

Forum:[Hack Forums](#)

Thread: [Creating dictionaries based on information from OSINT - Tutorial part 1](#)

2xTheTap115 - April 18, 2020, 4:42 am

Hello, D

I decided to write a small guide on creating effective and personalized dictionaries for cracking passwords based on data from "white intelligence" and knowledge about human nature (called social engineering;)) I think that creating dictionaries is crucial for the effectiveness of password cracking attacks and many people approach this topic with incorrect assumptions, which directly translates into their effectiveness in action. Based on the examples, I will try to show the basic assumptions in creating such lists that, in my opinion, increase our chances and save a lot of time during work. Although this guide will be very theoretical, I will try to put here links to sources / pages that in my opinion may be useful. As usual, if I made a mistake, let me know;) and now we are flying with it.

As I mentioned earlier, generating effective (not effective :)) dictionaries is crucial for success in the process of breaking passwords. But just having a huge dictionary containing all possible combinations of characters does not provide us with efficiency when breaking a password (an attempt to crack a well-chosen and complex password is quite strongly limited by the capabilities of our equipment and if we do not have a super-computer on our services, such a password cracking can really take a lot of time and sometimes it will be unreachable even if the huge dictionary will contain the password we are looking for). It is known that in the internet age we can use specially dedicated online services for cracking passwords (which I use with the rest), but they sometimes fail even though in many cases their effectiveness is quite good. However, I have convinced myself that a well-constructed dictionary will be ten times better than many powerful online services. I will compare it to a shot from a sniper rifle and a shot from a children's slingshot, we know what is more laughable: P

To better illustrate this, I will use the first better from the edge example. You want to hack into a wifi router, at the very beginning you only know the ssid network. You are intercepting a handshake and trying to crack a password. You start aircrack (or hashcat, it all depends on which program you prefer) in combination with several different dictionaries (let's say you used the dictionary with default passwords in succession, then you started the numeric dictionary (from 8-15 digits) and at the end you used a password built of leaked to the internet) but unfortunately you didn't break it. What will you do next? do you launch a dictionary with all possible password combinations? How long will it take you to crack a password with this technique?

And this is where white intelligence techniques come to the rescue. Thanks to the reconnaissance we are able to get some information about our goal and try to narrow down the area of our search in terms of a potential password. Returning to our example, instead of senselessly and laboriously breaking the password by the method of brute force, it would be better, for example, to check the geolocation of our network using Wigle (internet map of wifi network) and find out whether the network we are dealing with belongs to a company or rather a private person (if the network is located in a large block of flats, we can certainly assume that it is a private network, and companies are trying to "mark" their headquarters in services such as google to help potential customers reach them, so quick patting the coordinates to google maps will dispel your doubts: D). If it turned out that I have to deal with the company, the first place I would go is the company's website, which many times turns out to be a treasury of knowledge about its employees. Secondly, I would visit the social

media of the goal itself, but also of their employees (and here I point out that for me the most "valuable" employees are, of course, those from the IT department. For known purposes, errors made on their part are critical and many times it happens that it is on their part, the easiest way to get information is It is quite often that small businesses simply cannot afford to hire a company specializing in Internet services security that could watch over the security of the company 24/7 so they burden their technical employees to such an extent that it is very easy to make a mistake. I have often been a world of situations in which when searching Google Groups I came across otware of a group of employees of a company where they exchanged information about security or put on them various sensitive information from the point of business. You probably wonder what exactly it has is the connection with the creation of dictionaries? Hold on for a while and I'll give you a concrete example of how I would use it). After obtaining basic information such as names and telephone numbers of employees, working hours, distribution of departments in the company and the like I could try to learn a bit about politics of company passwords (if it exists at all, sometimes it happens). Let social engineering help us again :) it would look something like this: I would call an IT employee on Friday at 14.45 (Sounds strange but think about it so that everyone is tired after a hard week of work and when people realize that in a few minutes they end their heavy drudgery, many of them "turn off" logical thinking while enjoying the upcoming weekend) claiming to be an employee of one of the departments and pretending to be a completely "unknowing guest" I would sell him such a story "Here NAME SURNAME from such and such department. I have very serious problem. Yesterday someone broke into my private computer and stole all my bank passwords, data from various websites etc. The worst thing is that I had the same password everywhere. I reported it and told the police to change all my passwords. to do on my company computer but one of my colleagues from my department told me to at the beginning he contacted you because our company has some rules regarding passwords. Could you help me and tell me how to create the correct password? "I know that now people who are familiar with the topic will speak and say that nowadays administrators will not be fooled by this type of number just because they can change passwords" remotely "for all domain users. Yes it is true and in such a case such an attack will prove to be ineffective. But believe me or not that many small companies in Poland (in which I live ^^) can be caught. I used this attack several times myself and I received information about the complexity of passwords, which was enough to generate the right dictionary and reduce the time needed to complete the task. As you can see, a set of several seemingly innocent information combined with a good "played" phone (social engineering attack) acts like a deadly sniper shot: P I am aware of the fact that the examples I use are trivial ale it seems to me that they clearly show the value of reconnaissance and that every time spent on white intelligence will double pay.