Global Information Assurance Certification Paper

Obstacles to – And Workarounds For – Deploying Secure Systems

Craig D. Cox

GSEC Practical Assignment version 1.4b

Abstract

Regardless of the technologies applied by "black hat" attackers and "white hat" systems defenders, both activities their roots in human philosophies and attitudes. Effectiveness depends on understanding the mindsets involved – that is the crux of "social engineering" for the black hats, and it is the major contribution of the Honeynet project to the white hats. Black hat or white, once you understand the thinking of your adversary – and that of the stakeholders who are not direct participants in the conflict – you are in a better position to begin effectively applying technology.

This paper examines mindsets that the author has observed, and how they directly lead to the threats that organizations face. It then examines how frame of mind can be the starting point on which effective defense is built.

Impediments to deploying secure systems

Corporate Culture

A shortcoming I share with (some) other technically-oriented people is to "blame the user." On first examination, many problems can be traced to training issues. Ease of use is always at odds with security, and a good balance is often a matter of perspective. In fact the problem isn't quite that shallow.

The work that brings in a business's money must be suspended when training the people who do that work. In a business such as my employer's, where revenue is directly tied to hours spent in a project-cost (or job-cost, in some industries) structure, the loss associated with training is measurable. And folks aren't shy about measuring. This cost / time awareness seems to foster a grudging attitude towards learning any enhancement, security-related or not. And where the function of a security feature such as a password is specifically to put up a barrier – one that the legitimate user may overcome, but an intruder may not – there is that much more hostility towards making the barrier a difficult one. The executives whose time brings in the most money are the least amenable to training. They avoid losing revenue to class time where possible; however they therefore receive the least value on the technology dollar spent. This includes those dollars spent on defense. It often leaves their accounts and their data the most vulnerable to attack, as well.

Eric Cole's slide show leading into the first day of SANS Track One enumerated a four-point approach towards better security. (They are part of a six-point list that can be found on page 719 of his book “Hackers Beware.”) Two of these, "Know Thy System" and "Defense in Depth" are concepts in which users can (to an extent) participate. From a security standpoint, they should. The more sophisticated (that is, trained) a user is, the better able he or she is to distinguish between an application problem, a network problem, or something which needs the attention of a security

professional. As for Defense in Depth at the user level, one aspires to find users using passwords that are more sophisticated than a single character typed 5 times.

This outline originally also mentioned a "won't happen to us" mentality as contributory to lack of user support. However, during revision the "Blaster" worm made the rounds, raising awareness and illuminating the fact that complacency is cyclical. It is regularly chased away by the next headline-generating security threat. An extended period of normalcy will bring it back. Fortunately the "Blaster" and "SoBig/F" style threats have not yet been frequent enough in our environment to create a "chicken little" effect. The warnings that make it all the way to the major news services are still taken seriously.

Cost delta between white hat & black hat

There are impediments beyond corporate culture, however. There is a very real economic difference between becoming a black hat and a white hat. A would-be identity thief or criminal mischief maker needs little more than a sub-$1,000 computer, internet access, and time to find his way around. There are all sorts of resources aimed at these people – they need not even steal software if they look hard enough! Experienced programmers leave kits and instructions free for download, permitting anyone with criminal intent to cobble together a cookie cutter virus or exploit a sophisticated vulnerability without truly understanding what they're doing. This is why they're called script kiddies – they work from scripts without "deep" understanding. Offense in depth isn't required for defense in depth to be necessary.

(The "real time" nature of the security business is illustrated by the number of events that unfold while a paper such as this is in revision. The previous paragraph was composed editorially, without substantiating references – the etymology of "script kiddie" is an assumption on my part. Articles are now coming out characterizing the teen arrested for the "Blaster.B" variant as a script kiddie. See Antone Gonsalves' article in Internet Week referenced at the end of this paper. Gonsalves, though, speaks merely of a less sophisticated programmer, not one who follows boilerplate or "scripts" when constructing viruses. Even the Webopedia site doesn't outright explain the etymology, but does state that the black hat involved operates "without really understanding what it is s/he is exploiting because the weakness was discovered by someone else".)

Just recently the Honeynet project published evidence that credit card thieves were actually mentoring newbies into the racket, and advertising it as a "lifestyle choice instead of a criminal activity" ("Automated Credit Card Theft", page 2). The utter lack of respect for personal property is astonishing, as is the implied contempt for authority. The reader is reminded of the introductory paragraphs – our problems have their roots in attitudes or beliefs. The Honeynet research reveals that black hats wish to actively propagate their thinking – they are actively educating and rewarding others for being of like mind.

Further illustration of this attitude of contempt by black hats for white hats can be seen in this excerpt from the eWeek article about the CERT leaks last spring:

> [...]"holes are not released to help the admins, they are there to help the hackers and that is who should be using them!"
>
> Hack4life goes on to say that all future vulnerability reports will be released at 7 p.m. on Friday "to give hackers the maximum amount of time to actively exploit the vulnerability before sys-admins, CERT and vendors can act to patch the issue on Monday morning after their weekend off." (Fisher)

The weasel hiding behind the moniker "hack4life" seems to actually want to punish defenders simply for being defenders, and is proudly handing out vulnerability information like candy at Halloween, hoping that the result will be scripts handed to script kiddies before the defenders can react.

Defense in Depth does not come from a script. Defenders must have equipment and time as well, but also in-depth training. Script kiddies can find – or be fed – the chinks in the armor and cookie-cutter instructions on how to pry them open. Defenders need to know the entire system of armor to keep the gaps from being exploited. In other words, a much greater depth of knowledge is needed to defend a system than to attack it.

Because effective mentoring of new defenders must address that need for "deep knowledge", effective mentoring is rarely free. By joining discussion groups, newbie white hats can enjoy the same level of mentoring that newbie black hats enjoy. But by itself, coverage of the latest new exploit is insufficient to defend a system. As Cole points out, thee must Know Thy System in order to defend it effectively. This puts a significantly higher price tag on that white hat the defender wears.

