# Cracking Guide

Hey, before introduction I must say some words to you. Thanks for checking this e-book, I included there 100% of my cracking skills, 100% of pure knowledge and 100% of basics that you will need to start your journey with cracking. This e-book is mainly for people who are entirely new to cracking. Especially for this e-book, I created a .ZIP file with a collection of programs that are mostly used to crack accounts. I do not want to teach you saturated methods which are worth totally nothing. I will guide you how to get an unlimited number of accounts in like one day. ***If this e-book helps you, please leave positive feedback on my thread.*** Remember, this e-book is only for educational purposes. I do not take responsibility for how you use it. I do not like tons of colors, text variations, and stuff, that is why this e-book looks like this. It is basic like it should be.

**I divided this e-book into several parts:**

* *First of all – software, some knowledge.*
* *SQL Injection – how to use SQLi Dumper, the creation of dorks and everything related.*
* *Let’s crack! – how to use Sentry MBA.*
* *Security – how to do not lure cops into your house.*
* *D4t4b4s3s – everything about databases.*
* *Dehashing – how to dehash, what is hashcat and more.*
* *Money making – how to make money with cracking.*
* *Regex – how to make your combolists better.*
* *RDP/VPS – how to use them to crack 24/7, which RDP/VPS should you choose.*
* *The end – just read it, please.*

# First of all

First of all, you will have to download the necessary software to start cracking. I created an individual package with software, so don’t waste your time and download all the required software right now!

Software included in the pack:

* *Sentry MBA – basic and the best tool for cracking.*
* *SQLi Dumper – a most popular tool for SQLi Injection.*
* *Configs – configuration (.ini) files for Sentry MBA.*
* *hashcat – the best and most advanced software for cracking hashes.*
* *Combolists – some public and semi-private combolists to start your journey cracking.*

Now let’s talk about some terms that can be entirely unknown to you!

**What are configs?**

What are configs? Configs are configuration files for the program Sentry MBA in extension .ini. Configs contain information without which the acquiring accounts of the service would not be possible. They are one of the most important parts of this program.

**What are hashes?**

What are hashes? Hash is a kind of changing passwords for security needs. There are different types of hashes, but how do I know type of hash? There is an excellent website to check hash types

**What are proxies?**

What are proxies? It is a proxy server that performs call on your behalf. There are .ini files that do not need proxies to work; we call them proxyless configs. We can scrape proxies via software, but also we can find them on websites like [that.](http://www.sslproxies24.top/) You can also buy better proxies on sites like [that.](http://fineproxy.org/)

**What is scraping? Is it better than your methods?**

What is scraping? Is that better than your methods? It is suitable for beginners, but there is very little chance of finding interesting account. A more advanced, which uses most of the crackers is SQLI injection. It involves the exploitation of databases.

**What is Sandboxie?**

Sandboxie is a software that allows you to run software in a sandbox. What does it mean? It means that any malicious software should not go outside this sandbox and infect your computer. Why I said shouldn’t? Well, it is easy to bypass Sandboxie, and some of the malicious software creators already did it, that is why you can use Virtualbox.

**What is Virtualbox?**

It is a virtual machine that allows you to install on it any operating system. You can install Virtualbox on your PC with Windows 10, and as your virtual machine, you can select Windows 7 or for example Kali Linux. If you will run malicious software on the virtual machine, there is no possibility to get your real PC infected.

# SQL Injection

The first question that arises - what is it SQLi Dumper? It is a program that allows you to quickly get to the databases of various websites by scanning a URL’s for vulnerable sites. As a result, we can quickly obtain user:pass combination or email:pass combination which is much better than scraped. You can also get more stuff like credit cards info (that is illegal, I will not teach you anything about it), users IP’s, DOB’s, real names and much more. Let’s start then!

The first step is configuring SQLi Dumper. You must turn off using proxies by program. Anyway, proxies usage should be disabled while you start the program. Okay, so this step is done, let’s move to the next one! As you may know getting URL’s without using a VPN is now nearly impossible, so you have to get a VPN. But wait, you don’t know what is VPN? It’s a software that allows you to change your IP address. You have to do it because Google engine bans IP after tons of requests. I recommend you [NordVPN](https://nordvpn.com/) (it’s paid, but hey, you can crack accounts yourself or search around cracking forums for it) – easy to use with good amount of locations. You can also use other VPN’s like, DoubleVPN or [Cryptostorm.](https://cryptostorm.is/) In my opinion Cryptostorm is the best VPN ever made. They don’t store logs and other stuff. You are 100% sure that you are secure and no one is logging your traffic. I

will tell you how to properly use VPN with SQLi Dumper on an example of NordVPN and SQLi Dumper v8.3, let’s start then. Now we will move to the hardest, but the most important thing called dorks. Dorks are an employee who unknowingly exposes sensitive corporate information on the Internet. I know, the definition is so hard to understand, so I will show it in noob-friendly way. For example you are looking for gaming stuff on .com sites you will use dork like *intext:gaming site:.com.* If you are looking for sites which have word *shop* in URL you will use dork like *inurl:shop.* Now it’s understandable for everyone I guess. Usually dorks are divided into 3 parts – keyword, expansion (later named page format) and parameter (later named page type) and some additional parts like domain and search function. Keywords are NOT most important thing for us. Of course, you can’t use something like “games to play for free” as a keyword, because it’s totally LQ. The thing that makes your dork HQ is parameter (page type). If you will choose good parameter for your dork you can call yourself a HQ dork maker. Since tons of crackers are using dorks, we will have to make/get unsaturated keyword. If you think that keywords like *gaming, league of legends, headset* are unsaturated you are wrong. We will have to find the best keywords. Better keywords equal more private databases, but also good parameter equal more private databases. More private databases equal more accounts. Expansions are something like page formats. Most popular expansion is *.php?*. Parameters are page types, for example *GameID=*, *id=*, *id\_product=*. But how can we create good dorks? Should we use something like dork generators? Definitely NO! Dorks generators are totally useless (while you are using them in most saturated way – pasting keywords from keyword searcher, but we won’t do it) since most of beginner crackers are using them to make dorks. Dorks generators are using random algorithm to generate dorks. It means that the dork generators are connecting keyword, parameter and expansion totally randomly. That’s why manual or semi-manual made dorks are the best. We will have to create dorks by semi-manual method. How? Everyone have their own methods, some of methods are really good and with them you can get 100% private dorks. Some of crackers are using their own scripts/software to generate dorks, but by other way than dork generators do. We will be using known yet, but semi-private method. I assure you that this method isn’t overraped like public ones which you can find on cracking forums. We will be using old combos and databases to get factory new and private dorks. I will also teach you how to connect every part of dork properly. I will show you a manual method and explain how dorks are built and how all this stuff works. Let’s start from the beginning, where are all those elements (parameters and expansions) used? Them are used in sites URL’s, let me show you a picture.



