Hacker's Black book

13: 20 23. 06.99 (c)1999Frank Owens&l@tz@rus

Hacker's Black Book

This report is helpful in two different regard. It is to give the possibility to humans, who lost their password, of back-getting and for owners of Websites possible with protected contents of making it by application of simple techniques without long waiting periods to protect these contents.

Web masters, which know the techniques described in this report, have substantially better prospects to protect your Website surely from intruders.

Under the URL:

HTTP://speedometer.de/banner/secure/ the member range is to this report. There you find to utilities and Tools, in order to do the techniques over again described in this report.

Their Login: januar2000

Their password: xxx2345

Table of contents

Javascript password protection systems

The simplest kind of password protection systems is the so-called JavaSeript protection. To enter requested the user when entering a side or when clicking a certain left in addition a password. This kind of protection is very simple and offers only a Minumum at protection. When regarding the HTML source code of the side then often a Javascript code is similar to the following:

```
<head><title> Website-Titel </title> <script><P>

function jproto() {
pass=prompt("Enter your password","password");
 if (pass = "nasenbaer") {
document.location.href=http://protectedserver.com/index.html;
}
else {
alert( "Password incorrect!" );
}
}
</script>
</head><P>
```

As one sees, the entered password is compared and with correctness to indicated URL jumps. Now one sees, how the password was called and it can enter simply or select directly the goal URL.

Often also the password is used, in order to generate goal URL. For example the secret goal URL HTTP could: members. more protectedserver. com/members/hu8621s. htm, which Passwort"hu862ls "coded as part of the URL. The appropriate protective function in the HTML code of the side would look then as follows:

```
fucnction jprot () {
pass=prompt ("Enter your password", "passwords");
```

document. location. href="http. members. Proteetedserver. com/members /
"+pass+". HTML ";
}

Here more protection than in exists the first variant, however the listings are by means of the HTTP server against bad would often not list the listing estimated. One selects the URL by means of the Browsers http://members.protectedserver.com/members/hu8621.shtm **directly into the Browser, then one receives often a listing of all HTML sides in this listing, thus also the side, which is started over the Javascript password protection.**

fucnction jprot () {<P>

pass=prompt ("Enter your password","password");
document.location.href="http.//members.Proteetedserver. com/members/
"+pass+".html";
}<P>

HTACCESS Passwortschutzsysteme

Nearly all Web servers used today control the so-called HTACCESS password protection. First it from the Apache Web server begun, meanwhile are however many other Web servers to the HTACCESS standard compatible. Therefore it is used also very frequently by so-called Paysites. Z. B. the Websites www. playgal. com or www. hotsex. com use this protective mechanism.
A Website, which uses HTACCESS, is to be recognized by the fact that with enter the member range a Popup dialogue appears (not Javascript-generated), which measured following looks:

PICTURE MISSING

In order to understand the function of this protection, one should know some Gmndlagen of the Unix operating system. Under Unix (and/or Linux, BSD etc.. and

also under Windows Webservem like the Microsoft IIS the HTML documents are hierarchically in listing structures arranged and put down as also with a normal PC. One speaks here in particular of einer"Baumstruktur ". The root of the tree (English "root") is the Domain without further information. To Example www. IBM. com are the Domain and this are the root of the listing structure. If in the listing "secure" would lie now the HTML of documents and diagrams which can be protected, then now a HTACCESS file would have to be put down in this listing. The file must the names ". carry htaccess "(with point before it). The Htaccess file puts to be firmly in which file the passwords and on which kind the listing protect is. The HTACCESS file looks as follows:

AuthUserFile/usr/home/myhomedir/passes
AuthName MyProteetedSite
AuthType basic
require valid user

This HTACCESS file specifies that the password file is the file of lusr/homelmybomedir/passes on the server. The password file should not be appropriate for meaningful way in the range of the HTML Dokurnente, not be happenable thus via WWW. The options "AuthName" indicates, which designation in the PopUp dialogue is to appear (in the dialogue for example above "playgal"). Interesting to HTACCESS protection is that by the HTACCESS file also all sublists are along-protected underneath the listing, in which the HTACCESS file is. And this up to any depth. In our example one could put on secure "as many as desired further listings thus underneath the listing". These were protected all.
How now does the password file look? In the following one an exemplary password file:

Robert: 1Â$JRL0VdCRzYtbpekrLBYzl/
Manfred: $1$30$ddEyRldHykHUo654KE01i/
Thomas: 1sa$09grZEC5VRIWw. QkLA/Ge /

For each member the password file contains a line, which consists of two parts, which are separate by a colon. That first part is the log in name, the second part contains the password in coded form. This coding is very safe. It is machine specific. That is, that even if one would get this password file into the fingers one would know from the coded passwords the real passwords does not back-compute. With the password input the password is coded by the Unix Systemfunktion"crypt("and compared with the coded password put down in the password file. If it is alike, then the Login is OK ONE.)