Education is not the only padding on that price tag either. Many white hat tools come at a cost. (The author here makes the assumption that a black hat, who disrespects property so much as to think nothing of breaking and entering a system, will also think nothing of stealing whatever useful software isn't provided for free.) Although there are low-cost and free tools available to the defender, (many of which are well documented in SANS' own reading room), I find that businesses are interested in the level of tech support and warrantee service that comes with paying retail prices.

The SANS reading room also contains Torri Piper's September 10, 2002 work titled "An Uneven Playing Field," under the "legal issues" category. Her excellent discussion of black hat advantages also covers issues specific to law enforcement, which is outside the scope of this paper. I am concerned with the efforts of the defender in a private-sector business, and then more with cause and prevention than with mitigation.

This lack of economic barrier to the black hat, coupled with a teenage sense of derring-do, is a likely source of a great deal of nuisance hacking and script-kiddie virus writing. Not much more than a shrug and a "why not" attitude can lead to a great deal of cleanup work by the defender. See the materials provided by Mich Kabay at <http://www2.norwich.edu/mkabay/ethics/index.htm> as an example of how educators are beginning to identify ethical training as being just as important as technical training. (As this paper was in final draft, SANS NewsBites came out with a pointer to an article on MSNBC addressing this same issue. In the referenced article, Martha Stansell-Gamm compares the formality of driver education and licensing with the lack of comparable technical and legal training for kids before they receive Internet access.)

Administrator Overload

Unless the primary business plan is the sale of IT services, IT services are considered administrative overhead – a cost center upon the ledger, not a profit center. IT is seen as a necessary cost of doing business, and sometimes even as a luxury. Security (as it relates to IT) is a fairly new and sometimes poorly understood field. In cases where IT security awareness has not fully penetrated the executive boardroom, it can be perceived as expendable. Even where wiser thinking prevails, dollars spent are still allocated as a necessary evil, like insurance. It's money you hope to waste, because in a perfect world everyone would be equally (and highly) ethical and it would not be necessary to lock the doors, let alone secure the system.

Add to this baseline perception the brevity of modern software life cycles. The people in many corporate accounting departments remember when IBM, Wang or VAX delivered software that ran for decades without intervention. One unscheduled service interruption a year was grounds for changing vendors. These are the same accounting people who are now watching their corporations bleed dollars every two or three years on the next generation of operating systems, end user software and SQL. IT Security products have built-in features that can solicit updates on a schedule of weeks, days or hours, so as to promptly react to black hat activity. We update our anti-malware so often that a "subscription" model makes sense.

In fact, Kabay argues that the software companies themselves are part of the problem: “Bloated programs are routinely so full of bugs that consumers now think it is normal to pay money for a service release that fixes what never ought to have been released.” ("rant" document.) The down side is that it’s often necessary to select software with an eye towards compatibility with business partners, rather than strictly price and performance. This gives license to those companies with market share to produce substandard software, and backfill with patches.

In addition to bleeding dollars, the spiraling upgrade cycle also adds to the workload of the defender. It cannot be shirked. The price for falling behind in your application software is incompatibility with clients and business partners. For falling behind in operating systems, you can no longer upgrade your hardware at the end of its service life. Try finding Windows 98 video drivers for any computer manufactured in the

last year! Most damagingly, for falling behind in your patches and malware defense, you hand your employer's systems over to the black hats. As I write this paper, 330,000 computers being scrubbed of "Blaster" can attest to this. (Number of infections comes from Poulson in SecurityFocus.com.)

Don MacVittie, in a "security pipelines blog", asserts that the problem of administrative work overload goes deeper still; that instead of being a subspecialty of IT, security should begin to develop its own subspecialties – with full time employees for each – because duly diligent pursuit of any one discipline can take up all of a worker's time. I would suggest, however, that this is somewhat affected by the size of a particular business, and that MacVittie's comments hit the mark mostly at larger corporations. Smaller organizations typically have workers who wear many hats, and the ratio of (overhead) support staff to revenue-generating staff is not casually alterable.

In fact, at least in my experience, operations managers are very focused on such ratios. This tends to place a hard limit on dollars allocated to new sub-fields of IT, especially when IT is itself a new addition to the administrative overhead part of the ledger. At what point does it become cheaper to shut down the network and buy typewriters?

Mitigation / overcoming obstacles

The first section of this paper suggested that the practical problems we face as defenders have their roots in attitudes, perceptions and philosophies. While the solutions aren't as clear, I would suggest that it makes sense that they should also have those same foundations. The progression, in my view, should be understanding, followed by attitude (emotional "buy-in"), then policy. Once policy is firmly established, it can serve as the foundation for all of the efforts of the Network Administrator – including guiding the purchase and implementation of security-related software and equipment.

Corporate Culture

When the Nimda worm hit one week to the day after the September 11 catastrophe, many of us found executive buy-in on a level rarely seen before. Security awareness had officially been raised. Although Nimda was never associated with Islamic fundamentalists, that possibility crossed my mind during initial cleanup. I cannot have been the only one. But it is insufficient, not to mention unwise, to simply scare executives into awareness.

Enthusiastic buy-in should proceed from understanding; understanding not of the technical issues, but that there is a good-guy / bad-guy conflict in progress, and executives are (or have the opportunity to be) high-profile good guys. All they have to do is wear the cape. A further understanding that this is done in the defense of their hard-earned profits ought to be the final selling point. For details on communicating these concepts, the reader is referred to Jeff Hall's "Selling Security to Management" paper in the reading room under "best practices". Once these folks are on board, the

rest of the organization will follow. Good technological defense starts with policy. Chances are that once your executives are on board, policy is not far behind.

