

For hackforums.com, I copy and pasted this shit for you guys.

Format Layout

Spoiler (Click to Hide)

=

[Target:]

Listing/Reason: Say stuff about how immature he is here.

Real Name:

=

Age:

=

SSN:

=

Known Ip address:

=

Facebook:

=

Picture:

=

Work:

=====

[Contact information]

Aim:

Skype:

Skype:

Xbox GT:

Twitter:

Email:

Youtube:

Website:

SB:

=====

Family:

Address:

House Picture:

Home phone:

leaked by camel leaked by camelContact information

Cell Phone Number:

Parents work Phone:

Proof of him Being a skid

=====

jacked accounts

Aim

Skype

yahoo

Gmail

Other relevant information

Keep in mind, when you are doxing. Make sure to actively save and copy all your legitiment

information about the individual into the notepad or Basket.

PART 1

Spoiler (Click to Hide)

===Part One===

Preliminary information gathering

Once a situation has started, and you have decided to commence doxing someone, then it is

appropriate to find all information about the suspect.

I'm assuming most of you will have an encounter with the specific individual over Skype or a

gaming server, or even another instant messaging program.

The first thing I recommend doing is copying all known information about the current user into a

seperate notepad from your doxing format, this includes resolving his skype, taking down his

skype name, age, and area and number if listed on his profile.

I also suggest adding the user on skype as this will be used to your advantage later in the tutorial,

if he accepts then your in for some fun. If he dosen't then make a backup skype and add him on

that [Fake hot girls work great]

Also, copy down any information from their online accounts that you met them on, they associated on or friends of theirs that you came into contact with. You can easily extort these

individuals for your own gain.

A key part of doxing is information gathering, you are not going to magically be handed a dox

through a program such as Roxer Doxer or a similar email doxer, you have to work for it, and for

work to happen, you have to start from somewhere.

That somewhere is the area or place you first met the user in, it could be Minecraft, Skype or a

forum. Make sure to look into the users profile, threads and posts. If he has a sales thread make sure to research it, copy down any associated information regarding the user. this could include skypes, PP addresses or anything else. This will come in hand later during part 5 When paypal payments and my wingman method come into play. <https://pipl.com/> Can be usefull with an email, as can spokeo. <http://tineye.com/> Reverse image searching, this can be used to trace back custom avatars to photobucket and deviant art accounts ;) <http://www.zabasearch.com/> Another lovely search area when you have more information. Also lullar.com is amazing if you can pull their email.

PART 2

Spoiler (Click to Hide)
===Part Two===

Pulling information off an IP address.
There are many methods of pulling information off an Ip, most common and that I will share with you today is geolocation and isp information. This also includes a varient of ISP doxing. Once you have pulled the persons IP Address through a skype resolver, or a trick website. You may then proceed to order a whois on the IP. This can be done through <http://whois.domaintools.com/> <http://www.ipaddress.org/tracer/ipwhois.php> <http://whois.net/ipaddresslookup/> Pulling information off a skype name. Obviously you arn't going to find all his real information just from skype. This is why it's recommended to use some handy searching tools such as google. Google in my opinion is the ultimate tool in doxing. For instance, say you met a guy named darklord12321 on skype, he has his profile closed, but you know his skype name. You could commence to open up chrome and search for Skype:Darklord12321 in the search box, this would yeild results where he left his skype, for gaming or financial reasons. Maybe even to talk, this could yeild an online profile, an old alias, a community he owns or maybe even a facebook if you are lucky.

This also works for steam such as Steam: Dearthmaster1421 or IGN:lfatality [IGN stands for in game name] A lot of kids, expecially in Gmod and minecraft list there name in that format for an unban appeal, or even a staff application. This can be crucial to finding more information about the user rather than the regular information
Finding a skype name from an IP:
I don't own this, give all credits to the project owner. This tool is cool as shit.
Basically, you put their IP into this <http://agonystresser.com/reverseskype.php>
And it gets you a skype name that has been resolved with that IP. It's pretty cool in my opinion
This is owner by Xanii off HF.

PART 3

Spoiler (Click to Hide)

===Part Three===

Interlinking email addresses

Many users think because they associate accounts with there emails that they can't be traced through their meida system. There fucking retarded, this isn't the case.
Over the age of the internet, starting in 07, users started assosicating their emails with various services, they think tha just because they sign up for skype on one account, that it can't be linked to their facebook or vice versa.
But, as time goes on. Everyone is proven to be wrong.