Weak passwords

As one can recognize thus, it is very difficult to arrive in Websites, which are protected by means of HTACCESS. However some Web masters are simply too stupid to use the HTACCESS protection correctly and offer so to the aggressor some possibilities.
A weak password is a password that will easily guess can. Here some at the most frequent assigned username/password the combinations:

asdf/asdf 123456/123456 fuck/me
qwertz/qwertz qwerty/qwerty qlwè3 abc123

Particularly the large Pay Websites, which has some thousand members, is very probable it that such "weak" passwords are thereby. In addition one must imagine that some members in many different Websites member are and do not want all possible passwords to note.
Therefore the name of the respective Website is also often selected of the members as password.

Example:

www. hotsex. com: username: hot, passwords: sex
www. hotbabes. com: username: hot, passwords: babes

Or the members use simply only their name. Are naturally interesting at the most frequent occurring name particularly:

In the American one for example

john/smith John/John Miller/Miller rick/rick franc/franc

and further more. In German naturally different name is more interesting.
That is also asked Login which can be noticed simply consisting of "username/passwords", as it irn password dialogue, occurs also frequently.
The weakest of all passwords is however the so-called "ENTER" - password. The Web master must be simply confirmed to any data with producing new member data simply without input once unnoticed its Toot by mistake started with the appearance of the password of dialogue, without at all something to enter, then evenly more solcher"leerer a "entry is in the password file.
To the engaged Web master the following safety tips address themselves:

A producing "emptier" passwords prevent and control

The members not the passwords themselves to select leave, but one by coincidence generating (z.b. "kd823joq")

If the customers may select its username/password combination, not to permit that the username equal to the password is.

Direct chopping of the password file

Normally it should not be possible to arrive at the password file. In some traps it is however possible to come to it into the following traps:

Direct chopping of the password file

Normally it should not be possible to arrive at the password file.

In some traps it is however possible to come to it into the following traps:

The password file lies in public the HTML range of the Web server, thus in the listings, in which also the HTML documents accessible via WWW lie.

On the Web server have many user an own virtual Web server

The second case arises if the Website operator rents his Web server with a large Webspaceprovider, which operates many further Web servers on a computer (z.B. www. Web space service. de, www. webspace discount. de, www. simplenet. com etc.. then it is possible to come to the password file if one has an account on the same computer and the password file is publicly readable. Then one by means of ftp or telnet can change into the listing, by that kept and reading its password file. By means of a Brute Foree password Crackers like "Crack V5. O "can be back-computed then the passwords. The program needs however often many hours to it and it drives not always to success.

For an absolutely safe protection thus the Web master should not operate its Paysite on a Web server, which it must divide with other Websites.

The Admin Tools

Many Web masters of the Paysites have a so-called "Admin range", which is meant only for them. There you produce new passwords or delete old passwords etc.. Often these Admin ranges do not lie however in a password-protected range. The Web masters think, it became no the URL of their Admin Tools. But the URL is simple sometimes to guess. Often those is called URL

www. thepaysite. com/admin. htm

www. thepaysite. com/admin. HTML

or

www. thepaysite. com/admin /

One should test also further name possibilities. Because succeeds coming to the Admin side then one is naturally very best served: One can do so many new passwords in addition joints, how one would like!

Phreaken

By "Phreaken" one understands the employment about wrong information, in order to register itself with a Paysite as a new member. That is naturally forbidden and these references here is primarily the Webmastem to serve, so that they can protect themselves against such abuse.

We want to describe that here at the furthest common case, with which the membership on-line is paid via credit card and afterwards immediate entrance is given.