This picture should explain everything. Dorks created like that will look like this:

*inurl:default.asp site:.com inurl:default.asp site:com site:com inurl:default.asp*

*site:.com inurl:default.asp*

As you can see you can use four variations of this dork, each of them works the same way. The dot before *com* word means nothing, you can put it, but you do not have to. You can move elements forward and backward, so *site:com* can be before *inurl:default.asp* and *inurl:default.asp* can be before *site:com*, it does not matter. That is how dorks work, but it is the easiest part of this. You can create more and more advanced dorks. You can use more expansions and more parameters. You can search for better keywords and combinations of dorks. This is very extensive. Let me show you more advanced dork and explain it:

*site:example.com intext:"sql syntax near" | intext:"syntax error has occurred" | intext:"incorrect syntax near" | intext:"unexpected end of SQL command" | intext:"Warning: mysql\_connect()" | intext:"Warning: mysql\_query()" | intext:"Warning: pg\_connect()"*

Looks advanced? It is a little bit. Basically, with this dork, you can search for errors in MySQL database on site example.com. As you can see it is so simple, let’s take an *intext:”sql syntax near”*. It searches for *sql syntax near* string in the text. To make dork like this, you also need knowledge what SQL Error is and how/where you can find it. You can also do it with any other word like intext:”cracking software”. This dork will show you all the sites with *cracking software* words in the text of the page. Now everything about how dorks are built should be clear for you. You have already learned what dorks are and how to build them, it is still a small ‘dose’ of information about dorks. Anyway, it is enough if you want to start your journey with cracking. Let’s move to the most important part – creating private/semi-private and HQ dorks. First of all, you have to download pack of tools. You can find it above. If you already downloaded and unzipped it, you are ready to go! I will teach you how to write dorks by your hands, it is effective, and you can control all aspects. You can also use dorks generator, but it is overraped and overused already, I do not recommend it, you will waste your time, to be honest. As I said above, we will be using databases and combos to generate the dorks. How? Just by already leaked nicknames. Think a little bit about it – if someone’s account got leaked in random public database leak maybe you will be able to find another database leak with his credentials, this time private one. Nowadays people are using the same login/e-mail and password everywhere, they do not give a fuck about security, and we will take advantage of it. Millions of databases have already been made public, so you have millions of combinations to make unused yet dorks. Let’s start then! First of all – you need a good text editor. I recommend [Notepad++;](https://notepad-plus-plus.org/) it is easy to use and have all needed functions and amenities. Create a new text file on your desktop, right click on it and select *Edit with Notepad++.* Now you are ready to go! As far as I know people like definition called gaming dorks, so let’s make some. Probably now you think "where can I get databases?". I know an online cloud drive with tons of public databases. Click [here](https://cloud.mail.ru/public/DoJB/7jVCevA3Y/) to visit it. Now you have to search for gaming databases (if you want to make gaming dorks), you will know how to select them with site [Vigilante.pw.](https://vigilante.pw/) Now look for a random database on this cloud drive and try to find it on Vigilante (you can use Ctrl+F shortcut and make it easier). Let’s take GTAGaming.com database for example. As you can see on Vigilante it is gaming, so we got it! Let’s download it and look for usernames/e-mails. It is .sql file, so open it with Notepad++. As you can see there is much text, you can easily get lost in it, but I will show you a way how to make it easier for you. Scroll down until you see long lines with text and recognize e-mails or logins in it. One row equals one entry in the database. Copy the nicknames without spaces and special characters. Grab like 30 usernames and paste them into an external .txt file. Save it and put on your desktop or somewhere. Before we move to the dorks creation part, you need to see more page formats, page types and search functions.

|  |  |  |
| --- | --- | --- |
| **#** | **Page format** | **Details** |
| 1 | .php? | *Indicates a PHP page.* |
| 2 | .php3? | *Indicates a PHP page.* |
| 3 | .php4? | *Indicates a PHP page.* |
| 4 | .html? | *Appeals any file that is HTML. As popular as .php?, .php3? and .php4?.* |
| 5 | .htm? | *It also appeals any file that is HTML or XHTML.* |
| 6 | .cgi? | *Stands for Common Gateway Interface* [*(*Wikipedia*)*](https://en.wikipedia.org/wiki/Common_Gateway_Interface)*.* |
| 7 | .asp? | *Indicates that the web page is an Active Server Pages* [*(*Wikipedia*)*](https://en.wikipedia.org/wiki/Active_Server_Pages)*.* |
| 8 | .aspx? | *Pages with the .aspx extension use compiled ASP.NET.* |
| 9 | .jsp? | *Stands for Java Server Pages (*[Wikipedia*)*](https://en.wikipedia.org/wiki/JavaServer_Pages)*.* |
| 10 | .cfm? | *Indicate that the file is a ColdFusion file (content management tool).* |
| 11 | .cfml? | *Indicate that the file is a ColdFusion file.* |
| 12 | .pdf? | *Just a PDF file.* |

|  |  |  |
| --- | --- | --- |
| **#** | **Page type** | **Details** |
| 1 | item\_id= |  |
| 2 | page\_id= | [Click here to see the full list of page types](http://thecrackingbay.pw/pagetypes.txt) |
| 3 | user\_id= |  |

|  |  |  |
| --- | --- | --- |
| **#** | **Search function** | **Details** |
| 1 | inurl: | *Searching for keyword contained in page URL.* |
| 2 | allinurl: | *Searching for URLs with more than one keyword. E.g., allinurl:”free-games”* |
| 3 | intext: | *Searching for keyword contained in the text of the page. Ignores links, URLs and page titles.* |
| 4 | allintext: | *Searching in the text with more than one keyword. E.g., allintext:”gaming keyboard”* |
| 5 | intitle: | *Searching for keyword contained in the page title.* |
| 6 | allintitle: | *Searching in the title with more than one keyword. E.g., allintitle:”gaming chair”* |
| 7 | cache: | *Displays the version of the web site stored by Google in the cache.* |
| 8 | link: | *Displays a list of pages containing links to the page, e.g., link:www.google.com* |
| 9 | filetype: | *Searching for specific file type e.g .xml, .pdf, .doc, .xls.* |
| 10 | link: | *List webpages that have links to the specified web page.* |
| 11 | related: | *List web pages that are similar/related to a specified web page.* |
| 12 | inanchor: | *Searching for pages related to the specified anchor text.* |
| 13 | allinanchor: |  |
| 14 | info: | *Tells Google to bring back info about a specific domain.* |
| 15 | loc: | *List websites that are in specified after : city/country. E.g., loc:Amsterdam.* |
| 16 | define: | *List definitions about specified after : word. E.g., define:being.* |
| 17 | ~ | *Searching for synonyms for specified term. E.g., ~car.* |
| 18 | - | *Removes pages with specified term. E.g., -inurl:github.* |
| 19 | .. | *Searches for a specified range of numbers. E.g., intext:”guinness records 2010..2018”* |
| 20 | \* | *Can be any word. E.g., intext:”gaming\*” will search for gaming headset, gaming laptop, gaming PC, gaming mouse, etc.* |