The wise security professional will at this point be prepared with some practical suggestions for the organization's newly-convinced policy makers. Two of the first places to visit are user participation in training ("Know thy System") and in Defense in Depth. The latter is most obviously manifest at the user level as a strong, regularly updated password.

When building password policy, consider Mat Newfield's excellent user-friendly method for developing strong passwords, which is included as Appendix A. It will defeat most dictionary attacks and cause brute-force attacks to spend unreasonable amounts of time, and yet with very little practice, users can master the technique.

Cost Delta: Closing the Gap

In addition to providing policy and getting started with practical defense, executives have one other area of participation: providing budget. No matter how thoroughly on-board they are, budget dollars are not going to be unlimited. This is as it should be – what point is there in protecting revenue only to spend it all on the protection? Is it worth buying a burglar alarm, if that burglar alarm is the most expensive and valuable thing in the house?

Some ideas for maximizing the return on security budget include putting training near the top of the list. This is not merely a sop to SANS; training opens the door to some of the low-cost or free-of-charge tools that exist. A well-trained Administrator can counter some of the traditional arguments about warrantees and support by demonstrating self-sufficiency with these tools.

Those tools available are already well documented in the SANS reading room, and it is pointless for me to re-cover that ground. However, in doing research I did encounter a long list of resources posted to a "hacker" newsgroup. These are resources useful to both the black hat and the white hat, and my guess is that the black hats are helping themselves. My suggestion to the defender is to look the list over and use it as well. I have included it as Appendix B.

Although I've argued that black hat style mentoring is inadequate to equip a newbie to provide Defense in Depth, the educated Administrator will find the on-line discussion model to be a tremendous help. The information is much better suited to be a supplement to a deep understanding of systems than as a primary source of information. And as an Administrator becomes more seasoned, he or she ought to be contributing as well as scanning these discussion groups.

It seems odd for me to advocate contribution to discussions when I personally haven't yet done so. I can only promise that as my ability to provide sound answers increases, I will begin "walking the walk" as well. Certainly I already monitor news

sources and discussion areas for answers.

Other early priorities generally include a well-configured firewall and an antivirus defense. Once again, early training (whether from SANS or another respected source) will enable the defender to assess his or her own particular situation and assign priorities more specifically and appropriately. This discussion about the cost advantages of education is not intended to disqualify high-end big-ticket defensive software, but rather to suggest how to work within realistic budget constraints. Where budget is sufficient and specific need exists, there's nothing wrong with getting a high-end system.

Training can, and should, be spread around in an organization. Complacency can be counteracted with communication. Not "chicken-little" style hype, but (for example) lunchtime presentations focusing on brief topics. Topics to consider (remembering Hall's criteria for customizing topics to audience) could include:

- How to identify hoax e-mail, and / or virus bait in an e-mail (which are obviously related topics).
- Newfield's password-building tips, covered previously.
- A tour of Zone Alarm or similar software for the benefit of home PC owners.
- Home PC Safety tips for those with children on home computers. (You might contact Cyber Angels <www.cyberangels.org> for assistance with this. Most of their source material is for presentations longer than one hour, but it might be adapted for such use.)
- Sessions in which the relationship between threats and policy are discussed, to foster understanding, and therefore a more enthusiastic cooperation with the policy.

This last talking point is borrowed from one of Mich Kabay's newsletters, where he argues that reasons for policies should be embedded within the policies themselves, so that people are not made to feel "ordered about with arbitrary rules." The corollary then is that if you can't relate a policy directly to a threat, it may be a clue that your policy isn't helpful and could use a bit of re-working.

The point here is not that SANS students should go right back to work and parrot our training. The important point is that we are in a unique position to educate our co-workers about things that matter to them, and importantly, promote security awareness.

Administrator Overload

This is the most challenging point on which to offer suggestions. Thus far I have advocated intensive training; an almost evangelical education campaign starting with upper management and going through lunch-and-learn sessions for co-workers; participation in group discussions with people from outside organizations; and learning low- or zero-cost software tools that may have indifferent documentation. On the surface, these are not conducive to reducing the workload.

When examined as long-term investments, however, these activities might be defended as time-savers. Arguably, educated co-workers might cut down on a Network Administrator's security work. A google search will often keep you from reinventing the wheel, and if so, is a 20-minute answer to someone else's question truly time lost?

MacVittie argued that security staff needed to sub-specialize, to focus more narrowly in order to have the time to get the job done. I responded that this was a luxury for large organizations. However, discussion boards with active, knowledgeable participants can bring a sort of "virtual" extra employee into a small organization. This virtual tech is highly specialized in whatever skill happens to be needed, and is on call whenever the Internet is available. This perhaps begs the question, why should we give our time away on these boards? Are we undermining the turf of the consultant?

It's unlikely that the consultant will go extinct, so long as they're prepared to do deeper analysis than can be found on-line. The reason to contribute time is simply to keep the resource active, against the day when we have a need for it. If we abandon it, it will become the exclusive domain of the black hat.

The earlier reference to Cyber Angels' resources brings up another important time-saving point: Many security-minded organizations have presentation materials available, and wish to contribute simply to improve general awareness. There's certainly no sense in making extra work when these packaged presentations are out there. Watch for them (and pre-packaged solutions of any sort), and use them whenever appropriate.

Watch for other helpful trends, and support them where possible. For example, purchase IPv6 equipment where it is not too much more expensive than comparable IPv4 equipment. This may not immediately bring the full benefits of IPv6 to your organization, but you'll be ready when your ISP makes the jump.

The usual time management bromides also apply, of course. You cannot expect to give presentation to the Board on Monday morning, conduct a lunch-and-learn during the noon hour, have policies published by three and go into a suitably cushy job on Tuesday. Expect to parcel things out over time, and expect to have to continue juggling tasks until the long-term benefits begin to show themselves.