Phreaker use for it an anonymous lnternetzugang. In addition the test entrance is often abused by AOL. Test memberships are almost in each computer newspaper. In addition, okay. net offers immediate entrance according to indication of all data. One announces oneself with fantasy names and any bank account, which one knows ago from any calculation or sonstwo. One is long anonymous already one month via AOL or okay. net in the InterNet on the way.

Furthermore one needs a "valid" credit card number (preferably VISAS or Mastercard - in Germany Eurocard). To these to come, is already somewhat more difficult. A usual method is it, a so-called "Credit Card generator" like z. b. to begin "Credit Wizard" oder"Cardpro "more oder"Creditmaster". Looking for by means of "more metacrawler. com "and the terms" Credit Card generator "o. ae. often already brings the desired programs.

To the fact one should know that the on-line transaction centers cannot examine exactly, whether a credit card number really existed and whom them belong. There are only certain algorithms, in order to examine the number and the effective dates of a credit card for a valid structure. Therefore one can indicate arbitrary names and address for the registration and one of the generated numbers. However the generators do not supply the pertinent effective date.

However there is a simple however quite effective trick, in order to receive card numbers with correct effective date: Most of the above-mentioned programs offer the possibility of generating from a material existing credit card number new numbers. This procedure wird"Extrapolation "genannant. The generated numbers differ usually only in the last places and there the card numbers with the credit card

publishers usually in ascending order to be assigned, had the in such a way generated Kartennumrnern mostly the effective date of the map, from which extrapolates became. Folgendei screen excerpt show the extrapolation procedure: One can take its own, material-existing credit card and compute from its number new card numbers. The Gueltigkeitsdaturn is then with largest probability with extrapolates numbers identically to the effective date of the own, material credit card.

The user of these techniques does not need to have a fear that one can retrace him. The entrance by means of anonymous AOL test entrances offers maximum protection. None is available such entrance ' should a "Anonymizer" be used. One finds such for example under www. more anonymizer. com. Surf one over the Anonymizer, is not retracable the IP address. A somewhat weaker variant to hide its IP address is those to use a pro XY server. Most lnternet Zugangsprovider offers the possibility of surfen waiters a Proxy.

But note: If one uses its own lnternet entrance, thus no anonymous AOL entrance or Anonymizer or Proxy, then the operator of the Website, at whom one announces oneself by means of the wrong credit card data, can by means of the IP address, which the server logs, finds out, who betrogen it has and/or. it tried. In addition it needs to only contact and to it the IP address communicate your Zugangsprovider. The Provider leads i. D. R. over the last 80 days minutes, when who with which IP address on-line was.

Log in name checker

Some Pay Sites already gives during the logon procedure before the actual payment the possibility to possible new members of selecting a member name. If the desired name is already assigned, this is communicated and one is to select another name. Gives one for example "John" as member names, then mostly says the server that the name is already assigned. That is naturally one prima a condition for specified the above cheats for guessing passwords. Because now white one that there is already at least the name "John", thus must be only guessed the appropriate password. That is not at all white a substantial better initial position, as if one must guess passwords to Useramen, of those one whether they exist at all!
As Web masters of a Paysite one should make certain thus that the new member can select its user name only after verified payment!

Log in generator not surely

Often is it like that that the new member is sent for the payment of the Paysite to a credit card service (z.b. www. ibill. com). After Verification of the payment comes the new customer again to the sides of the Paysite and accordingly is then further-treated there. Usually it is sent after successful payment to a form, with which the log in data are produced. The new member can select a user name and a password and receives after choice of those immediate entrance. The form inserts the data automatically into the password file. Here however an often made error lies: One goes to production **a Usemame/Passwort pair simply by means of the "Back" Buttons of the Browsers back to the form, then one can produce a further pair of username/passwords in simple and legal way and that again and again.**

As Web masters one should use the following two protective mechanisms:

The credit card enterprise should convey a unique pin code, which one would then list from the still valid pin codes paints and so the form for username/password production with each payment only exactly ONCE be used can after successful examination. This procedure is called of most credit card enterprises also "One time Pin Hardcoding". The Script that the Usemamen/Passwoerter produces, should examine also by means of the HTTP REFERRF r Servervariablen whether the user comes also from the Kreditkartenuntemehmen. Otherwise a gewiefter hacker a Script can write, which tries different Pin Nurninern out from its computer simply until it finds a still valid. Those are pin z. B. seven-place, then it takes only 5000 seconds in the statistic means, until one finds valid pin, if the Scriptjede testct second pin. With a fast lnternelverbindung however also several tests per second are possible!

