The Ultimate Account Hacking Guide

By Draco Red

Disclaimer

The author and publisher of this eBook and the accompanying materials have used his best efforts in preparing this eBook. The author makes no representation or warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this eBook. The information contained in this eBooks is strictly for educational purposes only. Therefore, if you wish to apply ideas contained in this eBook, you are taking full responsibility for your actions. The author disclaims any warranties, merchantability, or fitness for any particular purpose. The author shall in no event babe held liable to any party for any direct, indirect, punitive, special, incidental or other consequential damages arising directly or indirectly from any use of this material, which is provided "as is", and without warranties. As always, the advice of a competent legal, tax, accounting or other professional should be sought. The author do not warrant the performance, effectiveness or applicability of any sites listed or linked to in this eBook. All links are for information purposes only and are not warranted for content, accuracy or other implied or explicit purpose. This eBook is copyrighted. No part of this may be copied, shared, or changed in format, sold or used in any way other than what is outlined within this eBook under any circumstances!

Table of Contents

Introduction

One of the things I've seen time and again, throughout the web, is the question, "How do I hack X?" Well, wonder no more, as you now have the one, all inclusive guide to hacking. The best part is that this guide can be applied to any type of hacking you want. Ebay? Yup. Paypal? Ditto. Facebook? Included. Email? Anything and everything; because this isn't a cookbook telling you the step by step "now type h t t p colon slash slash…" but rather it's a step by step guide to the process of hacking.

I'm not going to lie to you and tell you that once your done reading this you'll have magic powers to whistle into a phone and start a thermonuclear war; there will be things that are frustrating, tedious, and you will fail on occasion. This happens and is all part of the game. But a game it is, and what a glorious one at that.

This guide is written primarily around hacking into personal accounts, such as email, social networking, online stores and the like; but it's also applicable to more specialized accounts such as employee intranet accounts and the like.

Some of the information will also be applicable to other hacking situations, but the process of hacking an individual account is far different from that of hacking online storefronts or building up botnets.

The examples used in this guide are hypothetical and shouldn't be taken as admission of guilt to any crime or infraction. Any specifics are works of fiction, and shouldn't be taken as anything else.

Targeting

Who:

The first step for a targeted hack is, naturally, having a target. In some cases it's a person, but others it may be a business' social networking account or a specific email address. But the more you can hammer down who you're going after the better.

Are you looking to hack your ex's accounts? If so then you should have it down to what accounts they have that you want to access; do you need their email, their facebook account, their paypal account? It may seem self apparent, but this is an often overlooked step that can make or break your efforts. After all, the first step in achieving something is having a good working knowledge of what you're looking to achieving.

This will also help you prevent loosing focus and shifting from one target to another before you're able to finish; and believe me that this can happen very easily without even being noticed.

Objective:

The next thing that goes hand in hand with this is laying out your objectives. After all, your real objective isn't to "hack X", but rather hacking that account is itself a means to an end.

Are you trying to access their emails? If so, is it a specific email for are you looking to monitor all future emails. It's important to have clear criteria for what you're trying to do, as the steps involved can be very different for one or the other.

For example, if you just need to read one particular email, you can use the "forgot my password" feature to change their password, and access their email that way. But if you need ongoing access that won't work, since as soon as they're unable to log in they'll change their password again.

You *could* prevent that by going into their account settings and changing the account recovery questions / answers, but then it'll be obvious to them that they've been compromised. You have to decide before had if this is acceptable, or if it will prevent you from obtaining your later goals.

Obfuscation

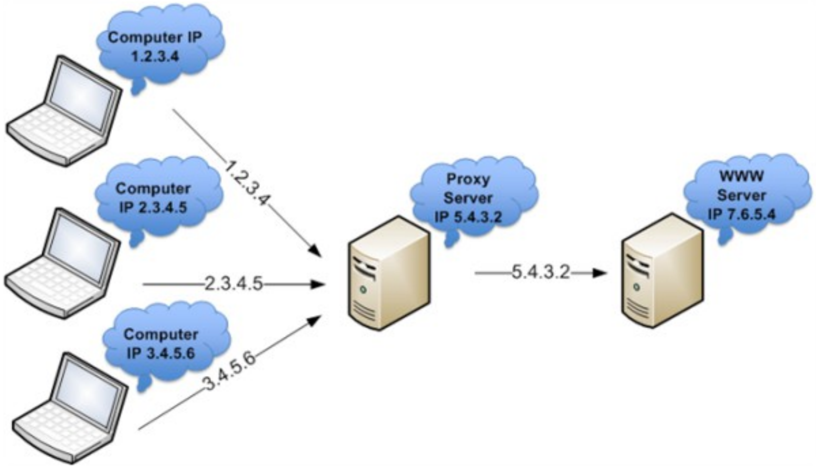
Obfuscation is the art and science of hiding who and where you are. This can often be the difference between getting off scot free and getting jail time, so it should be a topic near and dear to your heart.

Of course there are many ways to do this, and it largely depends on the techniques that you're using, but I'll cover some of the tried and true methods here.