One final point about organization: Research for this paper has brought to my attention a ton of resources. (See the aforementioned Appendix B to this paper. Reference is also made to Appendix H of the SANS Track 1 text, SANS Security Essentials with CISSP CBK, which is not repeated here.) Most modern browsers have a "folder" feature for organizing the bookmarks (or "favorites" if you prefer). If you keep up with the organization of these, they are invaluable to helping you put your finger on that web site, that article, that tool you sort of half remember finding. These bookmarks should be regularly backed up (along with everything else!) to outside media. Most browsers, again, have an export feature. I incorporate the date into my file name when I do an export-as-backup, so I can tell at a glance if a bookmark list is recent.

Other things I have found helpful include a PDA. It should not be necessary to state that the PDA should not carry sensitive information such as passwords; however, it's fair game for most other reference material. Before PDAs were economically available I found myself carrying loose-leaf binders full of reference information. These days I don't necessarily need photocopies of hard disk jumper settings, but a reference of port numbers, clever configuration tips & tricks found on google, and other organization-specific reminders will fit nicely in a shirt pocket rather than in an inconveniently large binder.

Finally, with a CD burner and a modest investment in blank CDRs, one can also carry licensed or freeware tools to client workstations where needed. If the machine on which the tools were burned to CD is known good, as are the tools, they are an invaluable resource during virus incident cleanup because the CD cannot be compromised. This is an advantage over carrying those same tools on the newer USB flash drives, although these devices are handy as well.

Summary / Conclusion

The variety of security issues facing us as Network Administrators largely have their roots in attitudes and perceptions. These included the uninformed lack of perception in the management of some organizations, and the galling antisocial attitudes of virus authors, script kiddies, crackers, and other fancifully named digital thugs. Industry pundits suggest that vendor focus on short-term profit over user benefit contributes to security issues. The increasingly unmanageable workload of the defending Administrator is also an obstacle.

Solutions proposed have included effective communication within corporations, on the theory that "forewarned is forearmed" and executive management will react helpfully to clear information; the notion that formal training opens the door to a large number of additional solutions; and a few pointers for dealing with excessive workload were hesitatingly offered. The reader should know, when absorbing that workload advice, that I don't currently enjoy a great deal of slack time at work and that I am speaking more from hopeful analysis than from experience. A small number of tools and processes that I personally have found helpful were also mentioned.

Whatever the other answers are, the most important one is communication. The white hat community must be exactly that – a community of people who interact, and "provide for the common defense." The black hats are certainly cooperating with each other, and they have a pronounced head start.

Appendix A: Mat Newfield's Password Protocol

The following information is pasted from an e-mail sent to me by SANS instructor Mat Newfield, who was kind enough to follow up by e-mail on a lecture point presented at SANS Inner Harbor, 2003. It is only lightly edited:

> Pick a phrase. Using the phrase and the rules that follow you will build a password. In this example, the phrase was "gone fishing".
>
> Use just the first and last letter of each word in the phrase. (phrase becomes "gefg")
>
> All "e"s are changed to 3
> All "i"s are changed to 1
> All "o"s are changed to 0
> All "a"s are changed to @
> A ! precedes the first character and at the end of the phrase
>
> ...following this procedure, the phrase is now "!g3fg!"
>
> Now you can add the different login situations to the end or middle or beginning of the phrase. For example for network based logins add "network" to the phrase. The phrase is turned into "!g3fgnk!".
>
> Now require quarterly changes. Since it is now summer the phrase is turned into "!g3fgnksr!"

When you begin to get creative with Newfield's rules, such as letting users pick their own leading and trailing special characters, or changing only odd-numbered "a" characters to "@", the password is hardened even further.

Appendix B: Usenet Post of Resource Links

What follows, astonishingly, is longer than the actual paper to which it is appended. It is a pasted list of links posted pseudonymously to a hacker news group. The links are offered to the newsgroup's readers irrespective of whether they happen to be "white hats" or "black hats." In fact, some of the newsgroups cross-posted, and some of the resource descriptions, imply that this may be a black hat addressing primarily other black hats.

The lack of identifying information makes proper citation difficult; the reader is therefore explicitly advised that the author of this paper takes no credit. The posting is provided because it appears to be an exhaustive list of resources of interest to defenders as well as attackers. The font is changed to courier to reflect its display in the google listing, as well as to distinguish it from the rest of this paper.

```
From: Lord Shaolin (abuse@127.0.0.1)
Subject: Security, Hacking, Encryption, Programming and Various
other links [LONG]
Newsgroups: alt.hacker, alt.hackers.malicious, alt.hacking,
alt.ph.uk
View: Complete Thread (23 articles)
Original Format
Date: 2003-08-24 14:08:21 PST

UPDATED: Added anti-virus software, personal firewall list,
commercial
firewall list and re-organised programming section.

Security Links

§ Good upcoming security forum http://www.security-forums.com
§ A totally HUGE security archive http://neworder.box.sk/.
§ Current and archived exploits
http://www.securiteam.com/exploits/.
§ 'Underground' search engine http://www.warez.com/.
§ Default logins for all sorts of devices
http://www.mksecure.com/defpw/.
§ One of the top mainstream security sites
http://www.securityfocus.com/.
§ TESO Computer security http://teso.scene.at/.
§ Asian security group, lotsa advisories
http://www.shadowpenguin.org/.
§ w00w00 Security development http://www.w00w00.org/.
§ USSR a strong security group http://www.ussrback.com/.
§ Good all around security site
http://www.packetstormsecurity.nl.
```

