

Re: comp.security.unix and comp.security.misc frequently asked questions

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2002-12/0099.html>

From: Bahekelwa S Imatha (bisoph@surfbest.net)

Date: 12/26/02

From: "Bahekelwa S Imatha" <bisoph@surfbest.net>

Date: Wed, 25 Dec 2002 21:02:09 -0500

POURQUOI LA FOI EN JESUS CHRIST

Tout homme est mortel, c'est une hypothèse à laquelle l'antithèse est impensable. La vie après la mort par contre partage les avis des communs de mortel. Le matérialisme tend à réduire toute la réalité à la matière, celle-ci dans cette optique suffit à rendre compte des phénomènes vitaux et psychiques. Par conséquent, l'homme n'est en rien différent des substances dont sont fait le corps perçu. La vision spiritualiste quant à elle, affirme chez l'homme un principe substantiel ou essentiel intrinsèquement indépendant de l'organisme. En ceci il y a lieu de prendre l'homme comme tout entier spirituel, infini, éternel habité par le désir de la perfection, mais limité par le corps dont il a à se débarrasser.

Tout compte fait, sans aucune prétention de juger les opinions, à la croisée des tendances, ci-haut évoquées, il convient de souligner l'embarras qu'il y a à considérer l'âme et le corps comme deux principes indépendants l'un de l'autre. L'homme comme simple corporéité, est un objet biologique et animal comme tant d'autres. Or l'homme est fondamentalement un être spirituel qui parle, qui pense, qui maîtrise la nature et qui finit par s'impliquer lui-même dans son activité productrice. Toutefois, la conscience dont l'homme est doté n'est pas de ce monde, il est idéal. Ainsi donc, l'homme vit dans son corps, il a son corps mais il n'est pas son corps. Il constitue un point de rencontre entre le monde et la transcendance.

Ce que nous pouvons retenir c'est que l'homme comme conscience est spirituel, opposé à une masse opaque et pleine. Grâce à la conscience, il est capable de voltiger au-delà du corps, se projeter dans l'avenir et bondir dans le passé.

Cette méditation veut nous interpeller à oser cette gymnastique de l'esprit, c'est adire nous poser ces questions existentielles quelles que bêtes soient-elles : d'où suis-je venu ? Qui suis-je ? Que puis-je espérer ? . Bien que souvent ces questions demeurent sans réponses nous ne manquerons pas de solliciter votre réponse ne fut-ce que pour ce dernier aspect : « Que puis-je espérer ? »

Voilà le tremplin, espérer, qui nous plonge justement dans l'avenir. L'espérance est censée avoir un objet sans lequel le mot est vide de sens. Nul ne peut vivre sans espérance d'autant plus qu'un sujet sans espérance est en proie à l'angoisse, c'est-à-dire, une crainte irrésistible d'un mal

imminent. Il se crée une situation de fuite. Fuite dans les plaisirs, fuite dans les principes moraux ou religieux, comme le yoga, le stoïcisme. fuite dans l'indifférence avec l'homme comme l'absolu. Entendons par là être qui existe par lui-même et dont tout dépend. Cependant, la fuite offre malheureusement une sécurité illusoire entre éphémère. L'exemple banal que nous pouvons considérer est l'expression courante « noyer son souci dans un verre d'alcool » nous nous demandons si c'est le verre d'alcool qui se noie dans le souci ou c'est le souci qui se noie dans le verre d'alcool. On peut oublier momentanément un problème, mais est-ce oublier résoudre le problème ? Le médecin n'utilise-t-il pas l'anesthésie pour traiter un patient ? Mais est-ce la douleur s'arrête par-là ? .

Le grand problème du cœur humain consiste à trouver l'objet de sa réelle espérance Autrement dit, l'homme a besoin de la sécurité interne. D'emblée on serait tenté de croire que l'aisance matérielle suffit pour répondre au grand désir du cœur humain. Mais d'où vient que la sagesse populaire dise que l'argent ne fait pas le bonheur ? Il n'y a rien d'étonnant si on voyait l'homme même le mieux nanti cherchant opiniâtement le bonheur même dans les livres. On aimerait bien se confier en un homme puissant de ce monde pour entre heureux. Mais l'homme est fini et limité. Il s'efface comme une vapeur et aussitôt même la place qu'il occupait ne reconnaît plus.

En dernière analyse, la confiance en un homme n'est que déception. Par conséquent, l'objet d'un désir éternel est éternel C'est Dieu.

Comment accéder à Dieu pour la sécurité de notre cœur ?

La seule source qui nous parle de Dieu et son amour c'est la bible> dans ce livre Dieu se révèle comme un DIEU D'AMOUR. Son amour est offert à tout le monde par Jésus-Christ. Selon l'évangile de Jean 3 : 16, cependant tout le monde ne sait pas expérimenter cet amour par ce que l'homme pécheur est séparé de Dieu, pourtant Dieu a créé l'homme pour vivre en relation avec lui mais l'homme a préféré son indépendance.

La conséquence de ce choix ce fut la rupture de la relation entre l'homme et Dieu. C'est ce que la Bible appelle péché. Marcher selon le désir de son cœur, faire sa propre volonté.

D'autre part l'homme n'est en aucune manière neutre. Comme dire Martin Luther, s'il n'est pas mené par Dieu, il l'est par le diable, l'ange révolté. Donc l'inimitié avec Dieu c'est l'amitié avec le Diable. Ce dernier offre un substitut pour tout ce qui est de Dieu. Par exemple à la place de la Bible, il donne les livres de magie, le tirage des cartes, l'horoscope .Il remplace la prière par les formules magiques, des malédictions, au lieu de l'église il propose des cercles magiques, des boîtes des obscènes etc. , les guérisons par la foi, il les remplace par des incantations des faux guérisseurs.

Du reste, l'homme séparé de Dieu est spirituellement mort, affirme l'apôtre Paul dans Romains 6 : 23. Tous les efforts de l'homme à savoir l'honnêteté, la bonne conduite, la religion, les prières, n'ont aucun pouvoir d'ôter les péchés. Par conséquent ne peuvent pas nous mener à Dieu.