Digital:

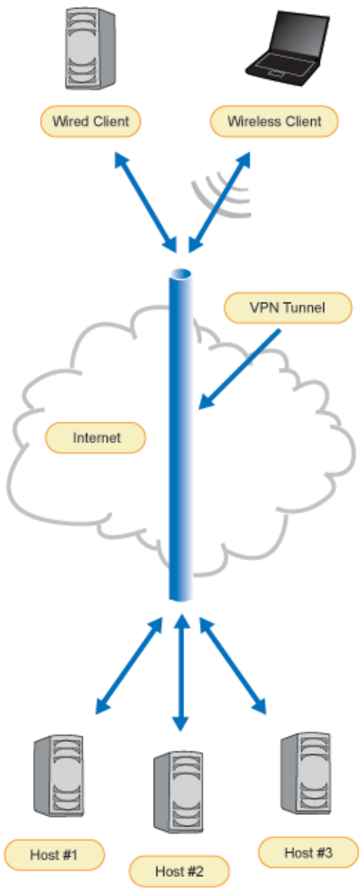
Proxies and VPNs: Using some form of a proxy is a must; for those who don't know a proxy is a system that acts as a relay between you and whatever systems you are accessing on the internet. This allows for the trail to lead to the proxy, but after that it drops off, hopefully leaving you fully protected.

The most common types of proxy services use the SOCKS5 protocols, these offer alright performance and once set up are very transparent, meaning that you navigate normally without really noticing that you're going through a proxy. They also let you hide most traffic; including email, remote admin connections and others.



A less common form of proxy is a PHP based web proxy. With these you would navigate to the proxy's page as you would any other website, enter the URL of the website you want to access and it acts as a go-between for you and the remote website. However the downside with these is that if you open a different window, or type in an address directly in the address bar you're no longer protected. They also fail to protect emails (other then webmail services) and can sometimes have problems with pages that use javascript or other active components.

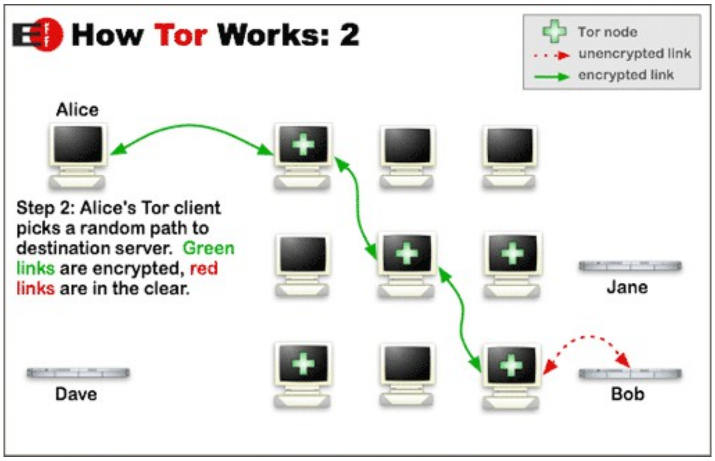
The big benefit of a web proxy is that they're simple to set up, and with minimal experience you can roll your own on any server that supports PHP and cURL. I've personally used PHProxy and it works quite well. Other alternatives are PHP Web Proxy and Glype. I've only used the one, but all three are free for personal use so it can't hurt to experiment. These aren't a first line of defense by any means; but it never hurts to have one available for those "just in case" types of situations.



VPNs work under the same general notion as a proxy, piping traffic to a remote location to hide who you really are. The implementation is different, in that the VPN connection shows up on your computer as another network connection, so it's as though your computer is connected directly to the remote network. This can be a good thing, making sure that all your traffic goes out via the VPN, but it can also possibly leave you open to having your IP linked to traffic that could identify you.

One of the main benifits of using a VPN over a SOCKS5 proxy is that VPN traffic is encrypted between you and the VPN server; while normal proxy traffic is sent un-encrypted. This means that if you're only using a proxy, it's possible for someone to intercept the traffic between you and the proxy server. The other big draw of using a VPN is speed; VPN connections tend to be much faster then proxy servers. Proxy servers often try to overcome this by caching data; this gives better performance but the down side is that it's storing information that could identify you or your activities later on..

But be warned, some proxy VPN providers keep connection logs, so they could be subpoenaed and forced to turn over information regarding your activities and identity. Doing so requires both money and cross-jurisdictional cooperation; both of which are in short supply for most government agencies. It's unlikely to happen, but it's still a good idea to look for a provider that explicitly doesn't keep those traffic logs. A good, if somewhat outdated, guide can be found here: http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/ I personally use Private Internet Access who are quite cheap, have good speeds, accept payment from a number of sources (including bitcoin) and provide both full VPN and SOCKS5 proxy service.


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

TOR: No discussions of proxies would be complete without mentioning Tor. Tor is a peer to peer proxy network that encrypts your traffic and then passes it through a number of different computers in order to hide where the traffic is coming from and where it's going to. By passing the traffic through a number in intermediaries the goal is to provide an almost perfect anonymity. Because of this, traffic coming from known Tor exit nodes is often viewed as being suspicious, so you may not be allowed to access some services. But for general traffic and research it is a must, you can download it from here: https://www.torproject.org/download/download

Open networks: Open wireless networks are an immense help for those who want to hide their tracks. Thanks to the proliferation of consumer high speed internet services and WiFi routers, there's a huge pool of people who have a network but don't know how to properly use or secure it. Perhaps the most invaluable tool I've found for exploiting this is a USB wireless adaptor with an external antenna. Thanks to the industry standard RP-SMA antenna connector on it I was able to pick up cheap high gain antennas to vastly increase my signal strength and range.

While most cards ship with a 3 DBi antenna, you can pick up a 9 DBi omni-directional antenna on amazon.com for under $5, including shipping. Even higher gain directional antennas are readily available as well, including DIY "Cantenna" solutions. One thing to remember when shopping for antennas is that the DBi is a logarithmic scale, so signal strength approximately doubles for every 3.3 DBi; so a 9 DBi antenna is almost twice as good as a 6 DBi.