Pictures not in protected listings

This error is one the most frequent, since it will survey easy: As previously mentioned, the respective listing and all sublists are always protected by means of the HTACCESS protection. If the pictures of the member sides are however in a listing, which is not contained in this geschuetzten"Baumstruk tur ", then this listing and the pictures can be regarded therein without input of username/password. Particularly simply is it if also approximately do not list the picture listing is protected. Then entering the path is sufficient to list around all pictures. These picture listings have often the name "image" oder"gfx ", "pic", "pix", "pictures. .. .. pie. .. .. graphics ". Simple trying one after the other with something fantasy here already often leads to success.

That. Htaccess file lies in the protected listing "members". There also the HTML documents for the members lie. The pertinent pictures lie however in this example in the listing "image," which not in the members hierarchy are and are not thus not password-protected. It concerns for example www. pornsite. com as roots of these Paysite, then simply the URL www can in the Browser. pornsite. com/image are entered, and one receives a list of the collected pictures (vorrausgesetzt, the directory Browsing is not server-laterally switched off).

Pack Sniffing

This possibility is somewhat more complicated than the other described, because some Vorraussetzungen must be met: It must sit in a LAN (Ethernet Netwerk) at a computer and have root ACCESS. Then one can use a so-called "pack Sniffer" as for example "SNOOP". One finds pack Sniffer usually as C-Sourcecode in the InterNet. One must compile these short SOURCE codes then only by means of GCC on the UNIX Shell and is possible already it to hear the packages, which are sent to and of other computer in the LAN. Because Ethemet networks use the so-called "Broadcast" technology. A package that for a computer in a LAN is intended, is sent in principle to all computers in the LAN. Pack Sniffing is thus again particularly in the traps dangerous, with which one rents with a Webspace Provider its Web server and naturally with many other customers in a LAN is there. An example is www. pair. com, one the largest commercial Webspace Provider in the USA. There are over 70 Web servers in a LAN, on the z. Time. Upper 30. 000 customers a virtual Web server operate!

As protection against pack Sniffing the employment of a "Segrnenied offers itself networks". Used with such a network the Boradcast technology will not become, sondem the packages directly by means of Rouling tables the target computer geroutet. One for Web Smer suitable solution is particularly the employment of SSL (Secure Sockets Layer). This minutes ve@schluesselt all packages, which thus be still intercepted can, but no more can not be read. SSL is offered by most Webhosting enterprises against small surcharge. SSL coding Web contents are at the minutes Prefix"hnps: recognize. For the enterprise of a SSL protected Wcbsite one must have an Ssl ID, it for example with www. verisipn. CO gives. A small disadvantage is however that HTTPS connections are somewhat slower than usual HTTP connections, since a relatively high coding Overhead exists.

Trojan horses bake Orifice and NetBus

Bake Orifice:

The American group of hackers of Cult OF The DEAD Cow (HTTP: www. cultdeadcow. com) a program with the name published "bakes Orifice", which calls it "remote maintenance tool for networks". The fact that the intention is another results already from the name: Bake Orifice (rear opening) translates one here best with "back door", because the program makes it nearly the children's game to drive Schindluder with Windows PCS. Funny the allusion on MicroSoft's "bake Office" system.

Only 124 KByte the large "server module" can to any Windows EXE program be coupled, in order to put underneath it nothing-suspecting users. If the file under Windows 95 or 98 is implemented, the server latches itself quasi invisibly in the system. Of this moment on the Trojan horse waits only for over UDP minutes to be waked.

With the Client leave yourself comfortably on strike computers to access. Among other things one can manipulate the file system (files to down-load, magnify the importance of etc.. tasks terminate, uvm. The function mode bake Orifice is already from other hacker Tools well-known; the convenient operation of the graphic "maintenance component" is new primarily -- few inputs and Mausklicks are sufficient to manipulate in order to terminate processes to log keyboard entries the Windows Registry or reroute IP addresses.