Certaines religions imposent la pénitence, d'autres recommandent les bonnes œuvres, les sacrifices etc., mais dans tous cela il n'y a pas de place pour le pardon des péchés accordé par Dieu. Seul Jésus-Christ par sa mort ignoble pour toi et moi sur la croix et sa résurrection victorieuse d'entre les morts s'est donné comme un pont entre l'homme pécheur et Dieu saint. Par Lui vous pouvez expérimenter l'amour et le plan de Dieu pour votre vie. «

Personne ne peut aller au Père autrement que par moi » dit Jésus (Jean 10 : 10)

Vous pouvez accepter Jésus–Christ par la foi comme Sauveur et Seigneur et ensuite vous pouvez expérimenter l'amour et le plan de Dieu. Accepter Jésus Christ c'est lui donner la direction de votre vie, c'est–à–dire céder le centre des décisions de votre vie à Jésus, c'est vous détourner des péchés et laisser à Jésus vivre sa vie en vous.

ACCEPTER CHRIST REQUIERT UN TRIPLE ENGAGEMENT

1. Engagement de l'intelligence :

L'homme qui prend une décision importante dans sa vie doit la mûrir. De même il convient de savoir en qui ou en quoi on s'engage car la foi chrétienne repose sur des faits historiques vérifiables. A savoir la naissance de Jésus, sa vie, sa mort et sa résurrection

2. Engagement des sentiments :

L'homme est par nature émotionnel, cependant, les émotions ne devront pas prendre une place excessivement important dans votre relation avec Dieu car cela ne peut que vous conduire au doute de votre salut. Certaines personnes connaissent des expériences bouleversantes dans leurs rencontres avec le Seigneur, ce fut le cas de l'Apôtre Paul, tandis que d'autres le font calmement ce fut le cas de Timothée qui a appris à connaître le Seigneur par sa mère. Votre assurance du salut doit se baser sur la parole de Dieu. S'il nous arrive de prendre en considération les témoignages des hommes, a plus forte raison, que dirions–nous du témoignage de Dieu rendu sur son fils et au sujet de celui qui croit en lui ?

« Voici ce témoignage : Dieu nous a donné la vie éternelle et cette vie nous sont accordée en son fils. Celui qui a le fils de Dieu a la vie ; celui qui n'a pas le fils de n'a pas la vie. Je vous écris afin que vous sachiez que vous avez la vie éternelle vous qui croyez au nom du fils de Dieu » (1Jean 5 : 9–13) C'est la plus grande promesse et la plus grande sécurité.

Le Saint Esprit de même rend témoignage a notre esprit que nous sommes enfants de Dieu, nous qui croyons en Jésus Vous pouvez, vous aussi devenir enfant de Dieu selon Jean 1 : 12

Que les sentiments puissent varier, c'est tout à fait normal car les circonstances ne sont pas toujours les mêmes. Mais Dieu n'abandonne jamais celui qui se confie en Lui.

3. Engagement de la volonté :

Vous pouvez vouloir aussi accepter. Le désir d'obéir à sa propre volée est une des raisons qui empêchent beaucoup de personnes à se donner à Jésus L'orgueil soit intellectuel, soit matériel maintient l'homme de faire le pas vers Christ. D'Autres estiment que la foi en Jésus comme une série des lois contraignant leur liberté, arrachant de leur cœur toute joie pour combler leur existence de tristesse. Mais quel est ce Dieu qui appellerait les hommes et les femmes à venir vers lui pour leur arracher de le la joie. Ne dit–il pas que « je connais les projets que j'ai formés sur vous ; projets de paix et non de malheur afin de vous donner un avenir de l'espérance » ? Jérémie 29 : 11

Pour se maintenir dans le péché, certaines autres personnes n'ont pas le temps de s'interroger sur la valeur de leur foi en Jésus–Christ, entretiennent de doutes volontairement puis les rationalisent. Cet état relève du manque de foi, et du désir de cacher la désobéissance à Dieu. Somme toute, cette réflexion ne saurait toucher à sa fin sans préciser ce

qui suit :

- 1) Dieu vous aime et il a un plan merveilleux pour votre vie
- 2) L'homme est pécheur ainsi il ne peut pas connaître et expérimenter ce que sont l'amour et le plan de Dieu pour sa vie.
- 3) Jésus-Christ est le seul chemin par lequel vous pouvez atteindre Dieu. Il est mort pour nous, par lui vous pouvez expérimenter l'amour et le plan de Dieu pour votre vie.
- 4) Vous devez personnellement accepter Jésus-Christ dans votre vie comme Seigneur et Sauveur. Vous pouvez recevoir Christ par la foi en l'invitant personnellement par une prière.

"Alan J Rosenthal" <flaps@dgp.toronto.edu> wrote in message news:H7IywE.4oH.0.water@cdf.toronto.edu...

- > *Archive-name: computer-security/most-common-qs*
- > *Posting-frequency: monthly*
- > *Last-modified: October 2002*
- > *Last-seriously-modified: January 2001*
- > *URL: <ftp://rtfm.mit.edu/pub/faqs/computer-security/most-common-qs>*
- >
- > *This is a faq file for comp.security.misc and comp.security.unix. It is*
- > *cross-posted to alt.security because I think it will also be useful there.*
- >
- > *Please check whether your question is in this file before posting.*
- > *Also, unix-specific questions should be posted to comp.security.unix, not*
- > *comp.security.misc; so if they're in here, there are now TWO reasons not*
- > *to*
- > *post them to comp.security.misc.*
- >
- > -----
- >
- > *Subject: Table of contents*
- >
- > *- This faq*
- >
- > *- Can anyone here tell me how to exploit the [whatever] bug?*
- > *or Can anyone here tell me how to break in to my ISP?*
- >
- > *- What do the "identd" lines in my syslog mean? Is this a security*
- > *exposure? Can I turn off identd?*
- >
- > *- I just noticed that [something]. Has my machine been compromised?*
- >
- > *- What does port number [whatever] mean?*
- >
- > *- Here's new, unbreakable encryption software.*
- >
- > *- What should I read to learn how to secure my computers? What should I*
- > *read*
- > *to learn about computer security?*
- >
- > *- Is there a newer version of cops?*

