Home

Search: type, hit enter

lolhackers.com School 4 Lulz

Track coverage (by Hatter and `)

Posted by xoxo on June 11, 2011 None comments

```
---Notes for the Track Coverage class ---
21:53 <@hatter> First rule of thumb for pre-compromise and starting your attack:
21:54 <@hatter> randomize your mac address.  use a laptop and public wifi.  use a
21:54 <@hatter> This class is mostly for post-compromize, but I'll at least throw
21:55 <@hatter> This is only for electronic attacks; not for basic docs work.
21:55 <@`> keep in mind that if you havent rooted/kitted a box netstat will show
21:55 <@hatter> When conducting your attack, use SSL if it is available.
21:56 <@hatter> Many intrusion detection systems and intrusion prevention systems
                using SSL.
21:56 <@`> and make sure you disable bash history, hide/disguise your processes a
21:56 <@hatter> unset HISTFILE ; unset HISTSAVE ; unset HISTCMD ; unset HISTCONTR
21:56 <@hatter> Can be used to disable the bash history of the compromized accoun
21:56 <@hatter> Make sure its the first command you run.
21:56 <%LordKitsuna> wouldnt ssl make it simpler to find you? since its a direct
21:57 <@`> hatter most boxes dont actually log bash hist until you logout
21:57 <@hatter> LordKitsuna: So's a plaintext connection.  Most proxies allow for
21:57 <@hatter> `: better safe than sorry
21:57 <@`> true
21:57 <%LordKitsuna> good point
21:57 -!- das1 [~Drew_Raci@LulzCo-B240C822.dhcp.mtpk.ca.charter.com] has joined #
21:58 <@hatter> The commands I pasted
21:58 <@hatter> Work for both a normal user
21:58 <@hatter> as well as a root user
21:58 <@hatter> The best thing to keep in mind is to attempt to minimize the trac
21:59 <@hatter> So in stead of doctoring a bunch of files later, you'll want to a
21:59 <@hatter> It makes cleaning logs much easier.
21:59 <@`> if you have root, btw, you can fuck with settings to keep less/no logs
21:59 <@hatter> on a UNIX system most log files are in /var/log/ , or in the daem
22:00 <@`> this should be obvious
22:00 <@`> but just throwin it out there
22:00 <@hatter> If you have rooted the system, the configuration files are typica
22:00 <@hatter> Also disabling syslog or metalog itself will usually prevent most
22:01 <@hatter> On Windows systems, the logs are performed by a system service vi
22:01 <@hatter> You'd have to use the sc.exe command to disable the logging servi
22:01 <@hatter> sc --help from a dos prompt should get you started
22:01 <@`> yeah killing syslog is a dead giveaway though hatter
22:01 <@`> ps aux | grep your-syslog-shit
22:01 <@`> hey theres nothing here
22:01 <@hatter> not disagreeing with you `
22:02 <@`> oh fuck we've been rooted
22:02 <@hatter> You can always replace the binaries with a loop that does nothing
22:02 <@hatter> of course, you'll have to watch out for integrity checking daemon
22:02 <@`> samhain's nasty
22:03 <@`> has a kernel mode stealth module
22:03 <@hatter> Yeah, I run it 🙂
22:03 <@`> basically a rootkit for your IDS
22:03 <@hatter> most of these daemons monitor file checksums of the programs as w
22:03 <@hatter> The second something changes, some send emails, other send SMS me
22:03 <@hatter> So when editing anything in /etc , /bin/ , /sbin , or /usr
22:04 <@hatter> its a good idea to check /proc/modules on the machine as well as
22:04 <@hatter> to see if there's any IDS systems running.
22:04 <%treysmee> snort?
22:04 <@hatter> Snort is a network layer intrusion detection system
22:04 <@hatter> Once you've breached the machine, you'll be dealing with system l
22:04 <@hatter> Snort will be irrelevant.
22:04 <%treysmee> pretty good one if the admin knows how to implement it properly
22:05 <@`> snorts a bitch too
22:05 <@hatter> If you have absolutely no choice
22:05 <@hatter> but to fire alarms
22:05 <@hatter> Then you'll want to write some sort of script
22:05 <@hatter> to trip ALL of them
22:05 <@hatter> fill it up with false positives
22:05 <@hatter> try to be the needle in the haystack
22:05 <%treysmee> gp
22:05 <@hatter> Keep in mind this is only if you have absolutely NO CHOICE.
22:06 <@hatter> Many rootkits use a kernel module
22:06 <@hatter> These rootkits will only work if there is modular support enabled
22:07 <@hatter> A good way to bypass this is by modifying the code to use /dev/km
                mounting it, rebuilding the kernel with the rootkit compiled-in,
22:09 <+FireStarter> you can use snipjoke on a linux server to help it be a pivot
                     the network
22:09 <@hatter> good point.  You can also use gre tunnels
22:09 -!- femto [45eb1a5d@LulzCo-B1EA63A4.mibbit.com] has quit [Quit: http://www.
22:09 <@hatter> Ultimately anything using encrypted traffic is good
```