§ SANS Security Institute with articles on EVERYTHING
http://www.sans.org/.
§ A Fairly immense WWW security FAQ
http://www.w3.org/Security/Faq/.
§ Computer Security Encylopedia http://www.itsecurity.com/.
§ Java Security informationhttp://java.sun.com/security/.
§ Help Net Security http://www.net-security.org/.
§ Security Search Engine http://searchsecurity.techtarget.com/.
§ FreeBSD security information http://www.freebsd.org/security/.
§ Netscape security information
http://home.netscape.com/security/.
§ Linux security community centre http://www.linuxsecurity.com/.
§ Dutch Security Information Network http://www.dsinet.org/.
§ A once great site from a white hat hacker
http://www.antionline.com/.
§ Network Security Library http://secinf.net/.
§ Infamous happy hacker http://www.happyhacker.org/.
§ Infosec papers and articles http://www.infosecwriters.com/
§ The BIGGEST security/privacy/crypto software archive
http://www.wiretapped.net/
§ The Info Sec Bible http://www.securityflaw.com/bible
§ Government Incident Advisory service http://www.ciac.org/ciac/
§ The ultimate resource for all security tools
http://www.networkintrusion.co.uk

Privacy and Anonymity

ÿ All about privacy http://www.privacy.net.
ÿ Well known privacy/security portal http://www.cotse.com
ÿ Anonymity, privacy and security
http://www.stack.nl/~galactus/remailers/.
ÿ Free, anonymous web surfing http://www.anonymizer.com/.
ÿ IDSecure service http://www.idzap.com/.
ÿ News, information and action http://www.privacy.org/.
ÿ Sam Spade Tools http://www.samspade.org/t/.
ÿ International PGP homepage http://www.pgpi.org.
ÿ Encryptable web-mail http://www.hushmail.com/.
ÿ Anonymity software http://www.skuz.net/potatoware/.
ÿ REALLY delete your data
http://www.cs.auckland.ac.nz/~pgut001/pubs/.
ÿ Anonymous access http://www.safeproxy.org/.
ÿ Web privacy http://www.rewebber.de/.
ÿ Web anonymiser list http://mikhed.narod.ru/en/free_proxy/cgi-
proxy.htm
ÿ JAP http://anon.inf.tu-dresden.de/index_en.html

Cryptography & Encryption

æ All about RSA http://www.rsasecurity.com/.
æ Cryptography Archives http://www.kremlinencrypt.com/.
æ Cryptography links http://cryptography.org/freecryp.htm.
æ Cryptography Info http://world.std.com/~franl/crypto/.
æ DriveCrypt http://www.e4m.net/.
æ CCIPS http://www.cybercrime.gov/crypto.html.
æ Cryptography resource http://www.crypto.com/.
æ Bruce Schneier's operation http://www.counterpane.com
æ Huge Crypto archive http://www.cryptome.org
æ An upto date thread containing crypto links
http://www.security-forums.com/forum/viewtopic.php?t=4761
æ Various info mainly on PGP http://www.skuz.net/.

Linux/BSD/UNIX

î http://www.linux.org.
î http://www.redhat.com .
î http://www.debian.org.
î http://linux.pagina.nl.
î http://www.linux.com.
î http://www.linux-mandrake.com/.
î http://www.slackware.com.
î http://www.linux-firewall-tools.com/linux/.
î http://www.suse.com/.
î http://linux.box.sk.
î http://www.linuxiso.org/.
î http://www.distrowatch.com/.
î http://www.freebsd.org.
î http://www.openbsd.org.
î http://www.netbsd.org.
î http://wwws.sun.com/software/solaris/binaries/index.html
î http://www.gentoo.org/
î http://www.turbolinux.com/
î http://www.lycoris.com/
î http://www.lindows.com
î http://www.trustix.net/
î http://www.yellowdoglinux.com/
î http://www.knopper.net/knoppix/

Zines & Texts

ü Great UK Zine http://www.f41th.org/.

ü 2600 The hacker quarterly http://www.2600.com/.
ü Massive Tutorial selection
http://www.tutorialfind.com/tutorials.
ü Online book collection
http://www.maththinking.com/boat/booksIndex.html.
ü Internet FAQ archive http://www.faqs.org/.
ü The Linux documentation Project http://www.tldp.org/
ü Another fine member of the box network http://black.box.sk.
ü Even more info from the box network http://blacksun.box.sk.
ü Internet How To archive http://www.howtos.nl/.
ü 45,000 text files old skool style http://www.textfiles.com.
ü Linux Networking Overview http://www.ibiblio.org/mdw/HOWTO/.
ü Currently the only Defacement mirror http://www.zone-h.org/.

Virii/Trojans & Firewalls

¿ Trojan archive http://packetstormsecurity.nl/trojans/.
¿ Fearless, everything Trojan http://www.areyoufearless.com/
¿ Up to date Trojan archive http://www.trojanforge.net/
¿ A good archive with info on each one
http://www.dark-e.com/archive/trojans/index.shtml
¿ Sub7's official Home Page http://www.sub7.net/
¿ Another comprehensive Trojan archive
http://www.tlsecurity.net/amt.htm.
¿ Home of BackOrifice http://www.cultdeadcow.com/.
¿ Huge Trojan removal database http://www.anti-trojan.org/.
¿ Excellent Anti-Viral software and Virii Database
http://www.sophos.com/.
¿ Mcafee's Searchable Virus Information Library
http://vil.mcafee.com/.
¿ Firewall Guide http://www.firewallguide.com/.
¿ Firewall FAQ http://www.interhack.net/pubs/fwfaq/.
¿ Firewall How To http://www.grennan.com/Firewall-HOWTO.html.
¿ Squid http://www.squid-cache.org/.
¿ Excellent virus news and info http://www.antivirus-
online.de/english/.
¿ The ULTIMATE IPTables resource
http://www.linuxguruz.org/iptables/.