- >
- > – *Tripwire fails the self-test, dumps core when building the database, and*
- > *dumps core when verifying.*
- >
- > – *Cops won't "make" in some versions of linux (GNU).*
- >
- > – *Various problems with building anything under Solaris, especially*
- > *"/usr/ucb/cc: language optional software package not installed".*
- >
- > – *What's that weird URL with SATAN/SAINT? I'm not running a web server!*
- > *or SATAN says "Can't find my own hostname".*
- >
- > – *SATAN doesn't display right in my web browser; it asks me to save the*
- > *file.*
- >
- > – *How do I find all setuid and setgid files?*
- >
- > – *Tcp wrappers (tcpd) thinks all hosts are 0.0.0.0 in Solaris 8 or in some*
- > *versions of AIX.*
- >
- > – *I can't get .rhosts/.shosts to work with ssh.*
- > *(Note: there is a newsgroup comp.security.ssh)*
- >
- > – *Should I block all ICMP at my firewall/router?*
- >
- > – *How do I prevent my machine from announcing OS version, daemon version,*
- > *etc in the banner message?*
- >
- > – *How do I recover from forgetting my root password? (Similarly: I messed*
- > *up*
- > *the root line in /etc/passwd and can't su or login as root; what do I*
- > *do?)*
- >
- > – *Is a portscan of a machine malicious/illegal/unfriendly?*
- >
- > – *Can my ISP/employer monitor [various things I'm doing]?*
- >
- > – *Why do some people get so upset when system penetration is called*
- > *"hacking"?*
- >
- > -----
- >
- > *Subject: This faq*
- >
- > *This is not supposed to be a statement of group consensus. This is simply*
- > *supposed to be a few VERY frequently asked questions and their answers, so*
- > *that we can snidely say "see the faq" when people ask them. The answers*
- > *supplied are supposed to be completely uncontroversial amongst people who*
- > *know what they're talking about. (My first answer might be a bit*
- > *borderline*
- > *in this respect but I don't recall ever having seen a contrary opinion*

here.)

- > *Except for the portscan question, in which I've attempted to present ALL*
- of
- > *the major views.*
- >
- > *Contributions of questions are welcome (with or without answers); however,*
- > *the idea is that they are supposed to be things which have straightforward*
- > *answers and which we see very frequently (at least prior to their*
- inclusion
- > *in this document). If your answer is long, it might not belong in this*
- > *document, at least as I see the purpose of this document. For example, it*
- is
- > *intentional that this document doesn't contain firewall recommendations,*
- even
- > *though that's a frequently-asked question here. (But see the firewall faq*
- at
- > <http://www.interhack.net/pubs/fwfaq/>)
- >
- > *Thanks to Juan Gallego, Lamont Granquist, and Martin Ouwehand for*
- additional
- > *suggestions re finding setuid files on different versions of unix. Thanks*
- > *to Dan Farmer for making me aware of cops 1.04+ (cf 1.04). Thanks to Dan*
- > *Niles and Jyrki Havia for tripwire bug details as posted to the newsgroup.*
- > *Thanks to Scott Barman for a Windows NT security book reference. Thanks*
- to
- > *Robert Graham for suggesting I cite his good firewall-seen.html file.*
- > *Thanks to Denis McKeon and Olaf Schreck for improvements to my bit about*
- > *editing the SATAN perl file (to avoid newbie errors).*
- >
- > *Disclaimer: The posting of this file is not to be construed as a*
- commitment
- > *to provide free consulting to people I don't know. Post your questions to*
- > *the newsgroup and I might answer them there, or someone else might do it*
- > *better. (Although if you say "please send e-mail copies", I'm going to*
- > *ignore your message.)*
- >
- > *Disclaimer 2: There ARE errors in this file, but at the time of writing, I*
- > *didn't know what they were. (If I knew, I would have fixed them.) This*
- > *document is offered on an "as-is" basis, no warranty is implied, blah blah*
- blah.
- >
- > *The metafaqs say you should choose a random day of the month to post*
- monthly
- > *faqs on, so I just used random() and got the number 22 (I don't think it's*
- > *necessary for it to be a cryptographic random number).*
- >
- > *Yes, I know that syntactically, these are not all "questions".*
- >
- > -----
- >
- > *Subject: Can anyone here tell me how to exploit the [whatever] bug?*

- > *or Can anyone here tell me how to break in to my ISP?*
- >
- > *No. We're security professionals. We try to secure systems. We think that*
- > *securing systems and fixing bugs are more intellectual activities than running*
- > *a program which someone else wrote which you don't understand.*
- >
- > *You should only attempt "penetration testing" of a system with the consent*
- > *of its administrators and/or owners. They will only be interested in your*
- > *services if you know something. You can start your education by learning*
- > *some general computer science and computer programming, and by reading*
- > *computer security textbooks and/or newsgroups.*
- >
- > -----
- >
- > *Subject: What do the "identd" lines in my syslog mean? Is this a security*
- > *exposure? Can I turn off identd?*
- >
- > *Discarding the timestamp and hostname, the lines look something like this:*
- >
- > *identd[10362]: from: 205.238.143.33 (mail.dejanews.com) for: 20546,*
- 25
- > *identd[10362]: Successful lookup: 20546 , 25 : flaps.users*
- >
- > *This states that the machine 205.238.143.33 asked your machine who was*
- > *connecting from port 20546 on your machine to port 25 on 205.238.143.33.*
- > *And your machine responded that the user was "flaps", and that flaps's*
- group
- > *is "users". (10362 is the process id number of this particular invocation*
- of
- > *identd; for example, if two identd requests happened at about the same*
- time
- > *and the two lines were interleaved, it would help you sort them out.)*
- >
- > *Theoretically, this is a security-sensitive data exposure, although the*
- > *practical effect of this is arguably nil. And it can be very helpful to*
- the
- > *admin of a machine which often has more than a few simultaneous users.*
- When
- > *one of your users does something untoward, this allows the remote machine*
- to
- > *log the username, and then the remote sysadmin's complaint to you will*
- > *contain information useful to you. A linux machine at home connected to*
- the
- > *internet via ppp and with only one user should not be running identd*
- because
- > *it does not contribute to this process. Very few things on the net*
- REQUIRE
- > *the sender to be running identd, because many machines don't have it and*
- > *because many people turn it off.*