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.

Last referers

- twitter.com/home
- www.lemon(...)1865.html
- twitter.com/
- bit.ly/ID1pwD
- www.twitt(...)g&mid=152

Top Browsers

- Google Chrome
- Firefox 5
- Firefox 4
- Firefox 3
- IE 8

Top OS

- WinXP
- Win7 x64
- Win7

```
22:11 <@hatter> As ` mentioned earlier in our planning
22:11 <@hatter> Edit logs, don't delete them.
22:11 <@`> anything not obvious is good
22:11 <@hatter> ^
22:11 <@`> for back connect shells you'll usually have arocess that sticks out li
22:11 <@`> thumb
22:11 -!- Emily [d5770f7b@LulzCo-5C546AF.mibbit.com] has left #school4lulz []
22:11 <@hatter> Staged shellcode, if available, is the best thing you can do --
22:12 <@hatter> it will allow you to run code on the same socket you came in on
22:12 <@hatter> in stead of creating a new connection
22:12 <@hatter> or opening another port.
22:12 -!- zaiger [~newfriend@OhIntehbutt.com] has quit [Ping timeout: 240 seconds
22:12 <@hatter> Additionally, polymorphic ascii encoders are a good idea -- don't
                generated code
22:12 <%LordKitsuna> so, you can mess with sys logs. but what about third party p
22:13 -!- zaiger [~newfriend@OhIntehbutt.com] has joined #school4lulz
22:13 <@hatter> You can find open files for a process in /proc/pid/maps
22:13 <@hatter> of course, replacing pid with the actual pid of the program.
22:13 <@hatter> its better to do this than use lsof; as lsof uses a lot more cpu
22:13 <@hatter> if you have to shred something or srm it, use nice +19 / renice +
22:14 <@hatter> additionally, you may want to use ionice 3 7
22:14 <@hatter> so that the disk io, as well as CPU usage
22:14 <@hatter> doesn't spike
22:14 <@hatter> Many systems have built in cpu monitors and built in IO checks, f
22:14 <@hatter> If you alert them, its game over 9/10 of the time.
22:15 <%LordKitsuna> my vpn hag such a huge i/o spike rapidxen paused my vps. nev
22:15 <@hatter> some example staged shellcode is available at
                http://www.wildcardsecurity.com/security101/index.php?title=Secon
22:16 <@hatter> The tricky part though
22:16 <@hatter> isn't just syslogs
22:16 <@hatter> You'll run into binary log files
22:16 <@hatter> for example, /var/log/wtmp
22:17 <@hatter> You'll have to either find a script, write one, or use a hex edit
22:22 <@hatter> pm me questions people
22:22 <@hatter> before we move on
22:22 <~Fox> Gents, brb restart
22:22 <+nyann> questions on what?
22:22 <@hatter> Anything you didn't understand
22:22 -!- Fox [~Fox@20F6D212.F71AD6B7.1ABC39CD.IP] has quit [Quit: Textual IRC Cl
22:22 <@hatter> I'll at least link you guys somewhere
22:22 -!- mode/#school4lulz [-m] by God
22:22 <@hatter> to read up
22:23 <+nyann> I guess it's important to know how to write assembly
22:23 <+nyann> I never learned that