PART 4

Spoiler (Click to Hide)

===Part Four===

Facebook&Skype

Now, Social meida is a goldmine is the world of doxing, it offers you an incredible amount of information about the individual, such as their hometown, friends, school, girlfriend, and assoscated family members.
A now semiknown method that I released on HF of linking skypes to FB is <https://www.facebook.com/?sk=ff>
You basically create a fake profile on facebook, then log into your skype and click find friends
what it will now do is say \" Hey facebook, this is skype here, mind taking all of my contacts,
leeching their emails and searching for them, then putting them in a scroll down area\"
Then, you

will be presented with

A simple box that you can scroll in, simply CTRL+F for a search box, put your targets name in

and see if he has a FB connected to his skype. If he does, it's a goldmine.

You can then go to his profile by searching for him after you saw he had a profile, look through

his friends and put his last name in there, then search for his parents ;).

I'm also going to include domains in this, most people have a whois gaurd but a lot don't.

You

have to be carefull of faulty information on their whois as well. Not everything you read on the

internet is real 🤪.

To look up information on a domain simply go to <http://www.whoissearch.com/> and enter their

domain. Armed with legitiment information from a domain whois you practially have their doxin.

Also, there is an array of ways you can grab IP's through Skype and other services. Such as

commview+Cain&Abel.

For those of you who are lazy, here are some sources.

<http://skypesyke.info/>

<http://skypegrab.info/>

<http://www.skyperesolver.com/>

<http://vdoss.info/empire.php>

These are credited to their original groups and Owners who host them. Not me, them.

PART 5

Spoiler (Click to Hide)

===Part Five===

Reverseing phone numbers

This is a favorite of mine, if someone has a number listed on there skype that is legitiment I go

directly toward this.

Basicaly, like a regular whois on a domain you can whois a phone number.

There are multiple sites for this, but I like to either use argali client or

<http://freerevcell.com/index.php>

Argali searches in buisness directories also, but <http://freerevcell.com/index.php> just gives you

the whois, you simple enter there number without any 's or spaces, then you click Caller ID op't

2, Opt 1 or Cellphone info.

This gives you the first and last name of the individual who registered the phone, basically if the

tango isa minor, it's his parent or the adult who he lives with ;)

Then, from that name and number you just google the area code of the cell or home phone [First

three digits] then you use anywho.com or argali and search for the name in that area. If they do use a legit phone # on there skype or contact area such as a domain whois, you can ge their addy from this method in around two mins.

PART 6

Spoiler (Click to Hide)

===Part Six===

Finding links in family and reletives

A good way for juicy info is to look for reletives of the select individual, this can be fun since you can dig up obituaries, marriges, and other information. Use google dorks with his name and family things and activities, his hometown, and words relating to family occasion, such as death, marrige, party, church. You will end up with some good information most of the time.

PART 7

Spoiler (Click to Hide)

===Part Seven===

Completion and credit reports

Once you have found the user, you can order a free online credit report of the individual or his parents, you can also look through his property taxes. To do this search for free credit report sites, like Freecreditreport.com Order the report and check it out, you can use this info to your advantage later in the tutorial for malicous usage.

PART 8

Spoiler (Click to Hide)

===Part Eight===

Pulling an addy

When you have a rough understanding of the individual it is advisted to do some good searching,
Note: If the Tango is underage, he will not have a listing in the sources provided. Instead, his family members will [Usually the mother or father]
You may have to do some calls ins asking for \"John doe\" Just say it's Marko and you want to know if he can hang out on thursday, don't ask an open ended questions as this may arise

suspicion. You want to ask Yes/No questions as it doesn't leave room for bullshit.
I also recommend viewing some tutorials on vocal tone analyzation. As this can be
usefull in
most situations of finding out if the targets parents or the individual on the other side of
the
Phone/VOIP is lying.
<http://www.argali.com/download.asp>
United States: <http://whitepages.com/>
UnitedKingdom: <http://whitepages.co.uk/>
Canada: <http://whitepages.ca/>
Australia: <http://whitepages.com.au/>
Also, if a user doesn't have a whitepages, but he shows up in the premium database
search with
anywho.com or argali, then the dox is somewhat confirmed, because the goon probably
decided
to call himself undoxable after he deleted his Whitepages information.