>
> *Your identd program probably has various options to configure what
> information it discloses; see the man page. You might want to run it with
> options to minimize data OTHER than the above (-o and -e in the common
> implementation), and/or perhaps run it with the option to report numeric
uids
> rather than lognames (-n), which is just as useful for tracking down
> offenders from your point of view. On the other hand, if you report
numeric
> uids, then in some cases the remote people will be able to gain
logname<->uid
> translation info (e.g. the outgoing connection is a mail message bearing
> 'from' information), so it's hard to say which discloses less data.
>
> *If you feel that this data is sensitive but still want to run identd,
there
> are some identd servers out there which report the data encrypted, so that
> all the target sysadmins can do with the information they get is to send
the
> token back to you for your own use. This facility might be available
as -C.
>
> *You specify these options on the identd command-line, wherever it appears,
> which is usually in /etc/inetd.conf.
>
> *The identd protocol is documented in RFC 1413. It is the same as "auth".
> The query specifies the port numbers only; the two IP addresses implied
> are the sender and target of the identd query. Thus you cannot query
about
> IP connections to other machines, although you can query about connections
> which don't concern you but are to a machine you have an account on.
>
> *RFC 1413 states, "If you wouldn't run a 'finger' server due to privacy
> considerations you may not want to run this protocol." I agree with this
but
> suggest that it might not apply to a cryptographic identd (e.g. -C).
>
> -----
>
> *Subject: I just noticed that [something]. Has my machine been
compromised?
>
> *Maybe. You probably don't know whether it always was like this. You
should
> look around your system enough of the time that you get used to how things
> look BEFORE you get broken into. And you should make a practice of
following
> up oddities you find, so that your judgement as to what is and is not
weird
> improves with experience.
>*******

comp.security.unix: Re: comp.security.unix and comp.security.misc frequently asked questions

- > *If it's too late for that, before posting to comp.security.* ask at least*
- > *one local expert in the OS you're running, or in the case of*
- unix/linux/gnu,
- > *one local unix expert. There may be a straightforward, happy explanation*
- > *for the behaviour you observe. Or there may not. Not all anomalies are*
- the
- > *result of an intrusion; to some extent "My machine has been broken into!"*
- has
- > *replaced the "I have a virus!" default explanation of a few years ago.*
- > *On the other hand, machine breakins are very common these days, too.*
- >
- > -----
- >
- > *Subject: What does port number [whatever] mean?*
- >
- > *RFC 1700 is obsolete. The standard current reference is*
- > <http://www.iana.org/assignments/port-numbers>
- >
- > *However, you can write a program which uses any port number, whether it*
- has a
- > *standard meaning or not; and similarly you can write a program which uses*
- a
- > *port number in a way contrary to its standard meaning.*
- >
- > *If you notice an attempted connection to a weird port number on your*
- machine,
- > *the connection might have been meant for some other machine running an*
- > *idiosyncratic service (perhaps someone typoed the IP address or hostname),*
- > *it might be a probe for a widely-spread trojan horse program, it might be*
- > *part of some kind of portscan, or plenty of other possibilities. Some*
- notes
- > *about what a particular port access might mean in practical terms (as*
- opposed
- > *to the intended purpose of that port number assignment) can be found at*
- > <http://www.robertgraham.com/pubs/firewall-seen.html>
- > *And a list of some non-standard ports used by various strange programs is*
- at
- > <http://www.chebucto.ns.ca/~rakerman/port-table.html>
- >
- > *If you notice your machine listening on an unexpected port, you may have*
- > *been broken into, or it may be a "feature" of your OS distribution or some*
- > *third-party software you're running. In unix, most ports your OS*
- distribution
- > *will use will be listed in /etc/services, along with MANY you don't use.*
- > */etc/inetd.conf lists services whose daemons are started on demand by*
- inetd,
- > *the internet "super-server" (see the man page). (/etc/inetd.conf entries*
- > *cause services to be offered; /etc/services entries basically just map*
- names
- > *to and from numbers.) In different ways depending on OS version, /etc/rc**
- > *specifies some standalone daemons to be started up on boot (or initlevel*

- > *change*); see man pages (including man init). These are conventional ways to
- > start services but any program can listen on a port (unprivileged processes
- > can only listen on port numbers ≥ 1024 in most multiuser OSes).
- >
- > Some port numbers are not fixed. There are several possibilities here, but
- > in unix these most notably include port numbers bearing services registered
- > under the "portmapper", which listens on port 111. Type "rpcinfo -p hostname"
- > for a list of services for which the portmapper is serving as a directory.
- > (Some of these port numbers may in fact be fixed, in which case client
- > programs have two different ways to find the port number (hardcode the port
- > number or use the portmapper).)
- >
- > To see what listeners you have running (open ports), the canonical incantation
- > is "netstat -an". But doing a portscan from a remote machine might be more
- > reliable if you suspect your machine has been compromised, because the netstat
- > program could have been replaced. (But do keep in mind the tricky "malware"
- > technique of only accepting connections with certain *source* port numbers.)
- > To find out what process is doing the listening, try something like lsof.
- > Again, once your machine has been compromised, this might report the
- > wrong answer; the purpose of using lsof would be to investigate the normal
- > behaviour of your machine, not to check whether it's been compromised.
- >
- > -----
- >
- > Subject: Here's new, unbreakable encryption software.
- >
- > It's probably not substantially new, and I'm sure it's not unbreakable.
- > Read the snake oil FAQ at
- > <http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>
- >
- > -----
- >
- > Subject: What should I read to learn how to secure my computers? What should
- > I read to learn about computer security?
- >
- > The number one thing to do is to install all of your vendor's security
- > patches and to disable unused services (in unix, comment things out of
- > /etc/inetd.conf, and remove daemon invocations from /etc/rc* (details
- > depend on OS version)). See some other basic information in

comp.security.unix: Re: comp.security.unix and comp.security.misc frequently asked questions

