

T.O.S.

- This is only for educational purposes!**
- You are responsible for all of your actions!**
- No leaking of this product, tools, or methods!**
- You will not do a refund!**

Table of contents

1. Preamblel
2. Anonymity
3. Targetting your IP-Range
4. Scanning IP-Range – Getting open RDPs
5. Generating Combofile
6. Cracking with DuBrute
7. How to protect the RDP after cracking
8. Useful links

1. Preamblel

I spent a long time looking for a working guide about RDP cracking, but was not able to find one. Since I invested so much of my time and tested many tools, ip ranges, and password lists, I decided to write a detailed guide about cracking RDPs. You won't need to buy cracked RDPs after you buy this! You will be able to provide yourself with your own cracked RDPs!

RDPs are the best choice for all blackhat, cracking, scanning, hacking, or warez activities. After cracking your first RDP you can also use it to scan and crack more RDPs.

2. Anonymity

Before even thinking about cracking RDPs, you need to be sure you are anonymous. Before scanning or cracking any IP-Ranges you should have a VPN to secure your network or use another private RDP or VPS. The IP address of every failed login will be logged on the target RDP server. So dont even try to crack RDPs using your home connection without any VPN.

Never forget - this is blackhat! Protect yourself and stay safe!

3. Targeting your IP range

For first we need to find a suitable IP range we want to scan for open RDP ports and try to crack them.

Usually you will be searching for RDPs from a specific country. There are several ways of finding the right IP range for your case. Let's say you want to crack RDPs from the United States (because they are usually very fast).

You can use the [Hurricane Electric Internet Services](#) to find IP address ranges by a specific ISP. For US RDPs you should search for some of the big companies like SoftLayer. See picture below for example.

| | | |
|---------------------------------|-----------------------------|---|
| 75.126.176.0/20 | SoftLayer Technologies Inc. |  |
| 75.126.160.0/20 | SoftLayer Technologies Inc. |  |
| 75.126.16.0/20 | SoftLayer Technologies Inc. |  |
| 75.126.144.0/20 | SoftLayer Technologies Inc. |  |
| 75.126.128.0/20 | SoftLayer Technologies Inc. |  |
| 75.126.112.0/20 | SoftLayer Technologies Inc. |  |

If you don't know any provider in the country you want to crack RDPs u can just scan the IP block from the country or google for some nice, big providers.

For finding major ip addresses by country I suggest you use one of the following sites:

https://www.countryipblocks.net/country_selection.php

<http://www.nirsoft.net/countryip/>

Both of the pages don't need any explanation. Just search for your country and you'll see the IP range. Let's say we use the Softlayer range 75.126.1.1-75.126.255.255 as an example.

4. Scanning IP Range

After finding one or more ip ranges we want to scan this ranges for open port using VNC scanner. I use VNC scanner because it's by far the fastest scanner to find open RDPs and it's really easy to use. In the file pack you got with this ebook, there is the VNC scanner with a GUI and a cmd-version. We will use the cmd-version in this ebook because it's the best way to run it on cracked RDPs.

- Open VNC scanner folder
- Right-click "start.bat", press edit

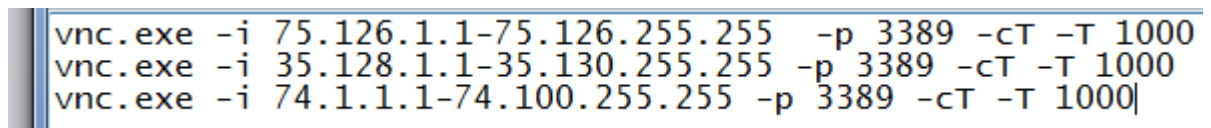
Example for our ip range:

```
vnc.exe -i 75.126.1.1-75.126.255.255 -p 3389 -cT -T 1000
```

Explanation:

```
vnc.exe -i FROM_IP-TO_IP -p 3389 -cT -T NUMBER_OF_THREADS
```

The color-marked numbers are the only details we need to change in the start.bat file. You will need to try out the best thread-setting for your internet connection. (It's usually 500-1000, try out what your connection can handle by increasing the number step-by-step.) To add more ranges you just need copy the line and change the range used. It will finish the first scan and start the second one after it. The following picture shows an example for a scan with 1000 threads and 3 different ranges.



```
vnc.exe -i 75.126.1.1-75.126.255.255 -p 3389 -cT -T 1000
vnc.exe -i 35.128.1.1-35.130.255.255 -p 3389 -cT -T 1000
vnc.exe -i 74.1.1.1-74.100.255.255 -p 3389 -cT -T 1000
```

To start a scan you just doubleclick the start.bat and a cmd window will appear showing the current status of the scan. It also tells you the remaining time for the current ip range so you can calculate how long the process will take.

The scan result (only the ip addresses with open rdp ports) is saved to a file "VNC_bypauth.txt" in the VNC scanner folder.