Tools

Security

» THE ultimate port scanner nmap. http://www.insecure.org/
» The one and only NT password cracker l0phtcrack 3.

http://www.atstake.com/research/lc/
» Get the latest version of john the ripper.
http://www.openwall.com/john/
» Windows process listener
Inzider.http://www.ntsecurity.nu/toolbox/inzider/
» hping craft those packets http://www.hping.org/
» Netcat, hackers swiss army knife
http://freshmeat.net/projects/netcat/
» TCPDump for packet aquisition http://www.tcpdump.org/
» The ONLY packet sniffer http://www.ethereal.com/
» Firewalk http://www.packetfactory.net/firewalk/
» Network grep http://www.packetfactory.net/projects/ngrep/
» Fragrouter
http://packetstormsecurity.nl/UNIX/IDS/nidsbench/fragrouter.html
» The best OS fingerprinter http://www.sys-
security.com/html/projects/X.html
» Fport port mapper
http://www.foundstone.com/index.htm?subnav=resources/navigation.
htm&subcontent=/resources/proddesc/fport.htm
» Tripwire Integrity checker http://www.tripwire.org/
» Check for rootkits http://www.chkrootkit.org/
» Open source intrusion detection http://www.snort.org/
» Security Scanner http://www.nessus.org/
» Paketto toolkit
http://www.doxpara.com/read.php/code/paketto.html
» Ettercap multipurpose sniffing
http://ettercap.sourceforge.net/
» Whisker CGI Scanner http://sourceforge.net/projects/whisker/
» Another huge CGI scanner http://www.cirt.net/code/nikto.shtml
» Kismet 802.11 sniffer http://www.kismetwireless.net/
» Airsnort the original WLAN sniffer http://airsnort.shmoo.com/
» NBTScan, NetBIOS network name scanner
http://www.inetcat.org/software/nbtscan.html
» Honeyd, your own honeydaemon
http://www.citi.umich.edu/u/provos/honeyd/
» STunnel, secure SSH wrapper http://www.stunnel.org/

Anti-virus

» Sophos - Good cross platform AV, updates can be a problem
http://www.sophos.com/
» AVG Anti Virus - Provides a free AV solution, technically
strong
http://www.grisoft.com/
» Panda Software Includes a free online anti-virus scanner for
Windows
http://www.panda-software.com/

» Mcafee - Well it's ok http://www.mcafee.com/
» Norton - Standard AV solutions for Windows, Corporate editions of both
(Norton and McAfee) are reasonable http://www.symantec.com/
» Kaspersky - My preferred AV solution, the most technically capable AV
engine http://www.kaspersky.com/
» NOD32 - Small company, but technically strong. Slow on updates http://www.nod32.com/
» Trend/PcCillin - Has improved a lot lately, also provides online scanner
http://www.trendmicro.com/
» Vet - Australian AV vendor http://www.vet.com.au/
» Norman - No experience of this one. http://www.norman.com/
» F-Secure - Very technically powerful software with a long history.
http://www.f-secure.com/
» Bitdefender - Also has a free AV version with online scan. http://www.bitdefender.com/
» OpenAntiVirus - Open source AV solution.
http://www.openantivirus.org/

Personal Firewalls

» Kerio Personal Firewall -
http://www.kerio.com/us/kpf_home.html
» ZoneAlarm - http://www.zonelabs.com/
» Tiny Personal Firewall - http://www.tinysoftware.com/
» BlackIce - http://blackice.iss.net/
» Sygate Personal Firewall Pro -
http://smb.sygate.com/products/spf_pro.htm
» Agnitum Outpost - http://www.agnitum.com/products/outpost/
» Mcafee Personal Firewall -
http://www.udsl.com/www.mcafee.com/myapps/firewall/ov_firewall.asp
» Norton Personal Firewall -
http://www.symantec.com/sabu/nis/npf/
» PrivateFirewall - http://www.privacyware.com/PF.html
» Armor2Net - http://www.armor2net.com/
» ETrust EZ Firewall - http://www.my-etrust.com/products/Firewall.cfm
» Freedom Firewall -
http://www.freedom.net/products/firewall/index.html
» Preventon -
http://www.freedom.net/products/firewall/index.html
» Steganos Online Sheild -
http://www.steganos.com/en/sos/index.htm

» Kasperksy Anti-Hacker -
http://www.kaspersky.com/buyonline.html?chapter=964564
» Visnetic -
http://www.deerfield.com/products/visnetic_firewall/
» Norman Personal Firewall -
http://www.norman.com/products_npf.shtml

Linux based firewall solutions

» IPCop - http://www.ipcop.org/ (My favourite)
» Clark Connect - http://www.clarkconnect.org/
» Smoothwall - http://www.smoothwall.org/
» Dubbele - http://www.dubbele.com/.
» Astaro Security Linux - http://www.astaro.com/
» IGWall -
http://www.infoguard.ch/en/templates/TmpFreestyle.cfm?contentID=
1&um1ID=70
» LRP - http://www.linuxrouter.org/
» E-smith - http://www.e-smith.org/
» ClosedBSD - http://www.closedbsd.org/index.html%20
» FloppyFW - http://www.zelow.no/floppyfw/
» Freesco - http://www.freesco.org/
» TheWall - http://thewall.sourceforge.net/
» LEAF - http://leaf.sourceforge.net/ (the best of the floppy
lot)

Commercial Firewall solutions/Appliances

» Netscreen - http://www.netscreen.com/
» Watchguard - http://www.watchguard.com/
» SonicWall - http://www.sonicwall.com/.
» Barricade - http://www.privador.com/?op=body&id=13
» Nokia - http://www.nokia.com/securitysolutions/
» Checkpoint - http://www.checkpoint.com/
» Cisco PIX - http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/
» Spearhead - http://www.sphd.com/
» Protectix Prowall - http://www.protectix.com/
» Microsoft ISA - http://www.microsoft.com/isaserver/
» Symantec Enterprise Firewall -
http://enterprisesecurity.symantec.com/products/products.cfm?pro
ductid=47&EID=0