- > http://www.cert.org/tech_tips/unix_configuration_guidelines.html
- > *Subscribe to the CERT advisory list and to your vendor's security alert list*
- > *to keep current in future.*
- >
- > *If you're trying to learn your way around unix and internet security in general, I suggest you want to start with a good grasp of unix basics, e.g.*
- > *from the Kernighan & Pike book. You'll also want to be strong in C, which education you can begin with the Kernighan & Ritchie book. (Of course there are alternatives to both.)*
- >
- > *If you're feeling strong after that and want to go for the details, read Farmer & Venema's "Improving the Security of Your Site by Breaking Into it" at <http://www.fish.com/security/admin-guide-to-cracking.html>, and the Cheswick & Bellovin firewalls book. For a gentler approach covering a broader range of security issues, read Spafford & Garfinkel's "Practical Unix and Internet Security". A more hands-on-oriented book about firewalls*
- > *is Chapman & Zwicky.*
- >
- > *If you're interested in cryptography, the canonical book is Schneier's "Applied Cryptography", and you might be interested in RFC 1750.*
- >
- > *I've received a recommendation for "Windows NT Security" by Rutstein.*
- >
- > *Some URLs with security notes for particular systems (in addition to those above, and don't forget your vendor's security patch list):*
- >
- > *Linux security:*
- > <http://metalab.unc.edu/LDP/HOWTO/Security-HOWTO.html>
- >
- > *Irix (out of date but contains notes which are still important):*
- > <ftp://rtfm.mit.edu/pub/faqs/sgi/faq/security>
- >
- > *Improve assorted file permissions for solaris 2.2 through 2.6, changing the pkg database to match:*
- > <ftp://ftp.fwi.uva.nl/pub/solaris/fix-modes.tar.gz>
- >
- > *Solaris security:*
- > <http://www.sunworld.com/common/security-faq.html>
- >
- > *Unix versus Windows NT:*
- > [<http://www.unix-vs-nt.org> is now a domain squatter; does this page have a new home, anyone?]
- >
- > *(Canonical URLs for additional platforms solicited! Non-vendor URLs preferred.)*
- >
- > -----
- >

Re: comp.security.unix and comp.security.misc frequently asked questions

- > *Subject: Is there a newer version of cops?*
- >
- > *No. Version 1.04+ is a bit old but performs some functions which are still as*
- > *useful as they ever were. (And the message "/usr/lib/sendmail could have a*
- > *hole/bug!" is still right although the cert advisory quoted could be changed.)*
- >
- > *(1.04+ contains an assortment of minor fixes and enhancements to 1.04,*
- > *and was released in 1993 by the original author (Dan Farmer).)*
- >
- > -----
- >
- > *Subject: Tripwire fails the self-test, dumps core when building the database,*
- > *and dumps core when verifying.*
- >
- > *Fails the self-test (on fast machines):*
- >
- > *You have to slow it down (just the self-test scripts, not the tripwire binary*
- > *itself). The test scripts create and then update a file, and then fail to*
- > *detect that the timestamp has changed. But this is ok, because the timestamp*
- > *has indeed not changed, because this all happens within a second on some*
- > *modern machines. This occurs in a few places in the test scripts. If a*
- > *second-boundary happens to be crossed during this brief interval, then that*
- > *particular test will succeed, but another one might fail soon.*
- >
- > *In the tests directory, edit 3 of the 4 files named test.*.sh:*
- > *in test.escape.sh, add "sleep 1" on line 46 (in the cert version), just before*
- > *running tripwire; in inter and update, un-comment-out the "sleep 1".*
- > *If this isn't good enough (obscure but can happen), use "sleep 2". See*
- > *<ftp://coast.cs.purdue.edu/pub/COAST/Tripwire/README-third>*
- >
- >
- > *Dumps core when building the database (if you have 8-bit chars in filenames):*
- >
- > *Tripwire 1.2 contains a bug relating to octal printing of 8-bit chars in file*
- > *names. The bug occurs in filename_escape() in src/utls.c. Double the size*
- > *of the "octal_array" to contain all 256 possible entries, and change*
- > *octal_array[(int)(*pcin)] to octal_array[*pcin & 255] farther down.*
- > *(This only works if you have eight-bit bytes, of course, but most of us do.)*
- >

comp.security.unix: Re: comp.security.unix and comp.security.misc frequently asked questions

>
> *Dumps core when verifying (this bug surfaces on some systems only):*
>
> *In config.parse.c just before the end of configfile_read(), on line 356 in*
> *the tripwire 1.2 distribution, there is a "rewind(fpout);". It should be*
> *conditional on "specified_configmode" as in the previous "if" statement:*
> *at this point the values "fpin" and "fpout" are the same (see line 184),*
so
> *it is actually rewinding the fp it might have closed in the previous line.*
> *So simply add the word "else" before the "rewind". (Perhaps change*
"fpout"
> *to "fpin" for clarity, although this won't affect its behaviour.)*
>
> -----
>
> *Subject: Cops won't "make" in some versions of linux (GNU).*
>
> *Remove the '#' from "BRAINDEADFLAGS" in the makefile.*
> *(This adds a "-lcrypt" to the compilation of pass.c.)*
>
> -----
>
> *Subject: Various problems with building anything under Solaris, especially*
> *"/usr/ucb/cc: language optional software package not installed".*
>
> *This is not a security question. Please ask in a solaris newsgroup*
instead,
> *or ask someone near you because it's a detail, and easy to diagnose in*
> *person but sometimes hard to diagnose over the net (depending on the*
problem).
>
> *If you get the message "language optional software package not installed",*
> *this means that the compiler is not installed. (Like, duh.) Sun doesn't*
> *include a C compiler with Solaris. Get gcc. Put it in your path and/or*
in
> *the makefile (e.g. CC=gcc). Perhaps do "ln -s gcc /usr/local/bin/cc" so*
that
> */usr/local/bin/cc points to /usr/local/bin/gcc, and make sure*
/usr/local/bin
> *is near the front of your path. This is still not a security question.*
>
> *If you are using the Sun compiler tools, or having problems with other*
missing
> *commands such as "make" or "ar", perhaps you need to add /usr/ccs/bin to*
> *your path. This is not a security question either.*
>
> -----
>
> *Subject: What's that weird URL with SATAN/SAINT? I'm not running a web*
server!
> *or SATAN says "Can't find my own hostname".*