If you happen to have an old or obsolete Android based phone, you can combine the two approaches. Using an app such as Servers Ultimate (free, Google Play), you can turn your Android phone into a proxy server. Just find an open wireless network, set up port forwarding and Dynamic DNS in their router and you're good to go (provided that they haven't changed the password from the default for their router). It's best if you can find a power outlet near by for your phone's charger so that you can just plug it in and hide it somewhere; allowing you to have your own free, anonymous proxy service.

Physical:

There will come times where you will have to go out there in person to do something, and this is where physical obfuscation comes in to play. Basically this is anything you do to hide your identity in person; it could be a disguise, fake IDs, disabling security systems or anything else for that matter.

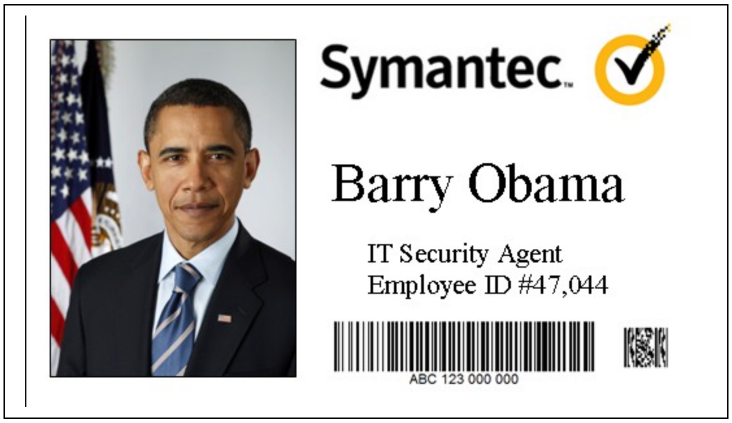
Often when asked to explain this I'll use the example of the Ninja. When most people think of a Ninja, they think of the martial artist dressed all in black and carrying swords and all other implements of death. But when it comes down to it, the Ninja's job is to be undetected, so they would be far more likely to be dressed as a farmer and carrying only farm implements. If they were in a royal residence they would look like a courtier or guard. The goal is to blend in, and to have no discernible differences from anyone else there so it would be impossible to describe them without also describing everyone else there.

So always dress as you would be expected for the situation. If everyone around you wears baseball caps, then you should too. If it's all suites, then you wear a suite. If you're in Boston, wear a Red Sox jersey and not a Yankees one.

However there can be situations where dressing differently from those around you actually helps you to blend in. By wearing a uniform you can often gain instant acceptance, and by looking like a janitor or other form of menial laborer you can instantly become a part of the background and nearly invisible. This can quickly backfire though, as a gardener or pool boy has no reason to be in their employer's personal office or study, while a janitor would not be noticed. Being out of place in such situations will instantly make you far more visible then you would be otherwise, so think ahead as to where you'll be going. One of the handiest things to have is a pair of black slacks, white button up shirt and black tie. I.E. the "Geek Squad" dress code. Odds are good that you're going for the computers, so dress and act as though you're supposed to be there.

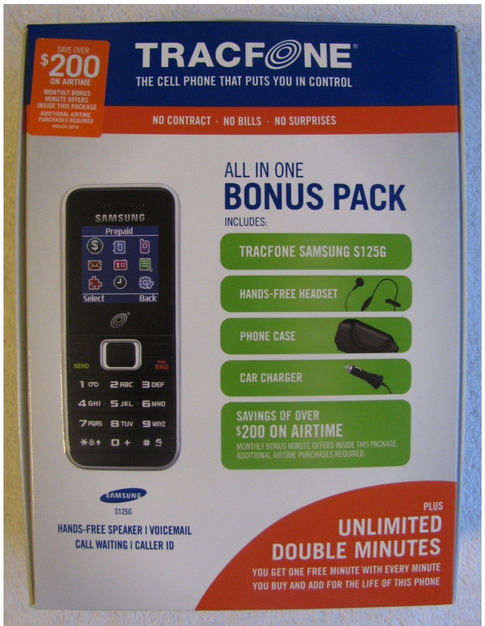
This is not me, It's just my body vehicle

Depending on the situation you may need to have a fake ID; this can be as simple as a name tag, to as complicated as a full fake drives license with matching credit and grocery discount cards. If your budget allows for it and you have a good fake ID you can rent a car for transportation. If not then it's sometimes handy to have a "spare" set of license plates. I harvest the rare earth magnets from dead hard drives and these make for very nice "quick releases" for a spare license plate. They're strong enough to stay on but can quickly be pulled off the car and discarded.



Seems legit.

Remember to be prepared, but not over prepared. You don't want to get busted for using a fake driver's license when a home made corporate ID would do the trick. Buying a PVC ID card printer is overkill for most people, but you can get quite far with a home "print your own business card" kit and DYI lamination stickers. When making a fake ID; it's best to do one that whoever will be looking at it won't know exactly what it *should* look like. Almost everyone has a driver's license, so everyone's seen them and will know if there's something off with it. But how many people outside of Symantec have seen and know what their corporate ID looks like? Name, photo, corporate logo, employee ID number; it has too look like *an* ID, not necessarily look like *their* IDs.