PART 9

Spoiler (Click to Hide)

===Part Nine===

Pulling SSN's

SSN stands for Social Security Number, anyone that's not an illegal immigrant or here on
a work
visa is issued one at birth, with a SSN your options to fuck the individual are
tremendously
improved as you can then continue your dirty destruction of him into the afterlife with juicy
methods.
To list some, Credit bumping, Account hijacking, and signign them up for bogus services
that
redistribute there information to the world.
This is a fun one, when you read your targets social to him he usually cries, or freaks
out.For this
method to work, the user has to be over the age of 18, if not, then his Dad's SSN works
as well.
But, think about it, your here to fuck the individual and not the family, dont try to pull and
bullshit
on people who don't deserve it.
To pull their SSN you need to go to <https://backstab.biz/>
Fill your account with BTC, and start pulling SSN's. it's a fairly large database used for
Private
investigators. It can also be used for us :]

PART 10

Spoiler (Click to Hide)

===Part Ten===

Paypal&ISP doxing

Paypal is probably my favorite payment system to dox from. Being that you can use it to your advantage.

Pinging as I like to call it is the act of using a compromised or otherwise legitimate paypal account to send the victim one cent, or even a dollar to lower suspicion.

Once you have sent him that money, you will receive a message like "You have sent .01USD to

Namehere\" This can be very useful, say you got some kid's name from a paypal, all you have to

do is geolocate, then search through <https://Anywho.com> and get his address through their.

Also, you can SE him into sending you 5\$ for a fake product or game key, minecraft account/etc. And

you will be provided with his shipping address!

But beware, this information is not always correct. Don't get ahead of yourself and post a fake

DoX, then you just look fucking retarded and everyone thinks you're a random.

Now, ISPs have preventative measures and methods get patched quickly, this is why it is

recommended to fabricate your own method on the subject.. Obviously this EBook is going to

be leached so I won't share my specific method, I can't do all the work for you.

It all revolves around Social engineering. Basically you are going to want to convince the target

[operator] to give you certain credentials about the customer's IP.

Before even starting it is encouraged to find the right operator, most middle aged males are

cocky and suspicious. This is why you should target older males+females, people who are

inconsiderate about their job and other degenerates who work there.

Method one. You're going to want to post as a legitimate customer, attempt to suck information out

of them using closed end questions, ask why your internet is down, try to stay away from them

asking who you are, but more about the problem.

The human mind is very exploitable, especially when emotions come into play, act urgent, ask

why your internet is down and not up. Try to make the employee feel sympathetic for you. One

thing to always do in this phase is to be polite, the nicer a person is the more chance of success

he has in getting confidential information.

And, if you get shut down then it's not a serious problem. I have had countless times that I was

shut down from operators, knowing I was snooping for information. But, also I had numerous

times where I was considerate, made my needs know, was polit and addressed the operator by their position and name.
To learn more about ISP doxing I would recommend reading up on social engineering, MLP and it's concurrent uses with doxing.

Resources

Spoiler (Click to Hide)

Here are a couple text to ACSI links you can toy around with.

patorjk.com/software/taag/

<http://www.networkscience.de/ascii/>

Formatted resources

==Skype resolvers==

<http://skypesyke.info/>

<http://skypegrab.info/>

<http://www.skyperesolver.com>

==Address search==

[Http://Anywho.com](http://Anywho.com)

<http://Canada411.com> [Canadian version of White pages]

<http://Dexonline.com> [Business]

<http://Infospace.com> [Amazing search engine for profiling a target]

<http://Masterfiles.com>

<http://Rootsweb.com> [Free ancestry]

Phone and Voip

PhoneValidator.com

Infospace.com

Automated information gathering

<http://www.argali.com/download.asp>

Non US Research

192.com [British Database]

Canada411.com

BTCbahamas.com [Bahamas Phone and directory Database]

Canada.gc.ca [Canadian resource and website]

English property records office [11441812881418]

VOIP skype fowarding

<http://www.didlogic.com>

Credit Report Tools

Experian.com

freecreditreport.com

Or search for more!