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Dork format** | **Example of dork** | **Notes** |
| 1 | <ptype>=”<keyword>” + „<domain>” | *page\_id="games" + ".com"* |  |
| 2 | <sfunct><keyword><pformat><ptype>= site:<domain> | *inurl:games.php?category= site:com* | Use domain without dot |
| 3 | <pformat><ptype>="<keyword>" | *.html?category="games"* |  |
| 4 | <sfunct>"<domain>" + "<keyword>" | *inurl:".com" + "games"* | Use only with inurl: and allinurl: |
| 5 | <keyword><pformat><ptype>=<num> | *games.asp?page\_id=8* |  |
| 6 | <sfunct>"index of/" + "<keyword>" | *allintext:"index of/" + "games"* | Use only with intext:  and allintext: |
| 7 | <sfunct>"<keyword>" +  "<domain>"<pformat><ptype> | *intext:"games" +*  *".com".htm?param=* |  |
| 8 | <keyword><pformat><ptype> | *games.php?id=* |  |
| 9 | <sfunct>"<keyword>" OR "<keyword>" | *intext:"games" OR "gaming"* | Searches for games or gaming word in text |
| 10 | <sfunct>"<keyword>" OR "<keyword>" -  <keyword> | *allintext:"games" OR "gaming" -free* | Searches for games or gaming words but without free word in text |
| 11 | <sfunct><keyword> -<sfunct><keyword> | *ext:pdf -site:example.com* | Searches for files with .pdf extension but not on example.com site |
| 12 | "<keyword> | <keyword> | <keyword>" site:<domain> | *"gaming | games | gamer" site:com* | Simply | replaces OR |
| 13 | <sfunct>"<keyword> | <keyword>" +  <sfunct><pformat> | *intext:"game | gamer" + inurl:php?* |  |
| 14 | <sfunct>"<keyword>" -<keyword> -  <keyword> | *allintext:"game" -terraria -minecraft* |  |

It will be easier to understand when I will introduce some „symbols”, so:

*<keyword> - insert here a keyword,*

*<pformat> - insert here proper page format,*

*<ptype> - insert here proper page type,*

*<sfunct> - insert here proper search function,*

*<domain> - insert here proper* [domain](https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains)*e.g., .de, .pl, .com, .net, .br, .ru, .edu, <num> - insert here a random number e.g., 100, 2, 547, 57, 4217.*

You can experiment with the dorks formats. There are tons of combinations, just think a little bit. I gave you, in my opinion, the best options for searching for exact keywords. So let’s test it before we make some dorks manually. I will copy a random username from the random database and make from it simple dork. I copied „betafield23” nickname, and now I will add to it only a search function. I

have made this dork: *intext:”betafield23”*. I pasted it into google and [look what I have got.](https://www.scribd.com/document/371804690/Base) You can repeat it and check if you will get the same result as me. In your dorks use random nicknames as keywords, and that is it. There is also another way to make dorks, with common/popular keywords. How? You have to use the proper parameter for your dork. However, how you can know which parameter is good for your dork? It is simple, just do a little research on websites. Let’s take a *pcgames.asp?id=* dork for example. It is effortless but good. After the page format, you can add a random number; it will make the dork less saturated. Do a little research about sites URL’s, try to look at them and make some dorks from them. Everything is about keyword and parameter. Of course, don’t forget about other parts of a dork, they are important too. For example – use mainly .php?, .asp? and .aspx? page formats, because on these you can obtain a SQL Injection. I gave you other formats just for a lookup, you can use them, but I do not recommend it. If you will connect the method about gathering usernames and the second method you will definitely create HQ dorks. I cannot use the brain for you, that is it. So yeah, let’s make some dorks now and paste them into SQLi Dumper. Open the file which you made in previous steps and start making dorks from nicknames. Use the table to make it faster and easier. Try to make like 50-100 dorks. Don’t make them too complex, just simple ones like I did. Hint – by adding a country code (e.g .pl, .com, .net, .ru) you can get „more private databases”. Another hint – if you are searching for (for example) European combos do not use domains like .co.uk. Use EU domains. If you are searching for Polish websites, just add to your dork .pl country code (domain). Try to make as many combinations of dorks as you can. Usually, use like 1.000-2.000 dorks. More dorks – more URLs to gather, but don’t hurry, I mean don’t make like 10.000 dorks at once. You will waste your time. Always use not more than 3.000 dorks. Okay, when you made them, we can move to SQLi Dumper. Open the program (always use v8.3 version, it is the best). Wait till it will load all needed functions and features and move to *Tools & Settings* tab. Move to *Proxy* subcategory and make sure that proxies usage is disabled (using proxies will slow the getting urls and dumping database process). Now you can go back to *Online Scanner* tab and paste your dorks in this big white field on the center of the window. Make sure that you do not have anything in the left, and right labels and all search engines are checked. Everything should look like this:



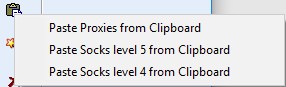
If everything in this step is done, we can move to next one – VPN configuration. We will be using the NordVPN because as I know, they do not store any data about you, like for example, HideMyAss does. There is only one thing – NordVPN is paid. You will have to find an account for it on any cracking forum or ask me for it; maybe I will have some. Okay, so download NordVPN and install it, then open. You will see the login window, so you have to log in. After logging in you can start changing your IP, move to *Countries* tab, hover your mouse on the random county (I prefer EU countries like Germany, Poland, Netherlands, Romania) and click on the button with three stripes. It will show you how many servers are available to connect with. Select first one (choose *The Best Servers for you* sorting) because it is not overloaded and in affordable distance from you. Connect with it to be secure, then click *Start Scanner* in SQLi Dumper window and select *URLs Only* option. As you can on the left side of the window there are a statistics about loaded URLs, quantity of URL’s, which URLs are added properly and elapsed time till you started the process. You have to watch the first position in *URLs Loaded* category – Google search engine. If you will see that Google stopped adding URLs to queue you have to change your IP by clicking on next position from the list in NordVPN. Don’t care about other search engines; Google is the most important for you now. Try to get like 5.000-7.000 valid added URL’s, then stop the process. If Google is adding URLs slowly, just change your IP again. You can choose between countries of course. The right amount of valid added URL’s per minute is like 500-1.000. It also depends on your internet speed, so don’t worry. I think that is all about gathering URLs. If you already have like 5.000-7.000 URL’s you can move to *Exploitables* tab. There is nothing about clicking the *Start Exploiter* button at 80-100 threads. Click it and wait till it finishes exploiting the URLs. It can take up to an hour, so be patient. More URLs equal it will take more time. There is no estimated amount of exploitable URLs. It usually depends on your dorks quality and previously gathered URL’s. Okay, so if the process already ended you can just move to the next tab (simple, ha?) called *Injectables* and again, click *Start Analyzer* at 20-30 threads. It will analyze if the exploitable URL’s are Injectable. If URL is injectable, you can easily get to the database of the selected site. This process can take up to several hours, so leave SQLi Dumper running in the background while it is analyzing the URL’s. More exploitables to analyze equal more hours to analyze it. If it is done, you can move to next step – database gathering. Select all injectable links from the list (right click on the list and choose *Select All* option), then expand the *Search Columns\Tables Names (MySQL and MS SQL)* – blue text right above the progress bar. Now you can see textboxes and settings. In the first four textboxes, you can type what you want, but you may ask what is the meaning of what we will write there? That are the tables/columns names (choose the default option - *Columns*) which we want to search in the database – for example if we want to search for email and password columns we have to write there this two keywords. We can call it target to search. If you are searching for email combos, I recommend you terms like email, e-mail, mail. If you are searching for password columns, you can type pw, pass, password. If you want to get usernames/logins columns search for login, username, the user. Of course, you can search for other things like IP address, first name, last name etc. It depends on your needs. If you already know what you want, you can move to next step. Check checkboxes next to this textboxes and click *Start* button (I prefer checking only two checkboxes e.g., email and password). A new window will open. In this window, you can see few things – website domain, full website URL, method, which term was found (*Search*) and quantity of rows in the database. If you already finished searching for columns, you must know how to select good databases to dump. What I mean by saying „good databases”? I mean that the database must have exact the same (or very similar) quantity of logins/emails and passwords. It’s again about using your brain – if database have like 100.000 logins and only 20.000 passwords it’s empty in 80%, so do not waste your time to dump it. Also, look at columns names. Okay, so if you already found a good in your opinion database, you must dump it. Do it by left clicking on the website URL and select *Go To Dumper* and *New Dumper Instance* option from the top panel. A new window will open. You can see tons of options. We will take care only about few of them. First of all, let’s change some settings to dump the database much faster. We can select threads to 50 by checking the checkbox near *Threads* word and moving the slider to the right. You can also set timeout to 2500ms and delay to 50-100ms. Leave retry limit at 5. Now on the list on your left side you can click on chosen by you table and click *Get Columns* button above it. You will get a list of columns. Find there columns containing username/password/whatever you want and click *Dump Data* button and yeah, that’s all about dumping. If you already dumped database you can save it by clicking *Export Data* button. You will see a small window with some options. If you want to dump in the format that the Sentry MBA accepts you must set custom delimiter to : char and export it as plaintext, then click *Start..*. Wait till SQLi Dumper finishes process and that’s all about searching, dumping and saving your database. Now you can just dehash it (if it is hashed) or import to cracking software. That’s also all about SQL Injection in SQLi Dumper at this point. To dump databases you can also use sqlmap, which is available on Kali Linux or you can install it on Windows (it requires python). It’s a bit faster than SQLi Dumper. I won’t teach you how to install it on your PC or how to install Kali Linux, you can find it easily by searching for it via Google. I can give you a few commands which will help you to dump the database. But you may ask what is sqlmap? Sqlmap is a software for dumping databases written in python. It is preinstalled on Kali Linux, but not on Windows. It’s more professional than SQLi Dumper, it do not have fancy GUI. It’s a console program, so you need to know few commands to make it run. First of all you have to scan the database (to know if it is vulnerable), so use **sqlmap -u „<site URL>”** command, but remember that you must type the site URL with quotes. After scanning you can get into the database. Firstly you have to check the databases, to do it use **sqlmap -u "<site URL>" --dbs** command (with double – character before dbs word). Again use quotes before and after site URL (do not use <> characters, they are here just to give you a preview). Sqlmap will throw a list of the available databases, so you must get a tables from selected database. By using **sqlmap -u "<site URL>" -D "<selected database>" --tables** command you can do it. Sqlmap again will give you list of available tables, so let’s get the columns from selected database using **sqlmap -u "<site URL>" -D "<selected database>" -T "<selected table>" --columns** command. Now you see the columns, so we are at the final point. Let’s dump data from them then! Use command **-u "<site URL>" -D "<selected database>" -T "<selected table>" -C "<column1 name>, <column2 name>, ..." --dump**. As you can see after -C switch I entered two columns (you can enter more, that’s why I put there ...). Remember to enter every column delimited with comma character, that’s necessary. But that’s not all, you can add some switches to this last command like **--eta** (shows estimated time of wait till the dumping process will end), **--hex** (if you are getting errors (orange color)), **--threads** (if you want to dump data with more threads, I recommend using this switch to dump data faster), **--proxy=<proxy>** (if you want to connect to the target URL using proxy), **--proxyfile=<path>** (if you want to use more proxies from a text file), **--tor** (to use Tor anonymity network). That’s all about sqlmap, it’s not necessary to use this tool, if you are beginner use SQLi Dumper, because it’s simple and easy to use. Sqlmap is move advanced, for more advanced users.