One finds an interesting practice report under the German address

HTTP: www. puk. de/Back Orifice/default. HTML

or

HTTP: www. bubis. com/glaser/backorifice. htm

In order to examine your system on an existing bake Office, there are programs such as BoDetect, (hitp: www. spiritone. coni/ cbenson/current_projects/backorificefbaekorifice. htm) or the program Borf D (HTTP: www. st-Andrew. AC. uk/ sjs/boredfbored. HTML)

It is manually very simple in addition, bakes Orifice to remove: Open the Registry (regedit.exe implement) and look under the key

HKEY LOCAL

MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

after an entry with the name ". exe "(default file name) and/or. with an entry long 124.928 (+/- 30 bytes). Delete this entry; it causes that "bake Orifice" servers. with each Windows start one activates automatically.
The program lies generally in the listing "\Windows\System" and is recognizable from the fact that it does not have a program Icon and a size of 122 KByte (or slightly more) possesses. If you should not find the file for any reasons, it can help you that different information is to be found as ASCII stringer in the Prgramrn code; like that the character string is contained "bofilernappingcon" with large probability, which you will find over search in the Explorer.
Additionally to "bake Orifice Prgramm Datel" becomes in the same listing still the "WINE)LL. DLL "to the rnitloggen of keyboard entries installs, which delete you also meaningful way, which can cause however alone no damage.
The problem with bake Orifice is that it is difficult to explore the IP address of the host since this changes when each a selecting the stricken computer. This problem solved, and a still more powerful solution created Carl Fredrik Neikter with its program "Netssus", which is quite similar. It offers still larger functions and is simpler to install.

NetBus:

After you hemngergeladen yourselves the appropriate file have, you should unpack these. Now you receive to three files: NETBUS. EXE, NETBUS. Rtf and PATCH. EXE
With PATCH. EXE concerns it the dangerous lnfizierungsprogramrn, the actual Trojan horse. Do not start this file thus! D IE file NETBUS. Rtf contains a short English guidance the Authors. The file NETBUS. EXE is the "Client" with that you infected servers to access can. These can start you without concerns. Start for testing the server on your own computer, by opening a DOS request for input and starting in the listing of NetBus the server with the parameter, Jnoadd ", thus

PATCH. EXE/noadd [RETURN]

Now the server runs. Now you can start the Client (NETBUS.EXE doppelelicken) access and your own computer '. Select in addition as address "local host" or "127. 0.0. 1 "if you the server terminate wohlen, select you irn Client"Server Admin" and then "CLOSE server".

In addition the infecting program can be changed in such a way the fact that it sends automatically the IP address to one of them selected to email address as soon as with one of NetBus infected someone computers into the InterNet goes. This is the enormous advantage against-practices r bakes Orifice. In addition one selects the Button "server Setup" in the NetBus Client and enters the appropriate information. Difficult it is only to find a free Mail server the Mails of each IP address accepts. Then one selects "Patch Srvr" and selects the too patchende Infiziemngsdatei (standard massive "patch. exe").

Who tries to infect another computer the file PATCH can. EXE now simply by email to another more lnternetnutzer send and the file "Windows updates" or than any mad merry Anirnation call. The file can be renamed to it at will (z.b. Win98update. exe or siedler2_patch. exe etc..). If the file is now started, optically nothing happens. However the NeiBus server installed itself already on the computer hidden and from now on automatisc ' was started each time, if the computer is gebootet.

If one made above changes to lnfizierungsprogramm, one gets now always automatically email with the IP address of the infected computer, as soon as this on-line goes into the InterNet. This You can enter IP address now in the Netssus Client and manipulate the computer.

Hackers use for safety's sake anonymous email addresses, it for example with holmail. com or maii. com gives.

In order to protect your system, Norton is recommended anti-virus HTTP: www. symantec. more de/region/de/avcenter/which beside NetBus bake Orifice recognizes. They can work also again manually. That automatic NetBus start is registered in the Registry under "\liKEY LOCAL MACHINESOFTWARF, \Microsoft\Windows\CurrentVersion\Run" and should be removed. However the file name can vary (patch.exe, sysedit. exe or explore. exe are some well-known names)