22:23 <@hatter> http://www.wildcardsecurity.com/security101/index.php?title=Assem
22:23 <%God> ` you fuck with metasploit?
22:23 -!- hexatron [~herp@LulzCo-C7486A9.hsd1.fl.comcast.net] has quit [Quit: Pin
22:24 <+FireStarter> I'm pretty good with metasploit
22:24 -!- hexatron [~herp@LulzCo-C7486A9.hsd1.fl.comcast.net] has joined #school4
22:24 <%God> i need to start fucking with it
22:24 < Eugenicist>  Not much to it
22:24 <+FireStarter> its good stuff
22:25 <+FireStarter> meterpreter is awesome
22:25 <%God> true that
22:25 -!- Eugenicist is now known as Pathogen
22:25 <+FireStarter> meterpreter is nice beacuse it doesnt write to the hdd
22:26 <+FireStarter> so less logs
22:26 <@hatter> ^
22:26 <@hatter> Living in the ram is really the best idea
22:26 <+FireStarter> and the encoding tends to get around some ids and ips
22:26 <+FireStarter> i think theres a way to encode the stage too
22:26 <@hatter> Yeah there is
22:27 <+FireStarter> metasploit is better used once your past the outer defenses
22:27 <%LordKitsuna> couldnt living in the ram give you away if they notice their
22:27 <@hatter> sure,
22:27 <+FireStarter> meterpreter is super small tho
22:27 <@hatter> most linux servers are kinda greedy on that though
22:27 <@hatter> Besides, anything you want to live in ram
22:27 <@hatter> should be relatively small
22:27 -!- hexatron [~herp@LulzCo-C7486A9.hsd1.fl.comcast.net] has quit []
22:27 <@hatter> a kilobyte or two
22:27 <@hatter> is unnoticeable.
22:27 <%LordKitsuna> ah
22:28 -!- dark is now known as cloned
22:28 <+FireStarter> and that wont trigger alarms
22:28 <+FireStarter> most alarms trigger when the ram is almost filled
22:28 -!- cloned is now known as dark
22:28 <+FireStarter> like 85+%
22:28 <%LordKitsuna> i watch ram use religosly for some reason
22:28 <@hatter> even normal monitoring systems
22:29 <@hatter> will mark that machine as problematic
22:30 <%LordKitsuna> since i had that huge i/o spike on my vps for seemingly no r
22:30 <%LordKitsuna> and now all these storys
22:30 <%LordKitsuna> im like god damnit now im wondering
22:30 <@hatter> filesystem based rootkit?
22:30 <@hatter> go check your fs driver
22:30 <@hatter> for the format
```

- Linux
- MacOSX

Δ Top

Visitors Online

251 visitor(s) online

powered by WassUp

Archives

June 2011

```
22:30 <@hatter> if its an ext3 drive check that
22:30 <@hatter> see if there's networking code in it
22:30 <@hatter> lol
22:30 <@hatter> additionally
22:30 <%treysmee> heh
22:30 <@hatter> BSD has an app called badsect
22:30 <@hatter> its used to mark sectors as bad on the drive
22:30 <%LordKitsuna> i have no idea what your saying lol fairly new to linux i as
                     time maybe he will
22:31 <@hatter> good way to hide files
22:31 <+FireStarter> alt streams are a good way to hide it on ntfs
```

Doxing (by Fox)