**Let’s Crack!**

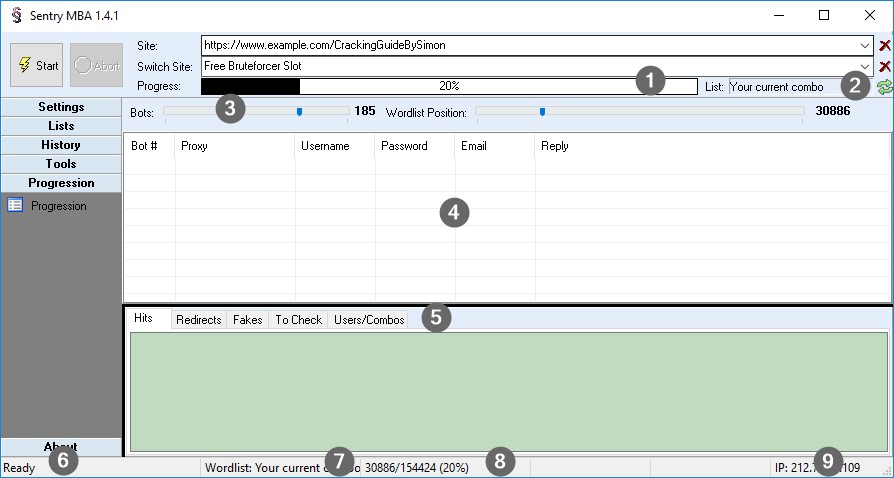
Okay, so you already know what SQL Injection is, how to create HQ and private dorks and how to use them. I guess you already got your dream database, so it is time to use it to get accounts. On the market are two types of software – sh!tty and very good. How to recognize them? It is simple; there is only two good software – Sentry MBA (created by Sentinel and Astaris. The latest, original and pushed by them version is 1.4.1) and SNIPR (made by PRAGMA). Rest of them are made only to make money from beginner crackers, so don’t even buy them. If there will be something good like Sentry MBA, I will write about it an announcement. SNIPR is paid and not that advanced like Sentry MBA (but SNIPR have tons of preinstalled configs regularly updated by authors, that is a significant benefit) which is totally free. I will teach you how to use Sentry MBA to crack accounts because using SNIPR is very, very easy if you already know how to use Sentry MBA, so let’s start. If you did not download my pack of tools yet, you could do it now (link is on the first pages of the e-book). Unzip it and search for Sentry MBA folder. Open the program, go to *Settings* tab (located on the left side of the window), then select a *General* subcategory. Now you can see some options, but at this stage, there is only one crucial button called *Load Settings from Snap Shot*. Now I can tell you what Snap Shot is – it is a .ini file (by crackers called config, I will use this term too) with info about the cracked website. It is just a configuration file which Sentry MBA needs to work. You can find these files mainly on cracking forums, but I provided some of them on my Discord server. I am regularly updating them, but if you find that something is broken just PM me. Okay, so it is time to load your config (Snap Shot). Click on *Load Settings from Snap Shot* button and load your .ini file. If you adequately loaded your config, you should see a website address in *Site:* box.



Everything should look like in the included image. Pretty easy I guess. Now if config requires proxies, we should load them, but how to recognize if config needs them? We must move to *Proxy Settings* subcategory. Moreover, again, there is only one option that you must know. If the checkbox next to *Do not use proxies* term is checked it means that you do not need to load proxies. It also means that the config is proxyless (do not require proxies) If the checkbox is unchecked, you need to load proxies. You may wonder why some configs require proxies and some of them are proxyless? It depends on site. If the site does not ban IP’s after a significant amount of request then you can make a proxyless config, but most of the sites ban IP after tons of requests, so that is why you need a proxy. It is time to load proxies (if your config needs them, if not you can skip this process). Move to *Lists* category, then select *Proxylist* subcategory. Where should you get your proxies? Well, it depends on your budget. You can get free HTTP(S) proxies [there](http://www.sslproxies24.top/) but don’t except that this proxies will be excellent. They are free, so yeah, don’t expect miracles. You can also buy proxies on sites like [fineproxy](https://buy.fineproxy.org/eng/) or [VIP72.](http://www.vip72.com/) Fineproxy is, in my opinion, one of the best paid proxies providers. You can also use programs called „proxylists scrapers” to scrape proxies from multiple sources. You can find them on cracking forums but remember to run them sandboxed or on your virtual machine. Okay, so let’s get back to Sentry MBA and select this icon.

As you can see you can paste from your clipboard three types of proxies, but how can you know which type you should choose? Well, I recommend you always using HTTP(S) (first position on the list), an exception is when config maker mentioned that

you should use SOCKS proxies. For you – a primary user, this does not matter in my opinion. We can divide HTTP(S) proxies into three categories – transparent, anonymous and elite. Let me explain all of them. Transparent – good, but still can show your real IP and identity. Anonymous – hides your IP and identity, but service still recognizes you as a proxy user. Elite – hides your IP and identity, additionally tells the system that you are not a proxy user. Okay, so copy your proxies from a text file and paste them to Sentry MBA. Hint – you can check your proxylist with software called uProxy (you can find it in my pack of tools). This program will show you which proxies are working and some more useful info. If you did it correctly, you should see all of your proxies on the table. You can move to the next step, the final one – loading your combolist. To do it move yourself to the *Wordlist* subcategory and click the folder icon near the green/cyan(?) box. Select your combo file; then you should see your combolist on the cyan background. If your combo is big it can take some seconds after it will be loaded, it also depends on your PC speed. Remember that your combo must be in user:password or e-mail:password format. There should be : char as a delimiter. Everything is set up; we can start cracking! Let’s move to *Progression* category. There is much to explain. First of all, let’s talk about this standard, big window, then we will move to this small one.



As you can see, there is a progress bar (1) which informs you about cracking/bruteforcing progress. Next to progress bar you can see your loaded combo name (2). There is also bots slider (3). If you are using proxyless config, I recommend you using not more than 10-15 bots/threads. If you are using config with proxies, you can go up to 150 threads. On the center you can see a table with some info (4) – Bot # is a number of bot/thread. Proxy – which proxy from the previously selected list is used by bot. Username and Password – currently checked by bot username and password combination. Email – nothing to do with it, it is not important. Reply – reply from website/server. Next, you can see another five tabs (5), let me explain the meaning of them. First one called Hits – you will see there all valid accounts (successfully cracked), it is the most important tab for you. Redirects – basically redirects, nothing to explain. Fakes – well, just fakes and again nothing more to explain. To Check – it is also an essential tab. If your proxies are very LQ, after few minutes of checking your hits and wrong combos will go to this tab. You have to watch this out. Users/Combos – some configs only capture premium accounts, and if the creator of config will improve a function that is moving the free accounts to separated tab, you will find them right there. Moreover, at the end, we can see a Sentry MBA status (6), actual wordlist (7), wordlist position (the same thing as the slider next to bots slider) (8) and your current IP (9). Hint – after loading a new combolist into Sentry MBA you have to click the green arrows button next to list box. Sometimes Sentry changes it automatically, but not always. Let’s move to this small window; I call it a “status window”. It shows you status about everything. Firstly let’s talk about *Results* section. It is nothing else than info from the tabs that I was explaining above (number 5). So if you will get a hit it will show in the first tab and next to *Hits:*. Next one called *Performance* informs you about already tested rows from combolist, retries made to server (it is really important, if you have LQ proxies you will have large amount of retries, if your proxies are HQ, retries amount will be much lower), combo/min (or CPM) – how many combos Sentry tests per minute and ORC Rate – nothing to do it at this step, some of the configs have automatic OCR solving function. It means that the captcha is solver automatically by Sentry MBA. That is info about percentage of correct solved captchas. Proxies tab informs you about your proxies status. If you are using a proxyless config you do not have to worry about it. The first category tells you about active proxies, next one about disabled and banned proxies. The count is about all proxies count. This category is also relevant. You have to watch it if the service you are cracking bans proxies or no. If your active proxies will be at 0, cracking process will automatically stop, so all proxies will be disabled or banned. Okay, and finally the *Codes:* category. It informs you about response from server. Let me explain all of those codes in a table.