Resuming ones lnfo find you under

HTTP: www. bubis. com/glaser/netbus. htm

Tip of the author

If you should intend to operate a password-protected InterNet service then you never come on the idea to use a Microsoft NT Web server! Windows NT has a safety system, which has more holes, as a Swiss cheese. Instead you should select a Unix Systein. Unfortunately German Webspacc Provider offers to NT solutions to a large extent. Here it is called thus, look out holds and with a Webspace Provider after a Unix server asks if necessary concretely! A substantial advantage of a Unix server is apart from security the advantage that one can log in there also by telnet and so substantially more controller over the server has. With NT Servem is not possible this! Recommendable and inexpensive current Web servers particularly are under BSDI or Linux. As everyone knows, Linux is even free and Apache, one of the best Web servers, is likewise free of charge available. In addition one should not underestimate also the performance advantages of a Unix system. Particularly within the range of Traffic strong Web offers almost exclusively Unix is used. You should thus for example an adult offer with many thousand fig. etc.. plan, then I put to you the employment Unix servers wftmstens to the heart. An interesting Website to the Thema"Unix vs. NT "is under
HTTP: www. lat mermany. com/maRazin/unix NT. htm

Legal aspects which the law says to "heels"?

§20à spying data:
1. Who provides unauthorized data, which are not particularly secured for it certainly and against unauthorized entrance, or another, with imprisonment up to three years or with fine one punishes.
2. Data in the sense of the paragraph 1 are only such, which are otherwise not directly perceptibly stored electronically, magnetically or or are conveyed.

§263 computer fraud: 1. Who damages the fortune of another with the intention of providing or third a rechtswiedrigen pecuniary benefit by the fact that he beinflusst the result of a data processing procedure by use of incorrect effects on the expiration is punished, with imprisonment up to five years or with fine.

§30á Datenveranderung: 2. Who itself rechtswiedrig data (§ 20à Abs. 2) deletes, suppressed, useless makes or changes, with imprisonment up to two years or with fine one punishes. 3. That Attempt is punishable.

§'303b computer sabotage: 1. Who stoehrt a data processing, which is for a strange enterprise, a strange enterprise or an authority of substantial importance, thus that he. .. a) an act after $ 30á Abs. 1 commits or for b) a data-processing system or a data medium zerstoehrt, damaged, useless makes, eliminated or changes, with an imprisonment up to five years or with fine is punished. 2. The attempt is punishable.

The career profile of the hacker

1.A Pemn, which investigates and tries gladly the details of programmable sytemen to expand their possibilities.

2. Someone, which programs enthusiastic (even obsessive) or rather programmed, than theorizing only over programs.

3. A person, whom chop VALUES to estimate white

4. A person, who is good to program fast

5. (disapprovingly) someone, that unrestrainedly everywhere interferes and tries information to uncover, by herumschnueffelt. Therefore password hacker, Network hacker.

The correct term is Cracker (Aufbrecher),

The term Hacker'beinhaltel often also the membership in the world-wide net community (z.B. internet). It implies that the described person adheres to the hacker ethics (hackers ethic). It is better of others than hackers to be designated than calling itself in such a way. Hackers regard themselves as a kind elite (a meritocracy, which defines itself by its abilities), however one, in which new members are very welcome. Therefore it lends a certain Beftiedigung to humans, as hackers to call itself to be able (if one however as hackers spends oneself and none is, one fast as a swindler - bogus - stamped).

The term to chop can designate the free intellectual study of the highest and deepest potential of computer systems. The determination can describe heels to keep the entrance to computers and thus information as freely and openly as possible. Heels the conviction felt by whole heart can include that in computers beauty exists that the aesthetics of a perfect program can release the thoughts and the spirit. ..

...outgoing of it that electronics and telecommunications are still to large part unexplored areas, it cannot be predicted at all, what hackers of everything to uncover to be able. For some is this liberty like a breathing of oxygen, the invention-rich Spontanitaet, which resists the life life makes and which doors to marvelous

Moeglichkei opens ten and individual power. But for many - and ever more becomes - the hacker is a ominoese figure, a besserwisserischer Soziopahl, which is ready to break out of its individual Wildnis and penetrate in other humans life, only around its own, anarchischen well-being being issued sake. Each form of power without responsibility, without direct and formal examinations and without reconciliation takes part in humans fear - and the right.

The hacker Crackdown

Anonymous working

You should not give anybody the possibility of making a profile of you in addition are the following to be considered:

Stops only too much well gotten used to hackers contact, if you exchange enamels with them, then should it with PGP encrypted be natural, to an anonymous account go (use no chopped account, better www. hotmail. com, www. yahoo. com. ..using a special Handles, which you use for nothing different one - you should change irregularly the action/account and provide naturally also a new PGP seckey pubkey for pair (also the passport cliche to change!).