Looking for files

[Site:Sitename.com:filetype:pdf](#)

Different Filetypes Doc, TxT, Xls, Pdf

Other:

http://www.whitepages.com/find_neighbors

<http://labs.jaduka.com/dukaDial>
<http://labs.jaduka.com/earthcaller>
<http://www.trojancondoms.com/Product/FreeSample.aspx>
<http://www.astroglide.com/SampleRequest.asp>

==Cloud server source==

I recommend using hacked RDP's for this type of work. Also make sure to trash the RDP after the

dirty deed. Make sure you install loads of malware and DDoS with it after to get it suspended and

wiped ;) This will make it much harder to see who did dirty things on it.

<http://www.rackspace.com>

==Extra isp information==

// Turning the IP address into a real name and physical address to be used for swatting

Next step is calling the their ISP as internet technical support for the company and pulling the

customer info via the IP, telling an agent you're an internet technical representative most effectively done by using LinkedIn to acquire a real technicians name (Ideally from Network

Operations/OST3), and telling them your systems are down at your call center. Then give them

whatever information you have, and get them to pull it up in one of their tools. Once you've

acquired the information you can use the last 4 digits of the SSN associated with the account

to reset the password to the person's email by calling in and providing the information you

acquired from the first call. From this point swatting is then done via Spoofed calls with a spoofing service such

as <http://www.spoofel.com>, <http://www.spoofcard.com>, <http://www.spoofthiscall.com>

Here are the Various ISP's and the internal tools they utilize, reference these when calling in to

Social Engineer

Customer info from an IP address.

=====

AT&T Info:

Tools:

SystemX Shows IP, what account it is, lookup by address, runs credit checks, see driver license.

Clarify Looks up account and logs into the account. Can do full social, ip, phone number, and

name.

Telegence Shows account information including last four of the ssn.

MyCSP Opens up Torch, SystemX, etc.

Phoenix Change phone numbers, rate plans, etc.

Torch Text messenger.

CSR Admin Logs into MyATT account.

CTI Transfer calls.

Agent Verification System Verifies employee ID.

CCC Tool Removes subscriptions.

DLC See how long the phone has been in service.

CCare Checks for upgrades.

Employee ID:

First 2 Initials, first 3 of the Social, letter at the end.

Example:

Name: Larry Stevenson

SSN: 306897661

UID: LS306Z

Employee Logins:

Computer:

Username = UID.

Password is set by the agent. Changes every month.

Tool Portals:

Username = UID.

Password is either randomized or set by the agent. Changes every three weeks.

Computer Info:

OS is Windows 7 with an Windows classic theme.

Virus protection is McAfee.

Some connect wired and some are wireless.

WiFi names are \"AT&T\" followed by a number.

Online Access:

<https://access1.sbc.com/>

<https://mycsp.cingular.com/mycspportal/a...abel=login>

https://attathome.att.com/athome_web/index.jsp

<https://sso.sl.attcompute.com>

<https://attawardslink.com>

<https://att.corporateperks.com/login>

=====

Verizon:

Tools:

CoFee Main tool agents use. Looks up accounts by phone number, name, etc.

CPE Manager Looks up accounts by the IP address.

Legend Another tool agents use to pull info off an account.

CoFee Login:

<https://www22.verizon.com/cofee/cpm/login/login.aspx>

=====

Comcast:

New Method: Have billing DEPT transfer you to the helpdesk.

Tools:

Grandslam Looks up by IP, SSN, phone, and more.

ASCR Looks up account.

Einstein Looks up account.

CPNI

Every Comcast tool is within Grandslam as Grandslam is Comcast's \"master tool\".

=====

Time Warner / Roadrunner / Brighthouse:

Call 1800TWCABLE. Enter in a phone number and zip in the area of the IP address.

Once an

agent picks up tell them a fake name, you work for TWC internet tech support, and you were

having trouble looking up a customers account with AAD. Then ask them if they can transfer you

to tier 3. They will transfer you then. Once you get transferred to tier 3 say your name and your

work for TWC internet tech support. Tell them you were having trouble pulling up an account by

IP address. Say that Unified was giving you an error not found. Tell them you don't have DOCSIS and ask them if they can look up the account in that. They should do it, so give them

the IP. Once they pull up the account ask for these things in the order listed:

Name

Phone

Address

MAC Address

User ID

Email

Account Number

After this point if you ask for anything else they may get suspicious. They may give it to you, or

you might have to call back. Try asking for this information on the account.

Security measure: Last 4 of the ssn and/or the 4 digit pin code

customer code

full driver license

After you get that call back TWC and ask to reset your password. Say you forgot the SQA.