|  |  |  |
| --- | --- | --- |
| **#** | **Code** | **Details** |
| 1 | 200 | *Everything is working. Successful HTTP request.* |
| 2 | 3xx | *A user action needs to be taken.* |
| 3 | 401 | *Authentication failed.* |
| 4 | 403 | *Access denied.* |
| 5 | 404 | *Resource not found/not available.* |
| 6 | 407 | *Proxy authentication failed.* |
| 7 | 413 | *Request entity is too large.* |
| 8 | 419 | *Authentication timeout.* |
| 9 | 420 | *Method failure.* |
| 10 | 421 | *Connection limit exceed/service not available. Your IP may be blocked/banned.* |
| 11 | 430 | *Invalid username or password.* |
| 12 | 5xx | *Syntax error.* |
| 13 | xxx |  |

Watch this codes to figure out what is going on. Well, if you already know everything about basic Sentry MBA elements you can move to the final part. Click the big *Start* button in the left top corner and let Sentry crack accounts. If you get a valid account, you will see it in *Hits* section. Output of your hit should look like **#<number of hit>:https://<username>:<password>@<website> - Success Source Keyword Match -> Found key [<success key>] – Source Length: <source length>**. You can right click on it and copy the combo to the clipboard. As an output you will get username:password. You can also go to *History* tab to see all of your saved hits (Sentry MBA have autosave function, do not worry). In History tab you can aim for a specific site by selecting a site filter. You can also save the hits in the selected format. I will not explain there everything about it; I will tell you how to add a custom filter to copy accounts. To do it you must move to *Options* subcategory. As you can see, there is a list called *Save Filter:*. On this list, you can find a default save filters. To add new, custom filter type it in the box next to *Save Filter:*, then click *Add Filter to Filter List*. There are some operators that you need to know (only a few of them, at this stage you do not need more).

|  |  |  |
| --- | --- | --- |
| **#** | **Operator** | **Details** |
| 1 | <COMBO> | *Your hit in username:password format.* |
| 2 | <KEYS> | *Captured keys like balance etc.* |
| 3 | <SITE> | *Cracked site address.* |
|  | **Additional options (extended)** |  |
| 1 | \n | *New line.* |
| 2 | \t | *Tab character.* |

So yeah, everything about cracking accounts using Sentry MBA should be clear for you now. You know how to import combolist, proxylist and how to operate with Sentry MBA. If you want to learn how to create a config for Sentry MBA search for tutorials on YouTube. I will not write a guide about it, because it is much work to write it as plaintext, video tutorials should be much better to understand.

# Security

Security is the most important thing if you are a cracker. First, seal your webcam (just kidding, but…). You must care about your security more than typical PC user. **Take care of your password**, yes, your own password. **Don’t use the same password for every service**. **Don’t use common things** like your name, date of birth, child’s name, mom’s name, etc. “When Mark Burnett analyzed 3.3 million passwords to determine the most common ones in 2014 (all of which are on his bigger list of 10 million), he found that 0.6 percent were 123456.”[(source)](https://wpengine.com/unmasked/). I recommend you to **generate your passwords**. It is the most secure thing that you can do, create a complex password. What I mean by saying „complex”? To create a complex password use uppercase and lowercase letters, special chars like #, @, !, %, use at least eight characters (more characters, more complex password), and as I said don’t use common things in this password. Your common password should look like this: 2q)q\v?'9CYUqEYg. You can create it via random password/string generator, but take care, some of them may send the generated passwords somewhere or log them. **Don’t use random e-mail hostings** that are important. Use e-mail providers with the best security, like Gmail, Hotmail (if you want to take illegal actions on this e-mails do not do it, they log everything obviously. Use [cock.li](https://cock.li/) for example). **Always enable 2FA** if it is available! You should do it to prevent unauthorized login attempts to your account and do not tell anybody in the web your phone number on which you are getting the verification codes. **Encrypt your passwords and back up them**. Back up encrypted passwords on a flash drive like pendrive. **Do not login to important websites** (like a bank, PayPal, etc.) if you are connected to public Wi-Fi or free to use VPN software. That should be enough about your accounts, move to the cracking part, why security is necessary? As you may know bruteforcing/cracking and SQL Injection to other services than yours is illegal. That is why **you should always be connected to VPN**. Connect to VPN at the start of your PC. As your main VPN, I recommend [Cryptostorm,](https://cryptostorm.is/) you should also read history about the creator of this VPN, [Douglas Spink](https://encyclopediadramatica.rs/Douglas_Spink) because he is also a member of Cryptostorm. Forget about Google, Bing, Yahoo, and other big company search engines (because of logging everything, again), use [DuckDuckGo](https://duckduckgo.com/) or [Startpage](https://www.startpage.com/) (personally I prefer DuckDuckGo). If you want to create a test account or a temp account, use temporary e-mail providers like [temp-mail.com.](https://temp-mail.org/) **Don’t create random accounts on one of your private e-mail accounts**. If you want to take illegal/shady actions, do not use Skype, Discord or forums PM system (it is the worst thing that you can do, obviously and usually, they do not even encrypt your messages) use [XMPP.](https://xmpp.org/) If you are downloading something from the web, **remember to open it on a virtual machine**. If you have some funds, you can **buy RDP or VPS**. Cracking on your PC is risky (if you did not know it already), so I recommend you to get a good RDP such as [BoomRDP.](http://www.boomrdp.com/) **Do not trust anyone** in any way. It is essential. **My opinion about Quad9** in one word – sh!t. If you do not know what Quad9 is, you can read about it [there.](https://www.globalcyberalliance.org/initiatives/quad9.html) They say that they only log geolocation data „for the purposes of tracking the spread of requests associated with particular malicious domains”, but I do not trust them at all.