Pay attention to it that your PGP key with at least 2048 bits key length is generated, in addition should you from safety municipalities not the 5. x version use, but with the old 2. 6.x version! !

If you want to absolutely rumtreiben yourself on the relevant IRC Channels, then change always yours nod and for change also your host (there many computers in the InterNet IRC Clients to have installed, you should not use Relays (or also IP'Source Routing and IP Spoofing, probier's out)

I know that changing of the Nicks is not so beautiful, because one gets thereby no Reputation with the broad mass; but Reputation is as deadly as useful (other hackers accept you immediately and are somewhat more geschwaetziger you opposite - around itself to form - however if you write first times so far bist'dass you your own Exploits, then you are anyway no longer dependent on the largest part of the hackers, and you do not meet the remaining so simply in the IRC)

Here so-called ReRouter, which passes a TCP on connection, is useful, which already in the regard is interesting, if one protected oneself against attacks of other hacker wants, if one caused too much annoyance on the IRC; -

Also here you could naturally use a special account fuer's IRC

My working environment

As point of A choice a large university with many Usern or a large Isp serves me. I use PPP instead of normal terminal programs around larger control of my connection to have to let run and because it is of advantage, over a line several sessions telnet, ftp.

A small computer serves me as Firewall and routs, I develops the PPP connection to my point of A choice and supervises all detailed packages. Furthermore I manufacture a Connection with SSH to the a choice computer, in order to pursue periodically all logged in user and network connections (which functions naturally only if the a choice computer is a Unix machine and no terminal server o. ae.). It is to be seen very interesting, what an administrator of everything makes, if it notices that somewhat with right things on its machine does not proceed. As soon as such sounding/investigations are noticeable to me, I break the connection off immediately, if I am however straight in a critical situation, must I DOS attacks use or the Admin out lock, in order to slow its work down, and/or. to prevent.

On the a choice computer it is not necessary to mask its present it is better to manipulate inconspicuously in the mass to submerge than any Logs.

The second, larger computer is my workstation, from here builds I a SSH connection to the first anti-trace computer on this anti-trace computer changes regularly, lies abroad and I has full control of it. From here I go over a further anti-trace computer to my Hacking computer; I have ' root' rights, the second RK computer am naturally only a simple TCP Relay also here, thus save I the stress with the log files eic. To Hacking computers in front I go into very safe Domains or chop from here on new Net@erke (it to exist naturally several this computer, which are changed besides irregularly), to scanning use I particularly a computer chopped for it which is scanners here all well hidden and additionally with 3DES coded.

The coded SSH connection is necessary, so that the Admins/Politessen cannot along-cut my activities at the point of A choice (or sonstwo).

If you have only one computer available, then you can protect yourself naturally also with the Firewall of Linux/FreeBSD/OpenBSD. It istjedoch more comfortably

to observe the connection over a special computer (I do not know, in what respect Linux and CO. a second monitor at a computer supports).
You still your Kemel should patchen, so that he supplies more to you with info. nations over detailed packages, thus are additional you able, DOS attacks, SOURCE Routing of attacks, Traceroutes etc.. to recognize and their origin.

Important one left

Resuming information is among other things here

HTTP://www.false.com/security

HTTP://www.insecurity.org/nmap

HTTP://www.secunet.com

HTTP://geek girl. com/bugtraq

HTTP://root-brightly. com

HTTP://root-brightly. com/doc

HTTP://www. sparc. com/charles/seeurity. HTML

HTTP://COMMANDS.com.inter.net/sod/

HTTP://www.phrack.corn

HTTP://www.cs.purdue.edu/coast/

HTTP://www.pilot.net/securityguide. HTML

HTTP://underground.org/

HTTP://www.lOpht.com

HTTP://www.infonexus.corn/-deamon9

HTTP://www.CERT.org

HTTP://www.CERT.dfn.de

ftp://ftp.blib.pp.se/pub/cracking

like that people that is nevertheless relatively instructive or? I wanted to use that as Vorgeschmack thereby their desire get my FAQ to read around it to get click up

HTTP://area66. notrix. de

or

HTTP://chc.notrix.net

or mailt me