Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Keep Current With Little Time

Once a secure network is established, it does not stay that way without work and keeping current is easily a full-time job. This paper discusses various ways for security professionals to keep current with less time.

Copyright SANS Institute
Author Retains Full Rights

AD
nitrosecurity Log Management

Keep Current With Little Time

Overview

Proactive, not reactive! There, I said it, now we can move on. Keeping current for security professionals is easily a full-time job and is probably the most important thing after establishing a secure network. Once a secure network is established, it does not stay that way without work. For many though, time is a problem. There are many ways to keep current with computer security. This is an attempt to cover many possibilities, with discussions on each, to help with your decision on developing a plan to keep current with less time. Many links are given for reference, to give a feel for what is out there. It would be senseless to visit every link to keep current. Keep in mind; this is about keeping current, which assumes that your network is already secure, and you want to thwart unknown future vulnerabilities. I think that it is appropriate however, to mention a site here (http://xforce.iss.net/) that is used for searching known vulnerabilities till present.

Books, Magazines

Books and magazines are great for learning and catching up but any printed material is really no way to keep current. By the time it takes to print the information and distribute it, it is probably already too late. Sure, there may be some good stories and good pointers, but leave it at that. It may be a month or more until read, and what about mistakes or missed information. It may be a long wait until the next print. Focus your attention elsewhere. For completeness, here is a short list of some material that may be of interest.
Magazines: www.wired.com www.2600.com www.fcw.com www.zdnet.com http://computerworld.com http://www.ieee-security.org/cipher.html http://www.elsevier.nl/inca/publications/store/4/0/5/8/7/7/ http://www.isec-worldwide.com/ http://www.infosecuritymag.com/ http://www.infosecnews.com/ http://www.advisor.com/wHome.nsf/w/MIS http://access.ncsa.uiuc.edu/ http://www.westcoast.com/ http://www.advisor.com/wHome.nsf/wPages/SAmain http://www.securitymanagement.com/ http://www.securitysales.com/main.cfm **Books:** http://www1.fatbrain.com/catalogs/computing/subjects.asp?VM=C&SubjectCode=IHA&qorder=best&from=VJN388

Conferences (with a word about 0-Day)

0-Day? What the heck is that? This subject deserves a section all to it's own but we talk about it here for good reason. 0-Day (zero day) is a term used to describe exploits that only the criminals know about, or exploits that the public does *not* know about yet. There are ways to gather 0-day exploits, like becoming "buddies" with the criminal hacker community (not the best way), discovering them for yourself (people do this for a living), and setting up "honey pots". A honey pot is a computer system that uses special software to pretend to be a real vulnerable system. WHY? These honey pots can be used to "fish bowl" or unknowingly trap a person in a system that is contained where that person can cause no real harm. Every step of this person can then be allowed to continue, whether for real or simulated, and logged. This way, new attacks can be safely discovered. Honey pot software (available from www.all.net/dtk/, www.engarde.com/software/ipwatcher/, and http://www.nfr.net/bof/ among others) is very successful when set up on high profile servers and when used in, you guessed it, conferences! Conferences are usually once a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

year and some are free, most are not. They can be anywhere around the world, which adds to your cost, that can already be very pricey. You ask again, WHY? Well, many conventions set up labs with hundreds of computers to play war games with. Since this is a place with a high concentration of hackers, it is a great place to set up your honey pot. And sometimes there is no substitution for real life face time. A person could learn a lot from these people, who may save some of their new exploits for showing off with. Here are a few links to some conferences out there:
www.atlantacon.com/, www.blackhat.com/, www.ccc.de/camp/index.html, www.ccc.de/WarmWelcome.html, www.cs.arizona.edu/xkernel/www/cipher/cipher-hypercalendar.html, http://conferences.calendar.com/, http://csrc.nist.gov/nissc/, www.cuervocon.org/, www.defcon.org/, www.gocsi.com/conf.htm, www.h2k.net/, www.hal2001.org/, www.iacr.org/events/index.html, www.ic0n.org/, http://internettrash.com/users/wraithtech/con99.html, www.itd.nrl.navy.mil/itd/5540/ieee/, http://members.tripod.com/~hwa_2k/canc0n.html, www.misti.com/conference.asp, www.nswc.navy.mil/issec/cid/shadowcon.html, http://phreaknic.org/main/index.php3, www.rootfest.org/, www.rsa.com/index.html, www.rubi-con.org/, www.sans.org/newlook/home.htm, www.summercon.org/, http://tisc.corecom.com/, www.toorcon.com/, www.u-h-c.com/, www.usenix.org/.