# D4t4b4s3s

Now, let’s look at databases – something you will have to work with all the time. However, what exactly database is? The database is a structured set of data. Some data from the database can be hashed, and you will have to dehash it, but you will learn more about it in next parts of this e-book. So it is not only a set of usernames or e-mails and passwords, some of the databases can be in a format like *id:username:password:IP:first\_name:last\_name* etc. I think that you want to know how to remove the unnecessary data from the database to make it pure user:pass or e-mail:pass (the process of removing unnecessary data from the database is called *parsing*, you should remember this term). To do it you will have to use a program called [EmEditor](https://www.emeditor.com/download/) (it is paid, but they provide a 30 days trial, so do not worry). It is much more advanced than Notepad++, and I prefer using it for every database-related action. It can open a 20GB of data without a problem, that is why you should use it. This software helps with every database-related action; you can easily sort/delete data using it. Okay, so after downloading and installing this software, you can right-click on a database icon (located on your desktop or somewhere else) and choose *EmEditor* option from context menu. Your database will be opened via EmEditor. Again, as an example of the unparsed database, I will take the *gtagaming.com* database.



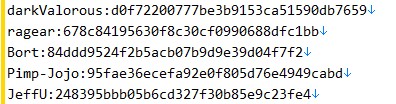
As you can see in included image every „data cell” is delimited with the comma character. We call this a delimiter. So you have to set the delimiter of each cell to the comma. To do it look at the *CSV/Sort* menu located at the top of the window. Right click on it and select *Customize CSV...* option from context menu. As you can see you can add/edit the formats and delimiters. The comma delimited should be added default, so I do not have to worry about it. If your delimiter is, for example, a – character, you have to add it by clicking *Add* button and changing the delimiter to – char. If you are done just click *OK* button. Select the proper sorting option from the menu *CSV/Sort* menu and click on it (I have chosen *Comma separated* one because my delimiter is a comma). As you can see everything that was delimited with a comma is now in the separated cell (every cell have a number). Now you can quickly delete unnecessary data, just select it and delete (it may take some time, depends on your PC components). I want to have a user:hash combo, so I removed every cell except one with usernames and one with hashes. If you did everything correctly, you could go back

to the standard view by clicking on this icon . As you can see the format of the database diametrically changed.



As you can see the format is still unreadable by cracking programs, so let’s remove the quotes and apostrophes. Do to it you have to click the combination of buttons Ctrl + F. Now you can see the small search/find window. So, let’s click on the *Replace >>* button and in *Find* field type the character that you want to be removed. Remember to not replace the quote character (in my situation) between username and password (so you have to replace the ,, and

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, characters, not single quote). Leave the *Replace with* field empty and make sure that you do not have checked the *Use Regular Expressions* checkbox. Click Replace All button to remove all characters. As you can see after replacing the characters, you have the database in format username,hash. Now just replace the quote with : character and everything is done! The output format is user:hash. You can import the combo to hash cracking software to make it user:pass, but you will get this knowledge in next part of this e-book.



You can do it with any database, just remember to select the proper delimiter. You can also replace delimiters by Ctrl + F. It is pretty easy, so I will not teach you how to do it. But how to combine all databases into a big one? Well, you can try to use other text editors, but again, EmEditor is the best for it. Using EmEditor you can easily combine millions of rows. Select files from your desktop/folder that you want to combine into one .txt file. Right click on one of them and select EmEditor option from context menu. When all files will be fully loaded choose *Tools > Split/Combine > Combine Documents into a Single File...* from the top bar. As you can see all selected files/databases are checked, so you just have to do is choose the destinated location of combined databases, name it and choose the extension of output file. If you are combining the databases, I recommend you .txt extension. Click *Save*, *Next* and again *Next.* Wait till all databases will be combined and it’s ready. Now you can open your output file with combined text.

# Dehashing

First of all – what is dehashing? It is a process of getting a plain string of random letters and numbers. It is also a security measure not to store plain passwords in the database. There are many types of hashes. There also exist „salt” term, but what is that? Salt is an additional part of the hash. It has randomly generated string added to the hash. If it is added, then the hash is harder to dehash. I will not explain every hash type there. To recognize a hash type you can use [this](https://www.onlinehashcrack.com/hash-identification.php) site (in hashcat every hash have it is own code, for example, MD5 have 0). However, how can you recognize hash? It is just a combination of letters and numbers. For example:

MD5 hash: *8743b52063cd84097a65d1633f5c74f5*

SHA-256 hash: *127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935*

You cannot even recognize what letters are used in the real password, so how you can check it? There are some programs to do it, but the most advanced and the best is [hashcat](https://hashcat.net/hashcat/) – console program that allows you to dehash almost every type of hash and get a plain string (password)(do not buy any paid dehashing programs, hashcat is free and the best). It is world’s fastest password recovery tool and can come in CPU-based or GPU-based variants. This software can dehash for you large databases with millions of rows. The dehashing process speed depends on your PC components. Better components equals faster dehashing. You will also need a large dick; oh wait, a large disk for dictionaries. However, why you need them? Hashcat without dictionaries/wordlists is useless (you can use a bruteforce mode to dehash without dictionaries, but it will take years to crack a simple password like *fuckmedaddy157*, that is why we will use wordlists). Wordlist contains billions of passwords combinations. Where can you find the wordlists? Well, one of the best free wordlists is [CrackStation’s one.](https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm) It is 15GB of wordlists (small dictionary, but very, very good). Another one are [hashkiller’s wordlists.](https://hashkiller.co.uk/downloads.aspx) What is the good amount of wordlists? As much as possible. When I was cracking hashes, I had over 200GB of wordlists on individual drive. [There](http://thecrackingbay.pw/wordlists.txt) is a list of useful links to download the dictionaries. Let’s move to the practical part. Download hashcat and unzip it into a folder. Open this folder, right click on blank space and select *Open command window* here option from context menu. You will see a console window with hashcat path. As you probably already guess, it will not work without commands, so you have to learn some, but you have to do something else before it. You have to create one folder and one .txt file in hashcat folder. Name the .txt file *hashes.txt* and the folder *dict*. In folder put all your wordlists (do not have to be in .txt extension, some of the wordlist have .wordlist extension, and hashcat still loads them). In the hashes.txt file, you will have to put your hashed database/combo in format user:hash or e-mail:hash. Move again to console window and type command:

## hashcat64.exe -m 0 --username hashes.txt dict

***-m*** *– after this argument type the hash ID (you can find all ID’s* [there*)*](https://hashcat.net/wiki/doku.php?id=example_hashes)*,*

***0*** *– the hash ID/code,* ***hashes.txt*** *– file with hashes,* ***dict*** *– folder with dictionaries/wordlists.*

After initializing this command hashcat will check compatibility and format of loaded hashes, then dehashing process will start. You can check actual status by clicking *S* on keyboard (you will see info like wordlist positon, current status, how much hashes got cracked already and much more) and bypass current wordlist by pressing *B*. You can also exit by clicking *E*. When hashcat will finish dehashing you have to save your dehashed combo in format user/e-mail:pass. To do it execute this command:

## hashcat64.exe -m 0 --username --show hashes.txt --outfile-format=2 -o cracked.txt

***0*** *– hash code that you set in the previous command,* ***hashes.txt*** *– file with hashes,* ***cracked.txt*** *– will be a file with your plain user/e-mail:pass output. You can name it as you want.*

That is all. Simple and noob-friendly. Now you can open your output file, load it to Sentry MBA or SNIPR and start cracking.