SAVE OVER $200 ON AIRTIME
TRACFONE
THE CELL PHONE THAT PUTS YOU IN CONTROL
NO CONTRACT · NO BILLS · NO SURPRISES
ALL IN ONE
BONUS PACK
INCLUDES:
TRACFONE SAMSUNG S125G
HANDS-FREE HEADSET
PHONE CASE
CAR CHARGER
SAVINGS OF OVER $200 ON AIRTIME
SAMSUNG
HANDS-FREE SPEAKER | VOICEMAIL
CALL WAITING | CALLER ID
PLUS
UNLIMITED DOUBLE MINUTES
YOU GET ONE FREE MINUTE WITH EVERY MINUTE YOU BUY AND ADD FOR THE LIFE OF THIS PHONE

Of special note is the utility of having a burner cell phone handy. It used to be when I was selling electronics, we would get people in asking for "disposable" cell phones; and at $40-50 minimum we would have to explain that they weren't really disposable, but prepaid phones. That however has changed, thanks to increased competition in the prepaid market. Walmart now sells a Tracfone, the Samsung S125G, for less then $10 that gives you 60 days service and 20 minutes talk time. Granted, 20 minutes isn't much, but with how many services require a phone call to confirm your identity, it's a small price to pay for a completely anonymous, temporary phone number.

Profiling

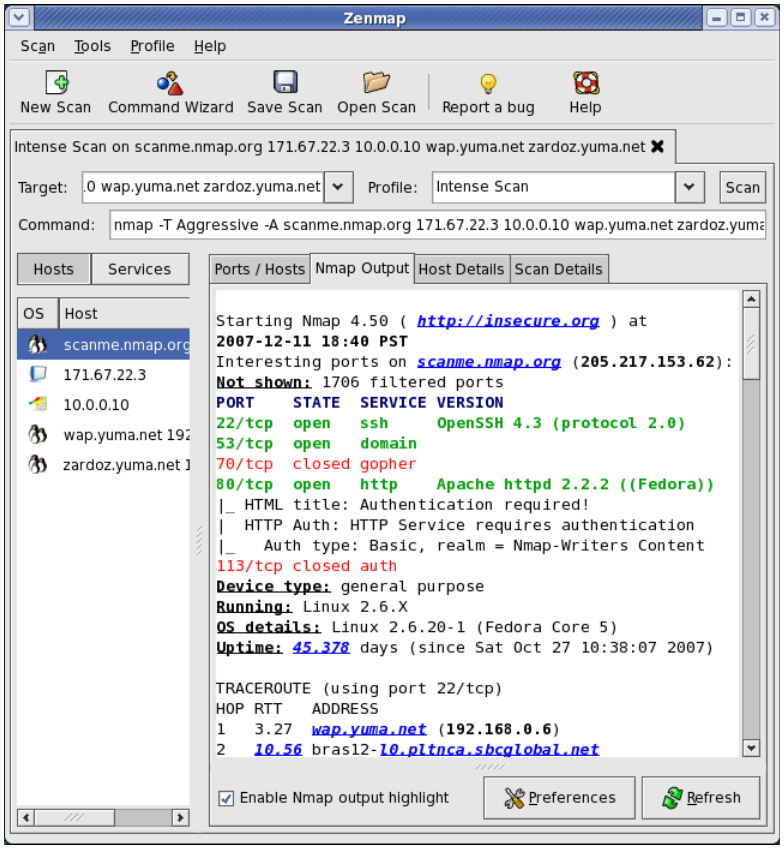
Hacking is in essence a form on identity theft. You're convincing the remote computer that you are in fact the target, and in order to do so the more you know about your target the better.

You would be amazed at the amount of information that's out there for the finding. If your target has a social network account then set up a fake account and friend them with it. From there you can usually find out where they went to school, their birth date, parent's names, children's names, their likes, their hobbies. Pretty much anything that would be a password recovery question is there for the finding.

You can run a reverse email or username lookup on services like Spokeo; run a background check on them using services such as BeenVerified. Both require a subscription; but if you go ahead and run your own username or email address on their free services you can get an idea what they can offer.

If possible observe them directly. If their computer is near a window, then grab a pair of binoculars. Do they use a PC or a

Mac? Do they check their facebook profile obsessively; do they play online poker until 3AM? Do they have a cat, or breed Rottweilers? Knowing their interests will give you a way in to their lives; both in person and online.



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net ✖

Target: .0 wap.yuma.net zardoz.yuma.net   Profile: Intense Scan   Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

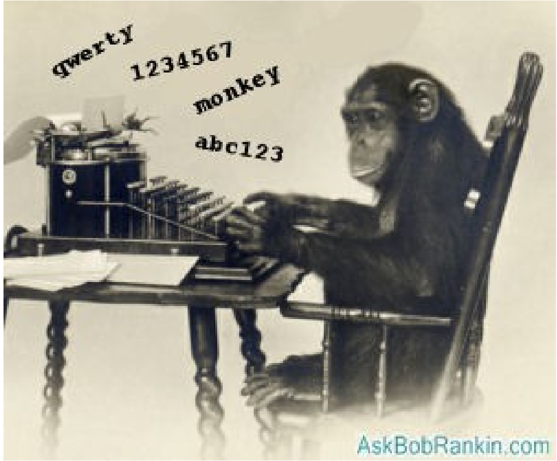
☑ Enable Nmap output highlight

If direct observation isn't possible then electronic observation is your next option. If you're able to access your target's wireless network then you can scan for the devices on their network, using a scanner such as Nmap, or simply check out the "Network" section in Windows Explorer to see what you can find. People will often have a quite a bit of their lives open and shared to anyone on their network, and this is something that you can readily exploit. If you can't access their network from the inside, you may be able to scan their computer directly over the internet. By getting an email sent to you from your target you can usually get their IP address from the email headers. If you're lucky, the target will have their computer directly connected to the internet, and you can scan them directly.