>
> *SATAN acts as a web server so that it can use HTML conveniently. The main*
> *thing it gets out of HTML is its hypertext capabilities (you can click on*
> *stuff).*
>
> *The web browser communicates with it using the HTTP protocol. This allows*
> *it to generate responses to queries dynamically, rather than having to*
> *generate a huge number of static files (to be accessed via file://). It*
> *includes a cryptographic random number at the beginning of the URL so that*
> *others can't contact your copy of SATAN and retrieve the information it's*
> *supplying.*
>
> *If SATAN claims it "can't find my own hostname" or if the web browser*
can't
> *resolve your hostname in the URL, try adding your hostname to /etc/hosts.*
> *You can list multiple hostnames for a given IP address in /etc/hosts;*
among
> *them should be the output from the "hostname" command and also your*
> *fully-qualified domain name ("myname.dept.organization.org" rather than*
> *"myname" or "myname.dept").*
>
> -----
>
> *Subject: SATAN doesn't display right in my web browser; it asks me to save*
> *the file.*
>
> *Newer web browsers seem to use different algorithms in guessing mime types*
> *when the web server doesn't supply them. Anyway, web servers are supposed*
to
> *supply the correct mime type and it's easy to fix SATAN to do so.*
>
> *Add, in perl/html.pl, in process_html_request before it sends anything*
> *(actually I see I put it just before the "Make sure they gave us the right*
> *magic number"):*
>
> *# local bug fix: must send http response code and content type header*
> *print CLIENT "HTTP/1.0 200 Ok\nContent-Type: text/html\n\n";*
>
> *There's some bad advice out there about adding a handler with the ".pl"*
> *suffix in your netscape preferences.*
> *1) This is wrong. What's relevant about the satan response is that it is*
> *indeed html code, not the fact that the requesting URL ends in .pl. A web*
cgi
> *URL might end in .pl but the program might return a gif. Unlike with*
e-mail,
> *mime types are an integral part of the http protocol.*
> *2) This is dangerous (the version of the advice which says to set it to*
> *invoke the perl interpreter). You don't want to execute arbitrary perl*
code
> *off the net. It also won't work, because the satan response is html code,*
not

> a perl program.
>
> The recommendation to deactivate an existing ".pl" handler is ok, but the
> above is better imho; it fixes the real problem, and the fix won't go away
> when you switch web browsers or use a different account.
>
> -----
>
> Subject: How do I find all setuid and setgid files?
>
> find / -local -type f \(-perm -4000 -o -perm -2000 \) -print
>
> or to do an "ls -l" of them:
>
> find / -local -type f \(-perm -4000 -o -perm -2000 \) -exec ls -ld '{}'
> \;
>
> You may want to add the "-u" option to ls to see last-accessed times
rather
> than last-modified times (esp to help gauge how harmful it would be to
> unsetuid the file).
>
> Some versions of "find" don't have the "-local" option. Its purpose is to
> avoid searching nfs volumes. If you don't have any nfs mounts, you can
omit
> the "-local". If you do, here are some other possibilities:
> * On some systems you can do something like
> find / -fstype nfs -prune -o -type f \(-perm -4000 ...
> * Some systems have "-xdev" or "-mount", which prevent find from
> traversing mounts. But then you have to run it for each local
> filesystem separately.
> * Do the check with nfs filesystems unmounted (e.g. single-user mode).
> * As an alternative to find, "ncheck -s" will tell you all setuid and
> setgid files, plus all device files (which is something of equal
> interest, although usually much less problematic in OS
distributions).
> It too must be run separately for each filesystem.
>
> Please note that this is insufficient if you suspect backdoors have been
> installed on your system. The backdoor installation activity could have
> included modifying the "find" command. The purpose of the above is to
find
> locally-installed or vendor-supplied security bugs waiting to happen, not
to
> find backdoors.
>
> Also note that on some systems, "-local" doesn't do what you'd think,
because
> it still traverses the entire remote filesystem, and rejects all nodes in
it
> as non-local. In this case you want "! -local -prune -o", i.e. if not

local

> *prune the search, else*

>

> -----

>

> *Subject: Tcp wrappers (tcpd) thinks all hosts are 0.0.0.0 in Solaris 8 or in*

> *some versions of AIX.*

>

> *This is because the line for that service in inetd.conf still says "tcp6".*

> *The vendor-supplied application you are wrapping can handle IPv6 (aka*

> *"IP-NG") connections, but the version of tcp wrappers you are using cannot.*

> *Change "tcp6" to "tcp" on inetd.conf lines which you edit to invoke the*

> *standard version of tcp wrappers.*

>

> *For ftpd for AIX, I've heard that you then need to add the '-f' option to*

> *the ftpd invocation. (Confirmation requested.)*

>

> *Alternatively, use a "IPv6-aware" version of tcp wrappers from*

> *<ftp://ftp.porcupine.org/pub/ipv6/>*

>

> -----

>

> *Subject: I can't get .rhosts/.shosts to work with ssh.*

>

> *If ssh doesn't do what you want, the output of "ssh -v" may be helpful.*

>

> *For .rhosts or .shosts (or hosts.equiv or shosts.equiv) to take effect*

> *with*

> *ssh with the default configuration, a few somewhat unobvious things must*

> *be*

> *the case. These are all good restrictions and the rationale is included*

> *here.*

>

> ** The request must be coming in from a "privileged port"; thus, the*

> *ssh*

> *client must be setuid. Without this restriction, any user could*

> *masquerade (for the purposes of passwordless login) as any other on*

> *the*

> *same source machine. (Even with it, root can; but there's no way to*

> *restrict THAT without the user typing something or involving a third*

> *machine (i.e. some hardware which root doesn't have access to).)*

> *Also,*

> *the ssh client must be able to read /etc/ssh_host_key (the private*

> *one)*

> *to be able to do the public key authentication thing to prove you're*

> *on*

> *the host whose IP address you're using. N.B. that the 1.2.25*

> *makefile*

> *sometimes turns off the setuid bit on ssh when doing a "make*

install"

> *(it's a bug in the makefile, fixed in 1.2.26).*

>

> ** .rhosts or .shosts must be owned by the appropriate user and not be
> writable by group or others. Sshd does not check for the situation*

of

> *single-user groups common on some versions of unix these days (esp
some*

> *versions of GNU/linux); you have to chmod g-w .rhosts/.shosts if
your*

> *umask is 2. (There is no way for sshd to detect the single-user
group*

> *situation; current membership of size one doesn't tell you its
history.)*

> *Similarly, your home directory should not be writable by group or
others.*

>

> ** The source host must be in /etc/ssh_known_hosts or*

> *~user/.ssh/known_hosts on the target machine.*

> *This is the difference between "RhostsRSAAuthentication" (allowed by
> default) and "RhostsAuthentication" (disallowed by default).*