Posted by xoxo on June 11, 2011 None comments

```
---Notes for the Docs class (I personally see no point in this) ---
20:46 <~Fox> So first off, I want to get his IP, email, anything.
20:46 <~Fox> So what I'm going to do to get these
20:46 <~Fox> is this
20:46 <~SexyBitch> Oh Hey Clone
20:46 <~SexyBitch> wassup bb
20:46 <~SexyBitch> wanna cybersex
20:47 <~SexyBitch> plz give me ur email and usernames
20:47 <~SexyBitch> oh ya
20:47 <~SexyBitch> look at my pix
20:47 <~SexyBitch> sexybitch.com/pussy.jpg
20:47 <~Fox> NOW ARMED WITH THIS INFORMATION I AM READY TO FACE CLONE IN BATTLE.
20:49 <+Nyse>  nc -l 80
20:49 <+Nyse>  nc -l 80 -vvv
20:51 <+Nyse> unless you can social their ISP
20:51 <+Nyse> it's nearly worthless.
20:55 <%treysmee> with said dox you can pretend to be that person in order to inf
20:55 <~Fox> We're going to go through the basic steps of checking social network
             information to find out things about the target
20:55 <+clone> fox, i dont disagree at all. i just start a different way.
20:57 <@hatter> The best way to find the social network stuff
20:57 <@hatter> Is definitely with http://pipl.com/
20:57 <~Fox> at the end of the day
20:57 <~Fox> Their name.
20:57 <%xoxo> hatter: you're the man
20:57 <~Fox> Their Address
20:57 <~Fox> their family.
20:57 <%God> pipl is sick as fuck
20:57 <~Fox> That's all that matters
20:57 <~Fox> and pipl
20:58 <~Fox> So in talons case
20:58 <~Fox> Anyone actually tried searching up good old talon?
20:59 <~Fox> PM me if you think you got it
21:00 <~Fox> ok.
21:00 <~Fox> Talon. Maryland.
21:00 <~Fox> Find him and PM me with docs
21:00 <~Fox> Use google, Pipl,
21:00 <~Fox> should be an easy get.
21:01 <~Fox> Whiteh8
21:01 <~Fox> again vigorously getting at it
21:01 -!- mode/#school4lulz [+v whiteh8] by Fox
21:01 <~Fox> tell em how you found him
21:01 <~Fox> and what you found
21:01 <+whiteh8> ?q=talon maryland h0no
21:02 <~Fox> so with a little background info
21:02 -!- bufUnd3rfl0w [~bufUnd3rf@LulzCo-46D1B5F.torproxy.org] has quit [Quit: l
21:02 <~Fox> he found our target from a prior dox drop
21:02 <~Fox> care to share what you found whiteh8 ?
21:02 <+whiteh8>  cyber_talon@hotmail.com or cybertalon@gmail.com
21:03 <+whiteh8> talon:x:1000:1000::/home/talon:/bin/bash
21:03 <~Fox> So we now have an email for the target. Cached by lovely lovely goog
21:04 <~Fox> There is a company attached to this person, plus full docs if one se
21:04 <+whiteh8> checking
21:05 -!- AloneTrio [~nonameno@LulzCo-3476163.fbx.proxad.net] has joined #school4
21:05 <+whiteh8> g0fault
21:05 <@`> got his livejournal
21:05 <~Fox> Ok so we got a LJ
21:05 <~Fox> More information about the target
21:05 <@`> ctal0n
21:05 <~Fox> Come on guys, PM me if you got anything
21:05 <@hatter> Probably lots of personal info there
21:05 <~Fox> This miserable fuck is a kiddie raper.
21:05 <@hatter> That's found by searching for cyber_talon@hotmail on pipl.
21:06 <~Fox> [14:06:05] Shidash: tal0n/skew/bandit/luck0elduck
21:06 <~Fox> [14:06:15] Shidash: Those are other aliases
21:09 <~Fox> ole_one_eye may have it.
21:10 <~Fox> Nope :/
21:10 <+whiteh8> AIM: unixroot102
21:10 <~Fox> Getting closer
```

```
21:10 <~Fox> so fucking close
21:10 <~Fox> Come on
21:10 <+Omega> Birthday: 08/05/1983
21:10 <@hatter> ding ding ding
21:20 <@hatter> http://ja.pastebin.ca/855720 kids
21:22 <+whiteh8> "talon jason md pastebin" returns it