The target's computer and network isn't the only thing to observe online. This is also a chance to observe the target's personality. Where ever your target frequents online, you should make a few accounts. Befriend them with one, and troll them with another; gauge their reactions to being provoked, and the language that they used. The better you are at reading them, the better your chances are of being able to find out what you need from them later on.

Weak Brute Forcing

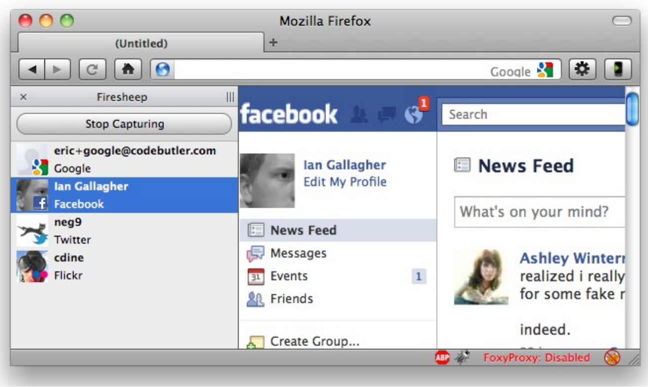
Next step is to go out and just try what you've found. Guess at what their password might be; get a list of the most commonly used passwords and try the first couple dozen from the list. Try their girlfriend's name, the name of their cat, what ever you've found to be important to them. When people are pressed to make a password, the things that are closest to their mind are often the ones that they'll choose.



This method is placed first because it has the best reward for the least effort. And because of that there's no real reason not to go for it. Sometimes people will have very weak, very obvious passwords, and you'll never know if you don't check. Success at this stage is low, but it's still high enough to make this a worthwhile endeavor.

Technical Exploits

This is what most people think of when they think about hacking; a security vulnerability that leaves the system open for the taking. Unfortunately these are almost never real; tending more towards legends and myths then anything practical.



Any technical exploits out in the wild tend to be more aimed at targeting individual computers; useful for building a botnet or spreading a worm, but all that useful in getting their email or facebook accounts. A huge exception to this is the existence of cookie and session hijacking tools such as the Firesheep firefox add-on and the FaceNiff Android App.

As always, Google is you're friend. Read, research and study up on possible vulnerabilities for whatever system you're trying to access. You will run into a number of false leads and dead ends, as well as numerous reports of vulnerabilities that have been closed and fixed for years, but every once in a while you strike gold.

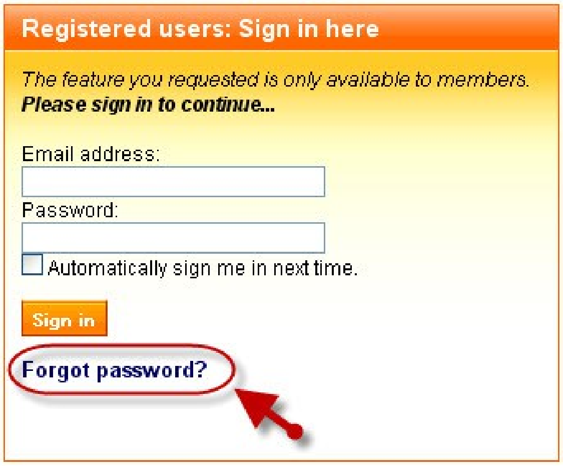
Be sure to keep your guard up, when doing your research. There's a huge industry out there involved with selling fake information or tools, knowing that if the people they're scamming are up to no good themselves then they're very unlikely to report a scam, because doing so will implicate themselves. Con artists know that the best way to disarm someone is to let them know that they're involved in a scam, but make them think they're on the winning side of the scam until it's too late.

Social Engineering

Ahh, now we're down to the meat and potatoes of hacking. Social engineering is the practice of tricking your target into giving you the information or access to the information you need. Sometimes it can be as simple as just asking them their password, but usually there's at least some level of subterfuge involved.

There are two main approaches in this; ether impersonating your target or impersonating the people with whom they have the account.

Impersonating the target is lower risk, but does have some draw backs. This is where the majority of your research comes in to play. If it's acceptable to change their passwords, then the account recovery feature is your first stop. Go through the process, guess the answers to their verification questions and your in. If you're not able to do that, then a call to tech support may be in order. See if they can give you the password or change the password for you, the worst they can say is "no".



Registered users: Sign in here

The feature you requested is only available to members.
Please sign in to continue...

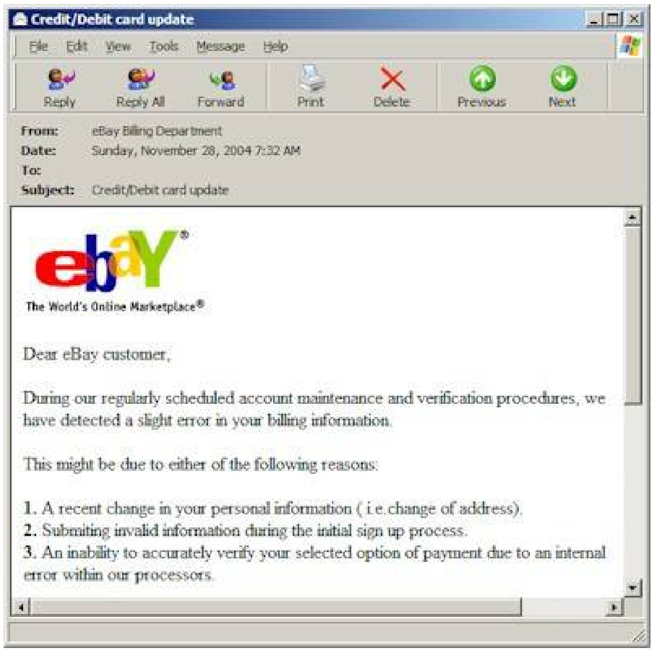
Email address:

Password:

□ Automatically sign me in next time.