IRC

For many, hacking is a social activity. People around the world enjoy hacking and love to talk about it with other hackers. Well, if they live around the world, how will they communicate you ask? Chat groups of course! Look around the chat groups for some of the following: #enforcers, #hackphreak, #x-treme, #coders, #nevaeh, #hackschool, #hackers, #dc-stuff, also look for groups that contain keywords like hack, 2600 or any other hacker related words. Not all chat groups are visible to your IRC program though. Many people join groups that are secret. To find secret groups, you could try to join groups that are not listed by using key words like the ones listed above. This may or may not get a person anywhere because even if you make it to a secret group, you may just get kicked out. Another way is to talk to people on the public chat groups and get invited to some of theses groups. To keep current this way, you will probably have to pose as a criminal yourself, which is not always the best solution. True, a person could learn from the bad guys, but one can also learn from the good guys. Learning involves trust and sometimes mentoring develops, which could negatively influence your behavior. Learn to be a professional not influenced to be a miscreant.

News Groups

This is another way that hackers can communicate and send little goodies out to others. Yes, there are other uses of news groups other than porno. It is also safer than IRC and will not take as much of your time. News groups can vary according to your service provider, so it is easier to just get on the news groups and look for your self. Look for key words like hack, crack, and 2600.

Web sites

As previous discussions mentioned, time is very important. Which is why web sites are a great way to keep current. Now, in keeping with the title, visiting every web site

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

mentioned here would take too long. I do recommend though, that you visit all of these sites to get a feel for them and choose for yourself which of them should be regularly visited. After reviewing the sites and picking the ones you feel comfortable with, you may want to bookmark them in a special folder, maybe called something like "Security" or what ever makes sense. Over time, you will get used to the sites and know your way around them quickly. You should also be able to tell very quickly if there is something important to pay attention to. The following is a good, but by no means all-inclusive, list of security related matters. Many links were already broken before this writing was over and had to be removed but is still comprehensive. They are divided into a few groups, vendor sites for updates, sites designed for white hats (security professionals – the good guys), and sites designed for black hats (bad guys – WARNING, many times bad guy sites exhibit pornography and other offensive material.). I should mention, it is not always easy to distinguish between white hats and black hats. My distinctions here are made through a show of professionalism and of references to improve security. **Vendors:** www.freebsd.org/security/, www.debian.org/security, http://java.sun.com/security/, www.redhat.com/cgi-bin/support/, www.microsoft.com/security, www.sgi.com/support/security/, http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access **White hats:** www.auscert.org.au www.boran.com/security/ www.cac.washington.edu/people/dad/ http://www.cerias.purdue.edu/coast/hotlist/ www.cert.mil www.cert.org http://www.ciac.org/ciac www.esecurityonline.com www.fedcirc.gov www.first.org www.gocsi.com www.hideaway.net/ www.incidents.org http://infosec.navy.mil www.infosyssec.com www.infraguard.net www.isalliance.org www.isc2.org/ http://www.issa.org/ http://l0pht.com/ http://lwn.net/2001/0308/security.php3 http://www-nasirc.nasa.gov www.netsecurity.about.com www.neworder.box.sk www.nipc.gov www.nsi.org/compsec.html http://www-ns.rutgers.edu/ www.ntsecurity.net/ http://oliver.efri.hr/~crv/security/bugs/ www.privacy.org/ipc/ www.rootshell.com www.searchsecurity.com www.securezone.com www.securityfocus.com www.securitywatch.com http://shadowpenguin.backsection.net/ www.telstra.com.au/info/security.html www.tno.nl/instit/fel/intern/wkinfsec.html www.truesecure.com http://ugu.com www.whitehats.com http://wiscinfo-nt.doit.wisc.edu/badgirt/ **Black hats:** http://attrition.org/, www.chaostic.com/unix.html, http://www.cyberarmy.com/zzine/, www.hackers.com/index2.htm www.hackers-supply.com/, www.hoobie.net/security/exploits/index.html http://www.nmrc.org/ http://www.technotronic.com/ www.insecure.org/index.html

Newsletters and Forums

This may come as a surprise. We have talked about time being of the essence so how can this be any better than web sites? Well, newsletters are not only sent out on a set period. Some newsletters are sent out when new issues emerge. There is something else though, that makes newsletters and forums especially attractive, and this has to do with how new security issues are reported. When vulnerabilities are discovered, they can be reported to the affected vendor or publicly reported. Reporting to the vendor gives the company time to issue patches to fix the problem. Reporting to the public, called full disclosure, has obvious problems. This would allow malicious hackers to take advantage of vulnerabilities before they can be fixed. Vulnerabilities are often reported to the vendor

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

first, then publicly. Full disclosure is also argued to force vendors to issue patches more quickly. Another argument is that it allows administrators to interimly fix the problem until a patch can be released. This is a controversial subject, and one that I will not argue here. The point is, full disclosure does happen and it mostly happens in newsletters and forums. Whether or not you agree with this practice, you should be watching for full disclosure discussions and is probably the number one way to keep current. Keep in mind, of course, not all newsletters and forums are full disclosure. Infosyssec has a great list of newsletters, so instead of list them all here, go there! http://www.infosyssec.com/infosyssec/secmail1.htm, http://infosyssec.master.com/texis/master/search/+/Top/Computers/Publications/Mailing_Lists. Here are a few other sites that may be helpful. www.auscert.org.au, mailto:cert-advisory-request@cert.org, www.cs.purdue.edu/coast/coast-news.html, mailto:ipsec@tis.com, http://lists.insecure.org/about/nmap-dev.txt, http://lists.insecure.org/about/vuln-dev.txt, mailto:majordomo@nl.linux.org?body=subscribe kernel-audit, http://archives.neohapsis.com/, mailto:nw-hack@dau-48.anthro.ufl.edu, www.securityfocus.com, http://www.unix-security.net/, www.usenix.org/publications/login/login.html. Some good forums: http://www.whitehats.com/cgi/forum/messages.cgi.