21:22 <+Omega> https://encrypted.google.com/#hl=enf&q=%22talon%22+%22maryland%22+
21:27 <%LordKitsuna> the home phone appears to be good still
21:28 <@hatter> http://anywho.com/rl.html
21:28 <+clone> it takes incoming calls.
21:28 <@hatter> you can verify home phone addresses with that
21:28 <~Fox> So Skype, SpoofCard, Throwaway burners
21:28 <@hatter> boost is a good company for burners because you can select your o
21:28 <~Fox> ProTip ^
21:29 <%LordKitsuna> google voice?
21:29 <@hatter> LordKitsuna: too trackable
21:29 <~Fox> Google Voice with a bounce not attached to your name in any way
21:29 <~Fox> GREAT
21:29 <@hatter> LordKitsuna: google records every call and cooperates with law en
21:29 <~Fox> Cause guess what
21:29 <@`> voogle goice
21:29 <~Fox> makes it twice as hard.
21:29 <~Fox> So Burner + Google Voice = Ok
21:29 <~Fox> Misdirection
21:29 <%treysmee> red boxing still works in certain areas/phones o.o
21:29 <@`> speaking of which
21:29 <+Omega> Now that M$ has Skype, I wouldn't use that either.
21:29 <%treysmee> very rare, but still
21:30 <~Fox> just know, that you'll be dealing with heat.
21:30 <~Fox> You gotta be a little bit of an actor hear
21:30 <%treysmee> also, creating a Linemans Handset AKA Beige Box is the lulz
21:30 <~Fox> *here
21:30 <%treysmee> thats a talk i could give sometime
21:30 <~Fox> When you call up the police station
21:31 <%treysmee> not many know how many spots you can access the telco
21:31 <~Fox> you immediately need to sound convincingly like your life is in dang
21:31 <@`> Fox, have them show you their guns on webcam
21:31  * treysmee idles, sry
21:31 <@`> while waiting for the swat team to arrive
21:31 <~Fox> there is an immediate threat to the home, and to the person.
21:31 <@hatter> If you can't hold a straight tone of voice
21:31 <@hatter> its best to record it
21:32 <@hatter> and play it back into the phone
21:32 <@hatter> during the cal.
21:32 <@garrett> ^
21:32 <@garrett> or pay a friend
21:32 <~Fox> Do NOT DEVIATE.
21:32 <~Fox> While on the call
21:32 <~Fox> you MUST
21:32 <%treysmee> nearvousness helps, as long as youre loud
21:32 <~Fox> STAY in CHARACTER.
21:32 <~Fox> Cry, if you can do that, baited breath, panting
21:32 <~Fox> all of those things can help sell the fact
21:33 <~Fox> that a big black nigger is in your house with a gun and is going to
21:33 <~Fox> please help us mr. police officer.
21:33 <+whiteh8> LOL
21:33 -!- `` [~Squirrel@82E597C.5202E511.FA6DD7A0.IP] has left #school4lulz []
21:33 <~Fox> Sell the story but don't over sell
21:33 <+clone> im sorry but why would you not play the perpetrator instead of the
21:33 <~Fox> Man 6 six foot, black, shotgun, mom is tied up
21:33 <+clone> ^
21:33 <~Fox> clone it's your choice
21:34 <~Fox> I've gotten a full scale set of two teams to raid a house from one o
21:34 <~Fox> Watched that shit over a street cam.
21:35 <~Fox> SWAT, Pizza, UPS, credit card fraud
21:35 <@hatter> oh
21:35 <@hatter> One more thing
21:35 <~Fox> whatever.
21:35 <@hatter> Go to the bookstore
21:35 <@`> theres a guy called nachas h writing a doxin guide
21:35 <@hatter> get all those little sign up shits
21:35 <@hatter> for magazines
21:35 <@hatter> where it gives you a free month
21:35 <@hatter> but then starts sending you a bill
21:35 <@hatter> fill out like 50 of those
21:35 <@hatter> spam out the mailbox
21:35 <@hatter> always kinda funny
21:36 <%God> i personal like opening up free cell phone accts
```

« Previous page