowd looks on in stunned silence

New Victorian Executive

- President - Steven Pemberton
- Vice-President - ### Position Vacant ###
- Secretary - Colin Linahan
- Treasurer - David Keegel
- List Chair - Morrie Wyatt

We very much want to fill the position of SAGE-VIC Vice-President. If you are interested, or want to nominate someone else, please come forward! The Vice-President will need to help organise meetings, solicit speakers, and regularly attend the monthly meetings.

My personal aim this year is to promote SAGE-AU to new members and other organisations, and investigate additional membership benefits for current members.

I hope to see many of you at our next meeting on the 14th of September 1999.



And after the talk, networking of the other kind

Regional Groups



Victorian Chapter

The Victorian group currently meets on the second Tuesday of the month at 6:45pm at

The Public Office
Top floor, 100 Adderley Street, West Melbourne
Ph: 9328 2821

- President:** Steven Pemberton
Steven.Pemberton@member.sage-au.org.au
- Secretary:** Colin Linahan
Colin.Linahan@member.sage-au.org.au
- Treasurer:** David Keegel
David.Keegel@member.sage-au.org.au
- List Chair:** Morrie Wyatt
Morrie.Wyatt@member.sage-au.org.au

The group mailing list is sage-vic@sage-au.org.au.



NSW Chapter

The NSW group currently meets on the second Tuesday of every month at 6:45pm at

Level 9/50 Miller Street
North Sydney
Phone 02 9779 1869 or
0417 232 934 for entry after 7pm

- President:** Titus Chiu
Titus.Chiu@member.sage-au.org.au
- Treasurer:** David Scott
David.Scott@member.sage-au.org.au
- Secretary:** Andrew Whyte
Andrew.Whyte@member.sage-au.org.au
- Syd. Organiser:** Zebee Johnstone
Zebee.Johnstone@member.sage-au.org.au

The group mailing list is sage-nsw@sage-au.org.au.



Queensland Chapter

The Queensland group currently meets at 7:00pm on the second Thursday of every month at

Room 343, Level 3
General Purpose South Building (No. 78)
The University of Queensland
Staff House Road
St Lucia Brisbane

- President:** Sam Lor
Sam.Lor@member.sage-au.org.au
- Secretary:** Mark Suter
Mark.Suter@member.sage-au.org.au
- Treasurer:** Brad Marshall
Brad.Marshall@member.sage-au.org.au

The group mailing list is sage-qld@sage-au.org.au.



ACT Chapter

The ACT group currently meets at 6:00pm on the last Tuesday of every month (excluding December) at

Computer Training & Consultancy
4/40 Thesiger Court
(upstairs in the AFPA building)
Deakin, Canberra

- Interim President:** Roy Meuronen
Roy.Meuronen@member.sage-au.org.au
- Interim Secretary/ Treasurer:** Steve Jenkin
Steve.Jenkin@member.sage-au.org.au

The group mailing list is sage-act@sage-au.org.au.



West Australian Chapter

The West Australian group currently meets at 6:00pm on the first Tuesday of every month at

Moon & Sixpence British Pub
300 Murray Street, Perth

- Organiser:** Tom Hallam
Tom.Hallam@member.sage-au.org.au

The group mailing list is sage-wa@sage-au.org.au.



Tasmanian Chapter

The Tasmanian group currently meets on the third Monday of every month at a different location depending on the event being held (check <http://www.sage-au.org.au/rg/tas> for info.)

- President:** Geoffrey Day
Geoffrey.Day@member.sage-au.org.au
- Secretary:** Bron Godwana
Bron.Godwana@member.sage-au.org.au
- Treasurer:** Vacant

The group mailing list is sage-tas@sage-au.org.au.