

Forum:[Hack Forums](#)

Thread: [Creating dictionaries based on information from OSINT - Tutorial part 2](#)

2xTheTap115 - April 18, 2020, 4:43 am

Returning to the starting point. What if the network turns out to be a private network? At first it may seem that reconnaissance in this case is pointless but this is a very wrong assumption. In fact, in this situation, we can consider two probable cases: either the owner changed the default password or did not. In the latter case, the matter is much easier because it is enough to check the router model (look at the ssid network. I am sure that if a person has not changed the ssid network, then the default password has not been changed. Now just "Google" this equipment to learn the rules creating passwords by the producer (I wrote about it in another tutorial). But let's consider an example where the ssid and password were changed. How can we narrow down the space for potential passwords ?. First of all, I would try to determine who exactly this network belongs to (this is a specific person). The easiest way will be to visit the place (its location is determined using Wigle) then we can based on information from mailboxes (or intercoms if we have to deal with a block of flats, in which case we will also need a phone application capable of analyzing the strength of the wifi signal (e.g. Wifi Analyzer) and based on the signal strength, we are able to determine the apartment from which the network comes from. Now just look at the name plate on the front door to find out the personal details of the owner). If, however, it turned out that it is impossible to determine the data in this way, we can use the so-called "subscriber lists" available on the internet (this is a digital telephone directory). Just enter the desired address there and thanks to that we will get to know the data of the person living at the given address (provided that such a person has agreed to enter it in such a book early and I am honest to say that in my country it is rare that people do not agree to it). For the purposes of our example, however, let us recognize that we have learned the name of the owner. The next step to take would be to check the social media of such a person (facebook, twitter and thousands of other portals) to determine their interests, workplace, hobbies, pages and things he likes, posts he publishes, etc. Any such information is invaluable. Why? Because each of them can be a potential password. People are very lazy beings by nature and strive for "simplifications" in every possible situation and thus become very predictable. There is only a percentage of people who follow the basic safety rules, e.g. when creating secure passwords, all the rest is based on simplifications, patterns that are easy to remember (e.g., cat's name + current year or your favorite football team + your child's date of birth). In many, many cases such people unknowingly publish "hints" to their passwords in posts on social networks (let's assume that someone posts a lot about their favorite football team, try to match the team name or name of the top player of this team with the current year. I guarantee you that at 65% it will be the password to his email inbox, wifi or other service. Variations of this pattern may be different, experiment, you'll see it works: D) Based on the information we have, we are able to generate a dictionary modified with specific patterns (such as current year, members' birth dates) families, names of favorite things, etc.) There are really many such examples and all in this field you are limited only by your own imagination and set of information. Of course, I would be ignorant if I said that it is a reliable method, it can always happen that it will not be possible to obtain a password in this way because, for example: the password will be randomly generated and will not be associated with any information shared by the owner of the network. However, I think that this technique is very effective and not only when cracking passwords (repeatedly finding a credit card I was able to set a pin to it within 15 minutes (you do not even realize how many people set the date of birth as a pin) and I have often called shock and disbelief on the owner's face. All in all it is an effective way to pick up XD). It is also worth mentioning here another important thing which is checking for password leaks from various websites. There are many different services such as [haveibeenpwned.com](#) where you just need to tap the email address and we can easily find out if the password for the email has leaked. With such

a password, we are able to generate thousands of other passwords based on it, which may prove effective in our attack.

And that would be enough when it comes to generating dictionaries. I am aware that what he describes is an iceberg tower and one could write a lot about it, but the assumption was about the basics. Below are links to pages that can be useful when creating dictionaries:

WEBSITES WITH DATABASE LEAKS:

- haveibeenpwned.com
- Vigilante.pw
- <https://down.tencent.pp.ua> - this server contains several hundred GB of various database leaks, personal data, credit card numbers from various services such as Amazon, Xaomi, Gmail as well as many Asian services. However, I warn you against downloading any software, scripts or similar stuff from there. This site does not belong to me and I am not responsible for the software there (I downloaded several GB of various leaks from it myself and they are cool but as I said before, do not download anything else from there !!! You have been warned: D)

Stella - April 18, 2020, 12:26 pm

Hey could you please add me for some more info? I really need your help!

telegram: @glizyglloo

discord: 14iraq#0014

skype: live:companyjohnsons