Luck?

Sure, why not? Many things have been invented and discovered through luck. A lot of interesting information can be found by just luck, why not security information? What am I talking about? Sometimes I like to browse my local library or bookstore just looking at random books till something interesting strikes me, after all, how could I know what I am missing if I did not know it existed? A person can do this on the Internet as well. Not to turn this into a search engine tutorial, but I would like to briefly mention, "not all search engines are created equal". Sticking with one search engine because it's what you use all the time is NOT wise. Before using your search engine again, go to http://www.cyward.com/notall.htm to read a little more about how search engines are used. Now, back to the subject (kind of). Let's talk about keywords. People *love* to think they are clever, especially hackers, so they invent words that sound clever to them. Most professions also have their own clever terms too; it's called jargon. Although hacker jargon can be difficult to search for because hackers like to replace letters with numbers and special characters, there are hacker dictionaries that are available online, search for them. To name a few dictionaries, take a look at these: http://tuxedo.org/~esr/jargon/jargon.html, http://www.lysator.liu.se/hackdict/split2/main_index.html, http://www.science.uva.nl/~mes/jargon/, and http://www.robertgraham.com/pubs/hacking-dict.html. Read through these dictionaries, pick out some popular terms, and write them down. Now, for the luck part of it, try some of these key words as URL's by prefixing with "www" or "http://" (without the "www") and appending ".com", ".org" or ".net". Vary the words and substitute letters, be clever! Also, go to a search engine and search with some of these words. Invariably, your search will take you to places you haven't seen and more jargon that you haven't heard, add these to your list and start over. Be creative! The other day I was just fooling around and

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

typed in www.yourmamma.com and a plain white page responded with "Your momma!" I was easily amused at this and although this does not seem to have anything to do with computer security, it shows that one may find things unexpected, which is exactly what you are looking for!

Designated Person

Hate cutting the lawn, cleaning the house, or taking out the trash? That's what kids are made for, right? Not only does it teach them values, it helps you out too! It's great to have people do things for you. Wouldn't it be great to have someone keep current on security issues for you? Of course it would! Provided that person did a good job of it. Why in the world would someone do this for you? Well I'm not sure that paying someone for this is such a good idea, however, having a trusted circle of friends or coworkers that also have this need can designate a person to do this on a rotational basis. Then, everyone benefits equally. Perhaps it can be discussed as to exactly how the designated person will obtain the information so everyone can be assured of the sources and the designated person could be shifted around weekly or monthly. Once the designated person has completed their daily update, that person could email the others in the group with hyperlinks and a few notes on important matters. It does not get much easier than this! Although not everyone can take advantage of this, it is great for the people who can.

Summary

With so many links, how in the world will this save time? Admittedly, this will take a little time at first. Look at all of the links and also some of your own. Find the ones you like and learn your way around them. To review, we have talked about books and magazines; forget them! We talked about conferences; forget them too. Remember, we aren't talking about becoming the ultimate hacking guru. Although this would be nice, and some of the material in here will help to achieve greatness, this subject is about speed. Next, IRC; too time consuming, forget it! Newsgroups, find one or two you like, subscribe to them and put a shortcut on your desktop. Web sites, definitely. Use cert.org and incidents.org with one or two more, along with the all the vendors of your operating systems that you use in your network for any service packs and hot fixes. How about newsletters and forums: definitely! Use bugtraq and one or two more. Luck? Forget it. Designated Person? Definitely. Find someone you can trust, the more people you can get to rotate through, the better. I suggest that everyone use the same plan to ensure you are getting the information you expect. If you do not think you are getting enough information, change your plan. Make a simple report to summarize, and e-mail to the group. I suggest organizing your bookmarks to point to the places that you choose to keep current with so you can get there quickly. Plan, organize, follow through, and keep current!

Citations:

"Insecure Mailing List Archive" 10/02/00 URL:http://lists.insecure.org/

Martin, Brian. "Full Disclosure: Effective or Excuse?" URL:http://www.synthesis.net/tech/fulldisclosure/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"Public Documents and Projects" URL: http://www.theorygroup.com/Theory/

Graham, Robert. "Hacking Lexicon" 4/02/01
URL:http://www.robertgraham.com/pubs/hacking-dict.html

"News Groups, Mail Lists, and Web Sites"
URL:http://www.infosyssec.net/infosyssec/index.html

"OTHER CONVENTIONS"
09/10/01 URL:www.defcon.org/html/other-conventions.html

Mcclure, Stuart Scambray, Joel Kurtz, George. "Hacking Exposed" Berkeley: Osborne 1999

© SANS Institute 2001, Author retains full rights

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**