Scene

µ The only scene site you need http://www.stolemy.com/
(ISOnews).
µ Check out the quality http://www.vcdquality.com

µ VCD site http://www.vcdhelp.com/.
µ Great site for Dreamcast stuff http://www.dccopyworld.com/.
µ The BEST for serials, cracks and keygens
http://astalavista.box.sk/.
µ The best site for free DVD software http://www.dvdsoft.net.
µ Massive scene archive, easily as good as isonews
http://www.nforce.nl

News Groups

A great source of information, discussion and answers to
questions
(or flames) depending how you put them ;)

ñ alt.hacking.
ñ alt.binaries.hacking.beginner.
ñ alt.computer.security.
ñ alt.security.
ñ alt.os.security.
ñ alt.security.pgp.
ñ alt.security.pgp.patches.
ñ comp.os.linux.security.
ñ comp.os.ms-windows.nt.admin.security.
ñ comp.security.unix.
ñ comp.security.pgp.backdoors.
ñ comp.security.unix.
ñ microsoft.public.security.
ñ microsoft.public.sqlserver.security.
ñ microsoft.public.win2000.security.

'Legal' Hacking

Ð Hack me http://loginmatrix.com/hackme/.
Ð Try2Hack http://www.try2hack.nl/.
Ð Hack3r/Roothack http://roothack.org/.
Ð Pull The Plug http://www.pulltheplug.com/.
Ð Root wars http://rootwars.org/.
Ð Hackers lab http://www.hackerslab.org/.
Ð Datafort http://hack.datafort.net/
Ð Arcanum, Hard! http://www.arcanum.co.nz/
Ð NGSec Challenge http://quiz.ngsec.biz:8080/

Programming

General

Scripts, Source and Books http://www.scriptsearch.com/.
Programmers Heaven http://www.programmersheaven.com/.
Loads of tutorials http://www.echoecho.com.
Plenty of Web Development scripts http://www.hotscripts.com.
Code for everything http://www.planet-source-code.com/
Freshmeat OS projects http://freshmeat.net
Sourceforge! The ultimate http://sourceforge.net
Thousands of HowTo's http://www.howtos.nl
MS Development Centre
http://search.microsoft.com/us/dev/default.asp
Excellent Programmers tools archive http://protools.cjb.net
PC Programming information
http://www.epanorama.net/links/pc/programming.html
3000+ Programming resources
http://stommel.tamu.edu/%7Ebaum/programming.html

JAVA & JavaScript Resources

Java & Internet Glossary http://www.mindprod.com/jgloss.html.
Java homepage http://java.sun.com/.
Absolute Java FAQ http://www.javafaq.nu/.
Thinking in Java http://www.mindview.net/Books/TIJ/.
JavaScript Resource http://www.javascript.com.
JavaScripts,tutorials & references
http://javascript.internet.com/.

C/C++ & UNIX/Linux programming

UNIX programming links
http://www.cs.buffalo.edu/%7Emilun/unix.programming.html
UNIX programming FAQ
http://www.erlenstar.demon.co.uk/unix/faq_toc.html
UNIX Sockets in C FAQ http://www.manualy.sk/sock-faq/unix-socket-faq.html
Mostly C/C++ information http://vasyaa.tripod.com/
C Course http://www.strath.ac.uk/IT/Docs/Ccourse
Another good C course
http://www.eskimo.com/~scs/cclass/notes/top.html

PHP Resources

PHP home page http://www.php.net.
PHP from hotscripts http://www.hotscripts.com/PHP/.
PHP resource index http://php.resourceindex.com/.
PHP FAQ's http://www.faqts.com/.
PHP Developer resources http://www.phpbuilder.com/.

Building dynamic sites with PHP http://www.phpwizard.net.
PHP Developer network http://www.evilwalrus.com/.
PHP Tutorials and more
http://www.thescripts.com/serversidescripting/php.
PHP and MySQL tips and tutorials
http://www.sitepoint.com/subcat/98
Webmonkey PHP resource
http://hotwired.lycos.com/webmonkey/programming/php/index.html
Zend PHP tutorials http://www.zend.org/zend/tut/
Applied OO PHP http://www.horde.org/papers/kongress2002-
design_patterns/
PHPPatterns http://www.phppatterns.com/
PHPArena http://www.phparena.net/
How do I make skins? http://www.domesticat.net/skins/howto.php
PHPGuru http://www.phpguru.org/

ASP Resources

ASPTear
http://www.alphasierrapapa.com/IisDev/Components/AspTear/.
ASP Codes and techniques http://www.asptoday.com/.
ASP, HTML, SQL and more http://www.w3schools.com/.
Think ASP think... http://www.4guysfromrolla.com/.
ASP 101 http://www.asp101.com/.
ASP developers site http://haneng.com/.

PERL Resources

PERL Archive http://www.perlarchive.com/.
PERL tutorials http://www.perlmonks.org/index.pl?node=Tutorials.
Old school PERL programming http://www.cgi101.com/.

Databases/SQL

MySQL home http://www.mysql.com.
PostgreSQL home http://www.postgresql.org/.
Firebird http://sourceforge.net/projects/firebird/
Various Others

Windows programming tools http://www.programmerstools.org/.
The art of Assembly
http://webster.cs.ucr.edu/Page_asm/ArtofAssembly/0_ArtofAsm.html
Python homepage http://www.python.org/.
Object Oriented Programming http://www.oopweb.com/.
XML 101 http://www.xml101.com.
Dev-X XML zone http://www.devx.com/xml/.