They will ask for the security measure and customer code then they'll reset it.

You'll want access into the primary email and the MyServices feature.

Make sure you get both reset, but sometimes you'll have to create the MyServices account.

Also if you want the SSID and network password go to the WiFi live chat once logged into the

target's account. The agents will ask for some information in order to verify you then they'll ask

for the modem MAC address. Give them the MAC address the employee read out to you earlier

when you asked them for the MAC address on file. They should then provide you with the SSID

name and password.

Resources:

Username Retrieval: <https://urt.rr.com/>

Password Reset: <http://pt.rr.com/>

Tools:

AAD Used to pull up the account once they have the information on the customer.

Unified Pulls up by MAC, IP, etc.

ATG Tools / DOCSIS Basically TWC's "master tool". Can do just about anything.

If you're ever asked for an employee ID just use this. It's legitimate.

Employee Info:

Name: Darryl Estes

EID: E12145

Location: TWRaleigh in Raleigh, NC

Regions:

Austin RDC

TWAustin

TWBeaumont

TWColumbusTX

TWCorpusChristi

TWDelRio

TWDilley

TWEaglePass

TWEIPaso

TWGonzalez

TWKansasCity

TWKerrville

TWLaredo

TWLincoln

TWNorthTexas

TWRioGrandeValley

TWSanAntonio

TWTexas Regional

TWUvalde

TWWaco

TWWitchitaFalls

Bright House Network RDC

TWBakersfield (Bright House)

TWBirmingham

TWCantonment

TWCentralFL

TWDefuniak

TWDetroit (Bright House)

TWEImore

TWEufaula

TWGreenville

TWIndianapolis (Bright House)

TWTampaBay

Charlotte NDC RDC

NDCCCharlotte

Columbus RDC

INColumbus

TWKYN

TWLouisville
TWMOH
TWMilwaukee
TWNEO
TWNEW
TWRegional Midwest
TWSWOH
TWWesternOhio
Coudersport RDC
TWCoudersport
Herndon RDC
TWHerndon
NYC RDC
TWBergen
TWLiberty
TWNyCity
TWStatenIsland
Orange RDC
TWDesertCities
TWHawaii
TWLosAngeles
TWMountain
TWMountainWest
TWNorthwest
TWSanDiego
TWSouthwest
Peakview RDC
NDCPeakview
TWAlegeny
TWBroomfield
TWCentralKYOH
TWClarksburg
TWDothan
TWMOOKKS
TWPeakview Regional
TWSoutheast
TWTerreHaute
TWVoIP
TWWesternKY
Raleigh RDC
TWCharlotte
TWColumbia
TWFayetteville
TWGreensboro
TWRaleigh
TWRegionalCarolinas
TWWilmington

Syracuse RDC
TWAAlbany
TWAthol
TWBerlin
TWBinghamton
TWBuffalo
TWCentralNY
TWKeene
TWLancaster (National division)
TWPortland
TWRochester
TWSyracuse Regional
TSG RDC
TWTSG

This isn't really a part of the social engineering lesson, but here are some TWC employee tools accessed online.

<https://tools.rdcnyc.rr.com/>
<https://uptime.rdckc.rr.com/>
<https://tools.nyroc.rr.com/>
<https://tools.tampflrdc.rr.com/docsis/>
<https://tools.ohiordc.rr.com/>
<https://docsistools.tampabay.rr.com/>
<https://tools.ohiordc.rr.com/onodera/>
<https://tech.indy.rr.com/>
<https://tech.insight.rr.com/>

You can find more by using the following Google dork:
<https://www.google.com/#q=inurl:tools+si...ite:features.rr.com+site:gallery.rr.com>

=====

Cox:

Tools:

Edgehealth/Proviso Looks up by IP and MAC.

ICOMS Looks up account.

SL2 Looks up account.

Home Cert Polls CPE

=====

Optimum Online:

Tools:

TDA Billing tool.

=====

TMobile:

Tools:

Quickview <https://quickview.tmobile.com/mosaic> Looks up account.

Watson <http://watson.tmobile.com/> (Account Lookup)

icam <https://icam.tmobile.com/> (Customer Account Management)

=====

CenturyLink:

Tools:

Ensemble Looks up account.

JWalk/Seagull Looks up account.

INET Logs into account.

=====

VirginMedia:

Tools:

Rizzor/TACACS/Badger/CDFE|IP