If you get no luck or changing the password isn't an option, then you're going to have to make contact with your target. Sending them a phishing email is a low risk starting move. With these, the more sophisticated the better. If you don't know how to make a web page with form submit, then you're pretty much stuck with a "reply with this information" email. But even those are successful a distressing amount of the time. If you've the knowledge to make a webpage then all the better.

Many ISPs provide free web space with every email address, so there are situations where you can have your page at www.TargetISP.com/account_recovery. If that's not an option then it you can use a low cost/no cost domain registrar you can get an associated domain to host your page. Look to see what's available, TargetISP-Security-Processing.com, Accounts-TargetISP.com, or other combinations there of. So long as it looks legit, the target will likely not look too closely at it. Google is currently offering a free domain name and year of hosting at http://www.gybo.com, so take advantage for all the free domain names you need. When making the page copy the layout, graphics, and formatting of the main site; doing so helps incredibly in making a page look convincing. Same with the phishing email; get a hold of a real email from the company and work based off of that.



From: eBay Billing Department
Date: Sunday, November 28, 2004 7:32 AM
To:
Subject: Credit/Debit card update

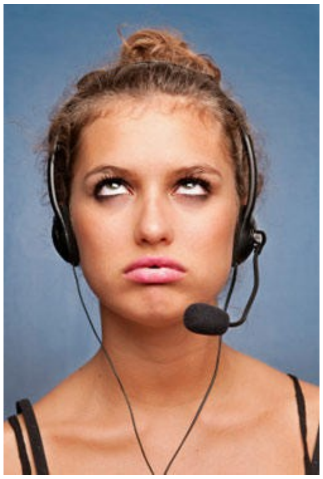
Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e.change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

The phishing emails can ask to log in to verify activity; add a PIN to the account for added security, or check and confirm an updated terms of service. Give them the threat that their account will be disabled if they don't do so; since they're the only ones your sending the phishing email to you're much more likely to pass through the spam filters.



The feeling of working in a call center.

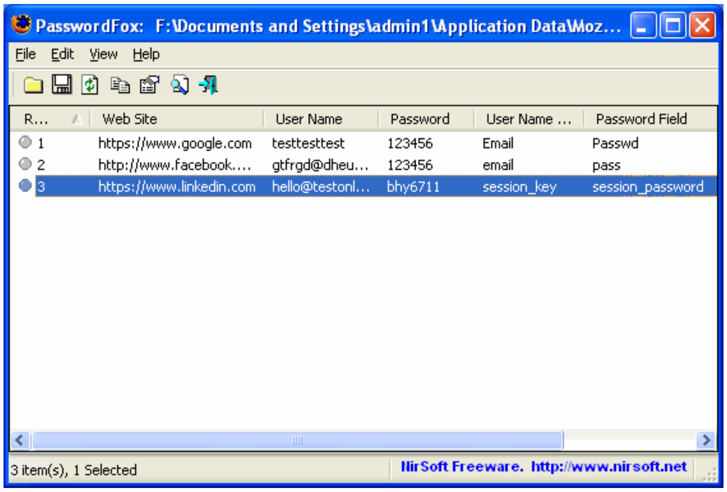
If there's no bite on the phishing email, next step is a cold call. This is part of where a burner phone comes in handy; call the target at home and give them your spiel. Rehearse the opening line before calling so that you can pass it in a single breath, sounding bored with the entire process. "Hello, this is Fake Name with X Company's security division; this is not a sales call. I'm calling regarding your account; our system has detected some unusual activity and has automatically deactivated your account. I just need some information to confirm your account in order to re-activate it and get you back online. First let me confirm that I'm speaking to Target Name, and that you're still at 123 Target Address St., SomeTown, SomeState. Alright; I've got your user name as Username, do you remember what your password is?"

The more information that you give them, and the more routine you can sound, the more likely that they are to believe you are who you claim to be. But, having worked in tech support previously, I can tell you that one of the most frustrating things will be that they often *won't* remember what their password is. Hopefully you'll be able to bypass this being in front of a computer while on the phone with them; this will allow you to try any options that they give you. If you aren't able to get them to remember their password, when be sure to continue with the ruse; just ask them some other piece of information to "confirm their identity" and end the call. If the target gets suspicious then they start to put their guard up and your job becomes much more difficult.

A while back there was a job being done on commission, hacking an account for a third party. No progress was being made via the usual tactics, so in order to get paid a more high risk / high reward strategy was called for. So, a new phone number was obtained, and another cold call to the target.

"Hello, is this Mr. Target? Ah, very good, I'm SomeName with Microsoft's Advanced Security Team. The results of the most recent Windows Malicious Software Removal Tool from Windows Updates indicated that your computer is infected with a new type of computer virus. It doesn't appear to be immediately threatening, but it looks to be using a previously un-detected security venerability. We do have a team in your area, and were hoping that you would be available to have one of our technicians come out and remove the infection, free of charge? We're attempting to gain information about this infection so that we can build a patch before it becomes a serious issue. As a thank you for your cooperation, you will receive a voucher for a free copy of any software that Microsoft produces, including Office, as well as one piece of hardware produced by Microsoft, such as the Microsoft Wireless Comfort Desktop Keyboard and Mouse."