Search Engines

þ The daddy of all search engines http://www.google.com.
þ Web index pioneer http://www.yahoo.com.
þ Huge numbers of results, relevance questionable
http://www.altavista.com.
þ C-net's offering http://www.search.com.
þ Pretty good http://www.dogpile.com.
þ Touted as the fast search http://www.alltheweb.com.
þ The Wolf-Spider, also owns Hotbot below http://www.lycos.com/.
þ Parallel scalable searching http://www.hotbot.com/.
þ One of the best also owns entry below http://www.excite.com/.
þ Easy to use http://www.webcrawler.com/.
þ Maybe remembered as Goto.com http://www.overture.com/.
þ Not as good as it once was http://www.infoseek.com/.
þ Popular with beginners http://www.mamma.com/.
þ Paid listing search engine http://www.northernlight.com/.
þ Answers your questions *sometimes* http://www.ask.com/.
þ IMO *THE* best place for finding definitions
http://whatis.techtarget.com/.
þ RFC search http://www.rfc-editor.org/.
þ Search the search engines http://www.metacrawler.com/.
þ Netscape Netcenter http://www.netcenter.com/.
þ FTP Search http://www.alltheweb.com/?cat=ftp&cs=utf-
8&q=&_sb_lang=en.
þ Shareware/Freeware Engine http://www.tucows.com.
þ Another Shareware/Freeware Engine http://shareware.cnet.com.
þ Freeware site http://www.brothersoft.com/.
þ Good Freeware site with reviews http://www.webattack.com/.
þ A piece of software, but excellent for searches
http://www.copernic.com/.

I bet you didn't know there were so many ;)

Others

¥ No longer hosting defacements but still good
http://attrition.org/.
¥ General news for nerds, also has security content
http://slashdot.org/.
¥ Excellent site for everything Computer http://www.zdnet.com/.
¥ The New Hackers Dictionary http://www.tuxedo.org/~esr/jargon/.
¥ How to become a hacker http://www.tuxedo.org/~esr/faqs/.
¥ Can't spell? One of my favourite ever sites
http://www.dictionary.com.

¥ Rightly ripping GRC.com http://www.grcsucks.com/.
¥ Also GRC it's self does have *some* good stuff
http://grc.com/.
¥ The best IT related news site http://www.theregister.co.uk.
¥ The best all around news site http://news.bbc.co.uk/.
¥ Cyberarmy, home of various h4x0r stuff
http://www.cyberarmy.com/.
¥ Excellent place for finding ALL kinds of software
http://sourceforge.net/.
¥ Intelligence Brief http://www.intelbrief.com/.

Online at http://www.darknet.org.uk and http://www.udsl.com

Cheers

ST
-

.: http://www.security-forums.com :.

Share your knowledge
It's a way to achieve
Immortality.

Works Cited

Cole, Eric. Hackers Beware. New Riders Publishing, 2001.

Gonsalves Antone. “Experts Say The MSBlaster Author Is A 'Script Kiddie'.” Internet Week.com August 29, 2003. Accessed September 1, 2003. <http://www.internetweek.com/story/showArticle.jhtml?articleID=14200106>

Webopedia accessed September 1, 2003 <http://www.webopedia.com/TERM/s/script_kiddie.html>

“Profile: Automated Credit Card Fraud.” June 6, 2003 The HoneyNet Project. Accessed July 30, 2003. <http://www.honeynet.org/papers/profiles/cc-fraud.pdf>

Fisher, Dennis. “More CERT Documents Leaked.” Eweek.com. March 29, 2003. Accessed September 1, 2003. <http://www.eweek.com/article2/0,3959,962697,00.asp>

Piper, Torri. “An Uneven Playing Field” September 10, 2002. SANS InfoSec Reading Room. Accessed July 30, 2003. <http://www.sans.org/rr/paper.php?id=115>

Kabay, Mich. "Ethics." Mich Kabay's Home Page. Accessed September 10, 2003. <http://www2.norwich.edu/mkabay/ethics/index.htm>

"Justice Official Calls For Parents To Educate Children On Cyber Ethics." SANS NewsBites Vol. 5 No. 36. September 10, 2003. Archive not posted as of 9/10/03, presumed future URL: <http://www.sans.org/newsletters/newsbites/vol5_36.php>

Stansell-Gamm, Martha. "My Turn: There’s One More Talk You Need to Have." September 15, 2003 issue. MSNBC.com. Accessed September 10, 2003. <http://www.msnbc.com/news/962420.asp>

Kabay, Mich. “A Rant about INFOSEC.” 1999. Mich Kabay’s Home Page. Accessed September 4, 2003. <http://www2.norwich.edu/mkabay/infosecmgmt/rant.htm>

Poulsen, Kevin. “The Bright Side of Blaster.” August 14, 2003 SecurityFocus HOME News. Accessed September 1, 2003. <http://www.securityfocus.com/news/6728>

MacVittie, Don. “Don’t Drive Your Security Staff Nuts.” August 21, 2003. Security Pipeline Trends. Accessed September 1, 2003. <http://www.securitypipeline.com/trends/index.jhtml;jsessionid=2ADFF2C3BLOTWQSNDBGCKHY>

Hall, Jeff. “Selling Security to Management” July 25, 2001. SANS InfoSec Reading Room. Accessed September 2, 2003.

<http://www.sans.org/rr/paper.php?id=393>

Newfield, Mat. <mnewfield@trusecure.com> “RE: Question from SANS Inner Harbor”. E-mail to Craig Cox <cox@rlf.com> August 20, 2003

“Offline Programs.” Cyber Angels. A program of The Guardian Angels. <http://www.cyberangels.org/homefront/offline.html> Accessed September 4, 2003.

Kabay, Mich. “Elements of Security Policy Style, Part 1”. NW on Security. (electronic newsletter available in archive from <http://www.nwfusion.com/newsletters/sec/2003/0721sec2.html>) July 24, 2003.

Lord Shaolin (online pseudonym, identity not provided). "Security, Hacking, Encryption, Programming and Various other links [LONG]." Usenet posting. 24 August 2003. Alt.hacking. Accessed September 3, 2003, via google groups.