Without

> *this, ssh is not gaining you any login security, although it is
still*

> *gaining you anti-sniffing security.*

>

> *When all else fails, try "ssh -v".*

> *Take further questions to comp.security.ssh.*

>

> -----

>

> *Subject: Should I block all ICMP at my firewall/router?*

>

> *No. You need to allow the "can't fragment" message through or you will
lose*

> *connectivity to some number of sites with wacky packet sizes on their
local*

> *nets (notably token ring). See <http://www.worldgate.com/~marcs/mtu/>*

>

> *Less crucially but still somewhat important, if you block the "destination*

> *unreachable" message then you'll get timeouts, after a long wait, in some*

> *cases when you could have received immediate "no route to host" messages.*

>

> *But blocking some of the rest might not be a bad idea, especially
"redirect".*

>

> -----

>

> *Subject: How do I prevent my machine from announcing OS version, daemon*

> *version, etc in the banner message?*

>

- > *In unix, find the daemon in question, possibly by finding its line*
- > *in /etc/inetd.conf, and read its man page. For complex config files*
- > *(e.g. sendmail), search in the config file for the constant portions of*
- the*
- > *string it's outputting (e.g. in sendmail.cf find the string "Sendmail"*
- with*
- > *a capital 'S'). For telnetd, some systems have "-h" to suppress the*
- greeting*
- > *and other systems' banners come from a file called something like*
- /etc/issue.*
- > *(Note that in redhat linux, you really want to modify /etc/rc.d/rc.local*
- > *rather than (or in addition to) /etc/issue*, because it regenerates*
- > */etc/issue* upon boot.) For Solaris 2.6 and greater, put "BANNER="*
- (without*
- > *the quotes) in /etc/default/telnetd and/or /etc/default/ftpd. The telnetd*
- > *included with Solaris <2.6 and SunOS can't suppress the banner, but*
- there's*
- > *no need to use that particular software; you could use GNU telnetd or*
- wu-ftpd,*
- > *for example; or you might edit the binary, as the strings appear in it.*
- >
- > *But this might not really be a security issue and it might not be worth*
- > *your effort. Suppressing banners probably doesn't restrict any*
- information*
- > *which is genuinely useful to an attacker. If an attacker has some*
- "exploit"*
- > *program for sendmail 1.2.3 only, then rather than checking the banner to*
- see*
- > *if your machine is in fact running sendmail 1.2.3, they might as well just*
- run*
- > *the exploit program, which is a direct check of whether you're vulnerable.*
- > *Whereas the banner suppression *will* interfere with some kinds of*
- checking*
- > *of daemon versions which you yourself may want to do occasionally.*
- >
- > -----
- >
- > *Subject: How do I recover from forgetting my root password? (Similarly:*
- > *I messed up the root line in /etc/passwd and can't su or login as*
- > *root; what do I do?)*
- >
- > *Basically, you want to boot from CD/floppy or in single-user mode.*
- > *Single-user mode in some versions of unix still prompts for the root*
- > *password, but can nevertheless be used to recover from messing up the root*
- > *line in /etc/passwd farther along, e.g. changing the shell to something*
- > *inappropriate. And in some versions of unix it doesn't ask for the*
- password.*
- >
- > *To boot in single-user mode, in a prom monitor (e.g. LI-A on a Sun, or*
- press*
- > *ESC while booting an SGI), you want a command like "single" or "boot -s"*

- > or "b -s". At the linux LILO prompt, you want something like "linux s".
- > If "linux s" gives you problems, "linux init=/bin/sh" might bypass the
- > normal boot sequence and just give you a shell, but you'll have to remount
- > the root filesystem (see below).
- >
- > After single-user mode, it's cleaner to reboot rather than to press ^D to
- > do the multiuser boot, because the init "runlevel" mechanism is hacky.
- >
- > It might be more rewarding to boot from OS installation media. They usually
- > give you the opportunity to run a shell (e.g. in irix inst, type "sh"; in
- > redhat linux, press ctrl-alt-F2; in solaris, get a menu with the right
- button
- > in the background and select "command tool" in the "utilities" submenu).
- > In this case, do a "df" to find your root partition on something like
- /root
- > or /mnt (or, in solaris, /a).
- >
- > Sometimes it's easier to make like a "cracker" and break in to it.
- > I imagine that most people who forget their root password have machines
- > which can easily be broken into...
- >
- > Once you're in, you can edit the password file (or /etc/shadow as
- > appropriate), or you can change the password without supplying the old one
- > as root by typing "passwd root". (Depending on how you got there, a plain
- > "passwd" might not know it's root's password you're trying to change.)
- >
- > If you clear the password entry, be disconnected from the internet until
- > you've set a new root password (probably after a normal reboot).
- >
- > If the above doesn't answer your question, please look for a faq specific
- > to your version of unix; if you end up posting here, please state precise
- > version of unix including version number (e.g. "irix 5.3", not just
- "5.3").
- >
- > Problems editing the password file or running "passwd root" include:
- >
- > /usr might not be mounted in single-user mode (and /bin might be a symlink
- to
- > /usr/bin, so most things might be on /usr). You can probably just type
- "mount
- > /usr" or "/sbin/mount /usr". Other filesystems might also be unavailable
- > but probably aren't needed just to change the password (and you're about
- > to reboot to get things back to normal after you change root's password).
- >
- > The root filesystem might be mounted read-only, depending on how you
- > got there. "mount / -o remount,rw" might fix this.
- >
- > -----
- >
- > Subject: Is a portscan of a machine malicious/illegal/unfriendly?