The combination of the carrot of the reward and free service, and the stick of their computer remaining infected got a foot in the door. From there some basic computer cleanup was performed, and a couple of programs from NirSoft run to access stored passwords and the job was done.


PasswordFox: F:\Documents and Settings\admin1\Application Data\Moz...
File
Edit
View
Help

R...	Web Site	User Name	Password	User Name ...	Password Field
1	https://www.google.com	testtesttest	123456	Email	Passwd
2	http://www.facebook....	gtfrgd@dheu...	123456	email	pass
3	https://www.linkedin.com	hello@testonl...	bhy6711	session_key	session_password

3 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net

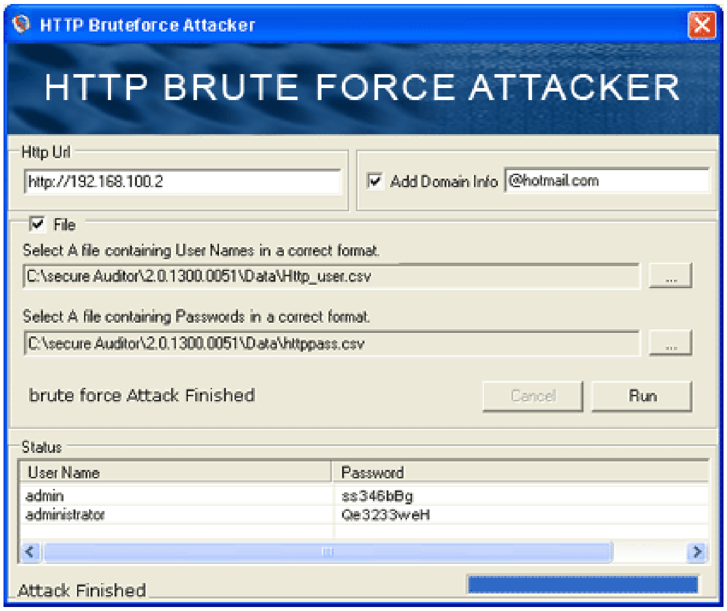
Of course, it’s always the details that sell something like that. “Microsoft’s Advanced Security Team” had a website, a nametag was printed, and vouchers for the free hardware and software were printed up to have more then one in the briefcase, and when he was given the voucher he was told that “It sometimes takes 48-36 hours for the voucher to be activated, if you’re still not able to use the code on the voucher to log in to the Advanced Security Team’s website, then call this phone number and they’ll manually activate it.” I never did find out what he though when trying to navigate the Microsoft Phone tree to get to the non-existent Security Team, but by then it was all a done deal.

The main thing is to be imaginative, but professional at all times. The biggest challenge with social engineering is to be different enough that your tactic hasn’t been tried a million times before, yet being innocent enough as not to raise the target’s suspicion.

The ultimate goal is to get your target to trust you, and then to betray that trust. And since trust isn’t easily given, it’s usually far quicker to impersonate someone that your target already trusts. So if you’re representing a business, then act as any other employee of that business would. Use their same terminology, dress to the company’s dress code, and behave in a way that generally speaks well of the company.

Strong Brute Forcing

Sometimes the target is just too on the ball for anything else to work. In these cases the only thing left is to just brute force the password.



Http Url: http://192.168.100.2

☑ Add Domain Info: @hotmail.com

☑ File

Select A file containing User Names in a correct format.
C:\secure Auditor\2.0.1300.0051\Data\Http_user.csv

Select A file containing Passwords in a correct format.
C:\secure Auditor\2.0.1300.0051\Data\httppass.csv

brute force Attack Finished

Status

User Name	Password
admin	ss346bBg
administrator	Qe3233weH

Attack Finished

Brute forcing is the process of just trying every possible password combination. And with just uppercase, lower case and numbers that's 62 characters for a normal English (more if you add the special characters such as *, &, $, and such). Not too bad; but that's for a one character password. Once you get to two characters you're dealing with 62 squared or 3,844 possibilities. Three characters you have to raise 62 to the third power, or 238,328 different passwords. Every time you add another character you raise it to the next power, so once you get to a four letter password you've got just under 15 Million possibilities and five letters is a little under a billion possibilities.

And that's the reason that this is the least favored possibility; there are simply too many options. One way to mitigate this is to use dictionary or hybrid attacks. The dictionary attack works under the principal that even though "R7sE^5" could be a password, it's far more likely to be "Bobby" or the ever infamous "letmein". Random passwords are more secure, but they're far harder to remember; so by having a list of commonly used passwords you're able to get a large portion of the total accounts out there.

A hybrid attack is, as it sounds, a mix of the two methods. It starts out with a dictionary, processes that and if there's no match, it then goes on to brute force the password. This offers the best of both methods in that it takes relatively little time to go through the dictionary, and if a password isn't found in there it'll use the more through method.

As for the specifics for brute forcing; there are so many different systems and different tools to hack them that all I can do is give very general advice. A quick google search is often all that you'll need to get the specific "how to" for whatever service you're trying to hack. For most web based log in services you should be able to find some sort of script or utility designed specifically to target it. PHP scripts are common, but you can find some utilities that are run from your own system. Hydra-gtk is one of the more prevalent ones, and is included in the [BackTrack Linux](#) dustro.

