



# CYBER 2.0

CONFIG FILE GUIDE



## Table of contents

■ Description .....	3
■ Instructions .....	3
■ Flags .....	3
■ Server .....	3
■ Scramble ranges.....	4

## Description

This file allows us to configure the parameters and preferences of our security system.

- **“Instructions”** – the config file starts with instructions on how to read and write the file . Comments (#) are essential for a configuration file but they do not affect on how the file behaves. They are used for the developers to communicate behaviours and document important actions.

```
# Instructions
# -----
# 1. The '#' character is used for comments.
# 2. You can use comments everywhere in the file. The text after '#' won't be considered as a configuration.
# 3. Lines that are not comments shouldn't start with spaces, tabs and etc...
# 4. In Key=Value lines, don't put spaces or tabs between the key, the '=' sign and the value.
# 5. List items are separated by 'enter' only. Example:
#     [Example]
#     A
#     B
#     represents two values: "A" and "B".
#     [Example]
#     A B
#     represents one value: "A B".
```

- **Flags** – this section controls the options which are enabled and disabled in the system.

flags can be determined with **true** or **false** commands.

**offline\_mode** : can determine if the station works online with the server or offline without. (**True** = offline , **False** = online)

**ignore\_server\_whitelist** : with this configuration, you can decide if the whitelist is loaded manually and whether to ignore the server's sent whitelist or not. (**True** = ignore , **False** = don't ignore)

**Start\_scrambled** : determines if the station will start in scrambled mode. (True = scrambled , False = not scrambled)

```
[flags]
offline_mode=false # If true, works offline and doesn't communicate with the server.
ignore_server_whitelists=false # If true, ignores whitelists sent from the server and uses only manually loaded whitelists.
start_scrambled=false # If true, will start in scrambled mode.
```

- **Server** – this is the server's configuration part.

**“Host”** : this is the server's IP address.

**“server\_client\_communication\_protected\_mode”** : this can determine whether the client is protected by scrambling or unprotected by unscrambling. ( 0=Protected , 1=Unprotected ) in this case the client is unprotected, which means unscrambled.

**“server\_client\_communication\_table\_replacement\_time\_seconds”**

```
[server]
# server_client_communication_protected_mode:
# -----
# 0 - PROTECTED Scramble the server client communication.
# 1 - UNPROTECTED Unscramble the server client communication.
host=10.0.0.15
server_client_communication_protected_mode=1
server_client_communication_table_replacement_time_seconds=60 # Value limit 86400 (24 hours)
```

**“Table\_replacement\_time”**: **very important not to change any setting in this category**

```
[table_replacement_times]
table_replacement_time_seconds=1
table_overlap_time_seconds=1
```

**“DLLs\_check\_mode\_values”**: Default mode should be “=1”.

“0” means that the system is checking for DLL files, it is a high security setting.

“1” tells the system not to scan or check for DLLs at all.

“2” this mode checks for DLLs but does not scan them

## ■ Scramble Ranges

In this section you can define which ranges of the IP addresses will be scrambled, as mentioned in the description.

Instructions: this section guides you on how to configure the scramble of subnet masks, exclude or include IP addresses.

```
# Scramble Ranges
# -----
# Description:
#   Here you define which ranges of IPs will be scrambled.
# Instructions:
#   1. Define which subnets will be scrambled using lower-case x character ONLY in the last octets (10.x.0.0 will not work).
#      Examples:
#          10.0.0.x
#          10.0.x.x
#          10.x.x.x
#          x.x.x.x - Everything is scrambled.
#   2. Define the IPv4s, IPv6s and host names to be excluded from the subnets above (at this point, there is no meaning for excluded IPv6...).
#      You can use single IPs or IP ranges in format of x.x.x.y-z, where y iz the lowest part of the range and z is the highest (including).
#      Range can be defined according to the last octet only (10.0.1.1-2.2 and etc.. will not work).
#      Examples:
#          10.0.0.50-60
#          10.0.0.62
#   3. Define which IPs and names will be included.
#      Do this to:
#      a. Include IPs and names that are not in the range of the included subnets.
#      b. Include IPs that were excluded above.
#      See (2) for formatting.
#      Examples:
#          10.0.0.54-66
#          200.0.0.1
# Note: Due to the fact that 127.0.0.1, ::1 and localhost are not in the range of normal subnets, they will usually be excluded.
[scramble_range_subnets] # Current limit: 30.
10.0.0.x

[scramble_range_excluded_ipv4s] # Current limit: 50 singles and 30 ranges.
10.0.0.100
10.0.0.106
```

“Scramble\_range\_subnets”: the subnet mask that is scrambled.

“Scramble\_range\_excluded\_ipv4” : the IP addresses that are not going to be scrambled

“current limit” : the limit of the addresses that is allowed to be filled in.

```
[scramble_range_excluded_ipv6s] # Current limit: 10.
::1

[scramble_range_excluded_names] # Current limit: 10.

[scramble_range_included_ipv4s] # Current limit: 50 singles and 30 ranges.

[scramble_range_included_ipv6s] # Current limit: 10.

[scramble_range_included_names] # Current limit: 10.
```