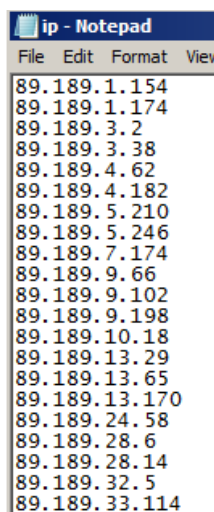
After getting some IP addresses (I suggest to use 3000 or more IP addresses for a crack session overnight) we need to change the format it was saved in.

```
COMMAND: vnc.exe -i 89.189.1.1-89.255.255.255 -p 3389 -cT -T 500
89.189.1.154 :3389
89.189.1.174 :3389
89.189.3.2 :3389
89.189.3.38 :3389
89.189.4.62 :3389
89.189.4.182 :3389
89.189.5.210 :3389
89.189.5.246 :3389
89.189.7.174 :3389
89.189.9.66 :3389
89.189.9.102 :3389
89.189.9.198 :3389
89.189.10.18 :3389
89.189.13.29 :3389
89.189.13.65 :3389
89.189.13.170 :3389
89.189.24.58 :3389
89.189.28.6 :3389
89.189.28.14 :3389
89.189.32.5 :3389
89.189.33.114 :3389
```

We need to get rid of the :3389 at the end of every line and also the extra spaces.

I use www.textmechanic.com to do this. But there are many similar tools out there that you can use to remove the unneeded spaces and the text :3389.

Save the clean output into a file named "ip.txt" and copy it into the DuBrute Folder (overwrite the existing file). It should look like this:



```
ip - Notepad
File Edit Format View
89.189.1.154
89.189.1.174
89.189.3.2
89.189.3.38
89.189.4.62
89.189.4.182
89.189.5.210
89.189.5.246
89.189.7.174
89.189.9.66
89.189.9.102
89.189.9.198
89.189.10.18
89.189.13.29
89.189.13.65
89.189.13.170
89.189.24.58
89.189.28.6
89.189.28.14
89.189.32.5
89.189.33.114
```

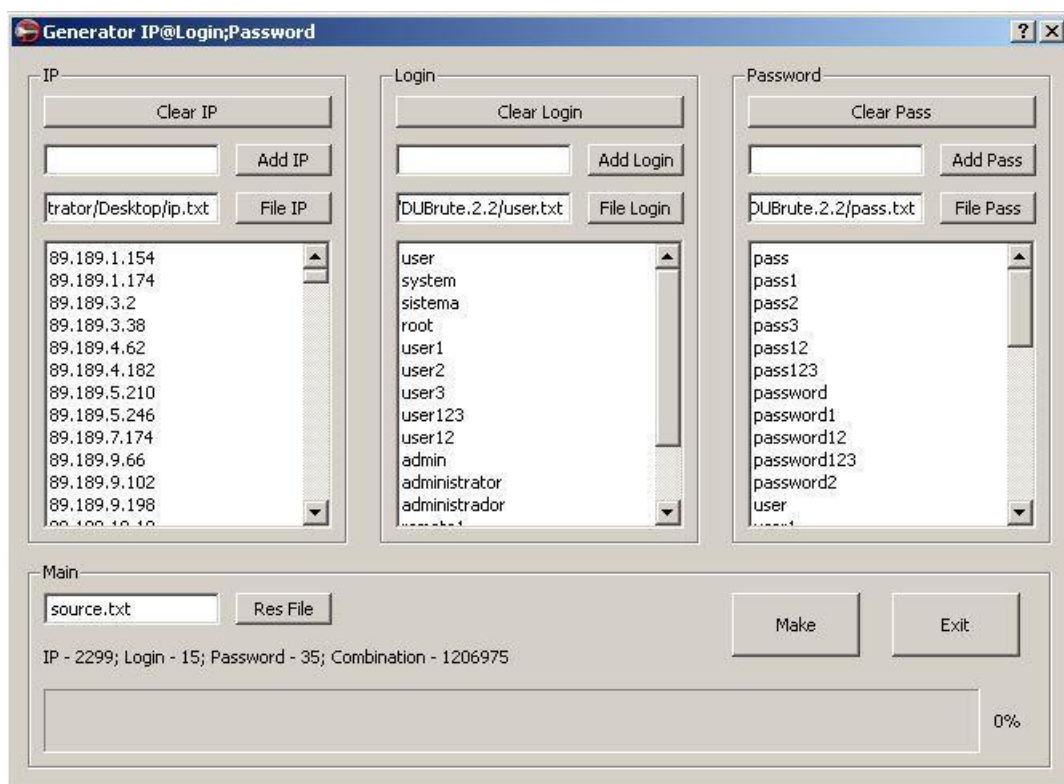
5. Generating Combo File for DuBrute

Before we can start to crack we need to generate a combo-file for DuBrute.

A combo file contains the ip-addresses we want to crack, the usernames we want to try, and all the passwords we want to try. It is very important to have nice password and user lists for the specific country! Different countries have different standard usernames and passwords!

Open DuBrute, click on "Generation".