- >
- > *This is included here because it's a recurring flamefest. Please avoid*
- > *simply repeating the same old basic statements, because we've heard 'em*
- all.
- >
- > *First of all, what a portscan is: Basically (there are myriad variants),*
- > *it's an attempted connection to every single port number on a given*
- machine
- > *or range of machines. Suppose you want to break in to a particular*
- machine.
- > *First thing you might do is to run a port-scanner to find out what all the*
- > *"open ports" are (ports with a listener). Then you see, aha there's an*
- > *imapd, let's try the imapd exploit program. Rather than just trying all*
- > *sorts of programs which wouldn't even connect let alone break in.*
- >
- > *Portscanning your own machine is valuable; you may find listeners you*
- didn't
- > *know were there, and then you can close them off and/or check their*
- security.
- >
- > *Since you have to secure each service on its own anyway, some people argue*
- > *that there's no need to defend against portscanning itself. On the other*
- > *hand, you might configure your system to page you, or delete all your*
- files,
- > *or perform some such useful action when it detects a port-scanning in*
- > *progress. Some defense systems cease accepting connections of any kind*
- from
- > *that IP address when they detect a portscan, and some sysadmins write to*
- your
- > *ISP and try to get you kicked off. This leads to "stealth port-scanners"*
- > *which try to avoid triggering the alarms by various means.*
- >
- > *Some people argue that there's not too much in the way of useful action*
- you
- > *can take automatically when you detect a port-scanning in progress, and*
- > *"counterattack" software is unwise and can be used via forgery to launch*
- > *attacks from your machine.*
- >
- >
- > *Now, the basic portscanning arguments. (The discussion is only about*
- machines
- > *you don't admin, obviously; there is an additional, finer dispute about*
- the
- > *situation with machines you have some legitimate association with but not*
- as
- > *sysadmin, but I don't propose to address that intermediate situation*
- here.)
- > *I might be willing to add other statements to this list if they're*
- similarly
- > *terse, and certainly do let me know if you feel I've inadequately*
- represented

- > *a viewpoint, except that I reserve the right to apply a sense of humour.*
- >
- > *Portscanning has been argued to be malicious/illegal/satanic because (see*
- > *rebuttals in subsequent section):*
- > *– a portscan is always/usually a prelude to or part of an attack, like*
testing
- > *doorknobs to see if they're unlocked*
- > *– my pager beeps when I get portscanned, which takes my time unfairly (aka*
my
- > *machine crashes, sends lots of e-mail, changes the root password to*
"soup")
- > *– if everyone portscans a few machines for fun, in total there will be a*
- > *constant barrage of portscans to all/many/some machines, overloading them*
- > *– an attempt to commit a criminal offence is itself a criminal offence*
- > *– portscanning someone ELSE's machine is a completely different matter*
than
- > *portscanning one's own*
- > *– a stealth portscan shows criminal intent even if you argue that a*
- > *traditional portscan does not*
- > *– any connection to a machine you're not explicitly authorized to use*
- > *constitutes the criminal offence of unauthorized access to a computer*
(i.e.
- > *it's already a breakin)*
- > *– various lame analogies*
- >
- > *Portscanning has been argued to be innocent/salutary/pure because (see*
> *rebuttals in previous section):*
- > *– the "hands-on imperative": people should be curious, people should*
explore,
- > *people should think*
- > *– a portscan uses a negligible amount of resources on the target machine*
- > *– if a portscan is a prelude to an attack, the ATTACK is what's wrong; the*
> *portscan is not wrong, and is not usually a prelude to an attack anyway*
- > *– legally, "mere preparation" does not constitute an attempt*
- > *– having a listener on a port solicits connections; you can't complain*
that
- > *someone makes the connection to the advertised port; port numbers are*
> *"well-known" for a reason*
- > *– if a portscan crashes your system, it's crappy anyway; if your pager*
beeps
- > *when you get portscanned, that's a stupid configuration*
- > *– if your machine is connected to the internet, it's your job as sysadmin*
to
- > *deal with network activity and you shouldn't complain if you don't like it*
- > *– various lame analogies*
- >
- > *NOTE! The above two sections are a pair. Don't cite a point from one*
> *section in your favour without examining its rebuttal in the other*
section!
- > *I am not attempting to resolve this issue here, just to decrease*
repetition.

>

> *Note re analogies: Analogies are a good way to express a point of view but*

> *usually the attempt to draw conclusions from them is essentially circular.*

> *I recommend using an analogy to express views but not to argue. Example of a*

> *useful analogy: "Looking through someone's protected files without their*

> *permission is like looking through their desk drawers." Very connotative;*

> *conveys concepts of reasonable expectations of privacy despite organizational*

> *ownership of the infrastructure; shows what the speaker thinks some of the*

> *fundamental issues are; but note it's still not a proof of anything.*

Example

> *of a useless analogy: "Portscanning isn't like trying to turn the doorknob,*

> *it's like looking at the doorknob while passing by on the street." Conveys no*

> *information other than "I think portscanning is ok". Neither is an argument,*

> *but one of them gives a wealth of information as to the basic perspective of*

> *the speaker and the other is useless.*

>

> -----

>

> *Subject: Can my ISP/employer monitor [various things I'm doing]?*

>

> *Do they have the technical ability? Yes. Your packets go through their*

> *equipment. Your packets are identified with your IP address, and they*

> *contain the IP address of the destination; your ISP's routers need to know*

> *the destination IP addresses to be able to route your packets.*

>

> *The data you send (e.g. passwords, mail message contents, URLs) is all also*

> *easily available, in the body of the packets. If you use www.anonymizer.com*

> *(in its non-cryptographic mode), the URL you request is still just as*

> *available in the outgoing packets.*

>

> *If you use some form of encryption, e.g. ssh, they could still at least tell*

> *the destination, even if the contents are unreadable. In general, encryption*

> *is the only way to render at least the contents unsnoopable, and only then if*

> *the encryption and decryption are both done on machines which the overseers*

> *DON'T control, and plain text not transmitted on any networks on which the*

> *overseers have machines or are able to attach machines. If you use their*

> *computers (including if you run the encryption program on a unix machine*

> *operated by them), then everything you do is available to them,*

theoretically.

>

> *But perhaps you were asking "May my ISP monitor X": is it allowed, is it*

> *ethical.*

>

> *I think most sysadmins would feel that once there is reasonable suspicion*

that

> *you are acting improperly (breaking into computers, violating the*

acceptable

> *use policy, etc), that it is ethical for the admins to take a closer look.*

>

> *It's unlikely that it's illegal for them to look at your stuff or what*

> *you're doing, although there are some exceptions. Under certain court*

orders

> *or subpoenas, it may be illegal for them not to look at your files or*