# Money making

I guess you were waiting for it. If you are wondering how to make money with cracking this chapter is for you. Now I will give you some methods to make money with cracking.

*#1 Sell cracked accounts* – yes, that is a useful method, but... But don’t open shop with Spotify accounts, Grammarly accounts or something overraped like that. Shops like that are overraped. Try to search for country-targetted websites which provides premium subscription or paid tokens (look for sites like that in your country). Don’t sell them on cracking forums, because you will not get customers for country-targetted websites, sell them on auctions-related websites in your country. The only accounts that are worth to sell on cracking forums, in my opinion, are VPN’s and pornrelated accounts.

*#2 Sell combos* – make your shop with private/semi-private combos that you got by SQLi Injection and sell them. You can make e-mail access targetted shop or simple shop with user:pass combos. Remember, don’t sell crap. You will only gain a negative reputation and scam reports.

*#3 Open a service* – open a service about something related to cracking. If you have useful hashcat wordlists and you are sure that you will be able to crack most of the hashes (~85-90%) you can easily open a service about cracking hashes. You will be able to gain some money by cracking hashes and use dehashed combolists for your personal needs (don’t sell them). You can open something new, I will not sell you ideas, use your brain.

*#4 Sell dorks* – if you are excellent dorks maker open a dorks shop. If you provide some vouches and your vouchers will be satisfied your sales will raise. You have to know what you are doing, again, don’t make crap, overraped dorks with public generators. Use your brain to make something delicious.

*#5 Sell your knowledge* – if you are an advanced cracker you can sell your experience. Open a coaching service about gathering dorks, getting combolists, or open a configs shop in which you will be selling your hand-made configs for Sentry MBA or SNIPR.

*#6 Sell currencies* – you can crack accounts to popular games and sell in-game currency. It is a really good business if you know that your customers will not get banned for it. You can sell gold, coins, items or whatever you want.

*#7 Crack4you* - if you have a good PC or RDP you can open crack4you service. Your customer will provide you combolist + config, and you will use the power of your PC to crack for him accounts. He will pay for hits that you will get for him, and you will have profit.

# Regex

Disclaimer – only underlined functions are regular expressions.

In this part, I will show you how to refresh your old combos. As I guess you want to know what is a regex (full name of it is a regular expression) – it is a sequence of characters that define search pattern. This definition might be hard for you, but it is easy. I will not go into advanced regex, because that is hard to understand, I will show you some methods to replace characters or add them to get pure new combolist. You will need a user:pass or e-mail:pass combo and EmEditor. Open your combolist with EmEditor and press Ctrl + F. Make sure you have checked *Use Regular Expressions* box. In find field type *[.]\*$* then press *Select All* button. Click on the main window and as you can see your cursor position is on the end of every line. Now you can add characters to every line. I recommend you adding characters like ! . - \_, you can also add a random number on the end of every line. I remember that some of excellent League of Legends crackers were using this method to refresh their combos and they were getting HQ hits. Next method is about deleting some characters from your combo. For example, if you want to make a user:pass combo from e-mail:pass combo you have to use *@.\*:* regular expression, then move to the main window and just click : on your keyboard to replace the selected string with this delimiter. You can also remove selected characters like \_ or . from your combolist. It is simple, just replace it with nothing. Another thing is about deleting the numbers from nicknames. To do it use *.\*:* regex, then move to replace tab and in find field type *[0-9]*. Make sure that you have *In the Selection Only* box checked. You can do the same thing with a password, but personally, I do not recommend it. That is all about it. You can make different combinations of regex and try your methods. Maybe you will obtain something new, and you will be making money off it, who knows.

# RDP/VPS

Have you ever dreamed about cracking accounts 24/7? It is possible of course, and no, you don’t need to have your computer turned on 24/7. You can buy a RDP (remote desktop) or VPS (virtual private server) (I recommend you buying RPD if you are a rookie/newbie) which allows cracking and turn on your cracking software on it. By this way you won’t overload your own PC, so what is RDP/VPS. It’s like your virtual computer located somewhere on the world. Basically, someone gives you access to his computer/part of his computer (he creates your own account on it) and you can use it like a normal PC. You can buy RDP with admin access, so you will be able to configure almost everything on it, but RDP’s without it are much cheaper. Your RPD can be a dedicated machine, so no one except you will have access to it, or it can be a shared computer (you will have your own account, like other people using it). Remember that not every RDP/VPS provider allows cracking and SQLi Injection, so you will have to read their T.O.S. or something like “what is allowed”. I personally don’t recommend anything. You should do a research on cracking forms or in web about RDP’s and choose the best which fits to you. Why? Because if you want to (for example) crack hashes on it, you will need a very large disk space and a fast internet to download the wordlists. If you want to crack on it you will need a good CPU and about 8GB of RAM. As you can see it really depends on your own needs. Next thing – what you should install on your RDP? Well, it again depends on your needs. I am

100% sure that you will need basic things on it (if they’re not preinstalled) like a web browser, advanced text editors and other basic things. You won’t need a VPN (if you don’t have admin rights), because you are not using your own computer with your IP, so don’t worry. Sometimes if you have a admin access you can change IP with VPN, but if you don’t have it, don’t even bother to try. Your request will be blocked. If you don’t have enough funds, just don’t buy RDP. Start cracking on your own PC (of course, it’s risky) and gain enough money to buy the RDP.

# The end

Thank you for buying this guide. I hope that you learned a lot from it. If you have any questions, feel free to ask me on Discord. As you may know, this is the most advanced cracking-related e-book ever made, appreciate it. It is not excluded that it is the last version of this e-book. We will see. If you like it, please leave an honest vouch under forum’s thread. It took me like five months to start writing (LMAO) it and about three weeks to combine everything into one e-book and gain additional information. If there will be any updates of this e-book, so it is necessary to join our fantastic community. I would like to thanks everyone that helped me with this e-book.

Regards, Owner.