Brute forcing is a last ditch attempt, so what do you do if it doesn't work? From this point you've really got two choices, first is to start back at the beginning and go through the process again. The second is to re-assess if it's worth the effort; there will come a time when you need to cut your losses and go on to the next challenge.

Once You Gain Access

Achieving Your Objective:

Your in, so now what? This is where having concrete goals to start out with comes in handy. There is nothing more of a let down then getting through the layers of security, only to have no idea on where to go next.

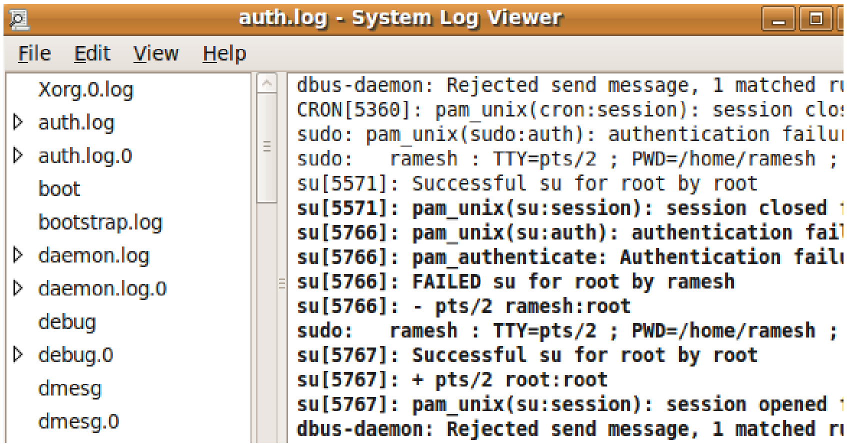
Sometimes this is obvious; if you're after a specific piece of information from their email then you download their account's contents and find it. If you're looking to compromise them socially or legally you can post heartfelt confessions of their facebook; start hitting on their wife's sister from their account, spam their entire address book with things to make them a social pariah.

Other times it's more subtle, like planting little things in their sent items that will implicate them in something down the road, or finding out if she really is cheating on you with that guy from work. But whatever it is do it, get it over with and then get out. The more time you're working on an account that's not your own, the more likely it is that you'll slip up and get caught.

Cleanup:

And that brings us to the final step, cleaning up. This needs to be immediate and total. Any email accounts that have been used have to be closed and forgotten; any websites that have been put up for phishing or social engineering have to be taken down, replaced with something innocent and forgotten about. If you used a burner phone then it needs to be discarded, same for if you used “spare” license plates.

Research before hand what logs may be kept by any systems that you’ve accessed and how to clear them. In most cases these logs will be kept in such a way as to prevent you from getting rid of them, but there are many things to clean that you will have control over. If you’ve sent an email from your target’s account, then be sure to remove it from the sent items. Messages that have been sent need to be removed; any changes you’ve made to the account should be un-done.



```
dbus-daemon: Rejected send message, 1 matched ru
CRON[5360]: pam_unix(cron:session): session clo
sudo: pam_unix(sudo:auth): authentication failu
sudo:   ramesh : TTY=pts/2 ; PWD=/home/ramesh ;
su[5571]: Successful su for root by root
su[5571]: pam_unix(su:session): session closed
su[5766]: pam_unix(su:auth): authentication fai
su[5766]: pam_authenticate: Authentication fail
su[5766]: FAILED su for root by ramesh
su[5766]: - pts/2 ramesh:root
sudo:   ramesh : TTY=pts/2 ; PWD=/home/ramesh ;
su[5767]: Successful su for root by root
su[5767]: + pts/2 root:root
su[5767]: pam_unix(su:session): session opened
dbus-daemon: Rejected send message, 1 matched ru
```

The best case scenario is that they never know that they’ve been hacked; or are never quite sure. If it’s un-avoidable, then ambiguity is your friend. Don’t let them know to what extent they’ve been compromised, or leave plausible alternative as to how they were compromised.

You will be tempted to brag, or to revisit afterwards a see the results; but these temptations must be avoided at all costs. Best bet is to just forget that it happened, get rid of any evidence and appreciate your handywork from afar.

Resources

- PHProxy: http://sourceforge.net/projects/poxy/
- PHP Web Prozy: http://sourceforge.net/projects/php-proxy/
- Glype: http://www.glype.com/
- VPN and Proxy Providers: http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/
- Private Internet Access: https://www.privateinternetaccess.com/
- Tor: https://www.torproject.org/download/download
- Cantenna information: http://www.turnpoint.net/wireless/cantennahowto.html
- Servers Ultimate: https://play.google.com/store/apps/details?id=com.icecoldapps.serversultimate
- Port Forwarding Information: http://portforward.com/routers.htm
- Dynamic DNS: http://dyn.com/
- Default Router Passwords: http://www.routerpasswords.com/
- Burner Cell Phone: http://www.walmart.com/ip/TracFone-Samsung-S125G-Prepaid-Cell-Phone-Bundle/20933059
- Reverse Email Directory: http://www.spokeo.com/email-search
- Public Records Search: http://www.beenverified.com
- Nmap: http://nmap.org/
- Firesheep: http://codebutler.com/firesheep/?c=1
- FaceNiff: http://faceniff.ponury.net/
- Free Year of Hosting and Domain Registration: http://www.gybo.com
- NirSoft, password recovery software: http://www.nirsoft.net/
- BackTrack Linux: http://www.backtrack-linux.org/