- "File IP" loads the file with the IP addresses we scanned with VNC scanner
- File login loads our username list
- File password will load our password list.

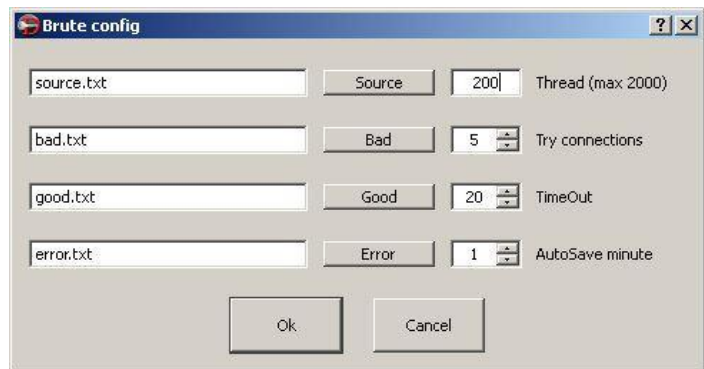


The number after Combination shows you how many combinations the combo file will consist of. After pressing "Make" we are finished with the preparation and now we can start to actually crack the RDPs. Move to step 6.

6. The cracking process

After we have prepared the combolist we can start cracking.

There is only one setting you need to adjust in DuBrute. It's the "threads". With a usual connection of ~10 Mbit up and down i could get nice cracking rates at 200 threads. You need to test it out for your specific connection. Usually something between 30-2000 should be OK.



7. Explanation of numbers in DuBrute

Source: IP addresses to crack

Bad: Tried IP addresses. No login found.

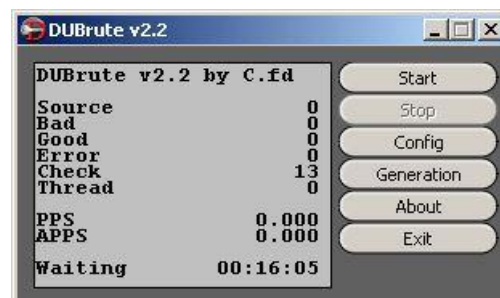
Good: Cracked RDPs

Error: Connection not possible

Check: Needs further check

PPS: Crack-tries per Second

APPS: Average Crack-tries over whole task



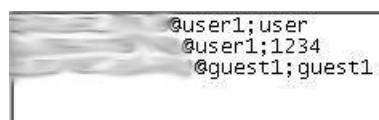
Now lean back and wait (or better go sleep, it takes some time).

All cracked accounts will be shown in the good.txt file in the DuBrute folder.

like: [192.168.1.1@Administrator;password](#)

You can just start connecting to them and checking them by using remotedesktop.

We are finished!



8. How to not burn your freshly cracked RDPs instantly

- Don't upload malicious software that is not FUD (scantime AND runtime!). A potentially AV will detect it and the owner could be informed. If he finds you he will kick you out.
- If u got an admin account, DON'T use the standard admin account! Make a new one for yourself and use it! By using this method u will not have a risk to connecting to the RDP with the same username while the owner is connected. Also if the owner connects, u can stay connected. He will not kick u out of the session automatically. Also yo don't change anything in his profile by using the other username.
- Don't use 90% or more of the server and network resources. The owner will search for the missing resources and find the root of evil. He will find you and "fix" the problem (by changing passwords, setting up better security).
- Don't install any software that is visible for all users. Try to get the software you need on the RDP als a PortableApp, so it will not be listed in the control panel. If u need urgently a software fully installed, install it in a different (hidden) location of your choice. Also don't install the application for all users.
- Don't uninstall any software. Also don't uninstall the AV. The owner will usually see it fast and handle the problem.
- When you need to use a browser for surfing use always your own portable browser, or use inprivate/private mode of the browser you use.
- Try to change as less as possible. More changes higher the risk of getting caught and the RDP will be lost.

9. Useful links

- <http://bgp.he.net> - IP ranges by country and ISP
- <http://www.nirsoft.net/countryip/> - IP ranges by country
- <https://www.countryipblocks.net/> - IP ranges by country
- <http://www.bmyers.com/public/1958.cfm> - 500 common bad passwords
- <http://mashable.com/2015/01/20/worst-passwords-of-2014/> - Worst passwords 2014
- <http://texttool.blogspot.de/> - Text tool for editing large lists (IP list)
- <http://www.textmechanic.co/> - alternative text tool
- <http://www.google.com> – Find more password and username combinations ☺

With this ebook you get a small user and password list to start. Password lists and usernames can be gathered from any cracking forums! I don't link them in this ebook cause I don't want to make ads for other forums then HF.

Just use Google and you will find for every country enough password and word lists to create your own, very much fitting password list. It's worth spending time on gathering and generating good password lists for your specific target. It will let u crack much more RDP's.

T.O.S.

- **This is only for educational purposes!**
- **You are responsible for all of your actions!**
- **No leaking of this product, tools, or methods!**
- **You will not do a refund!**