General instructions for BUTCA CTFs

Please note: Any attacks or exploits you learn in CTFs during Cybersecurity courses are **illegal** to perform on any system that you do not own, according to Finnish law. In BUTCA, all the attacks (or data traffic) take place in a simulated environment.

However, exploit and information gathering tools you use in CTFs will not discriminate between your own systems and the internet. You do not have to intend to attack someone else's system for it to be a crime, **thus always make sure you are using the tools in the sandbox environment, to the sandbox addresses**. Usage of the knowledge you gain from the CTFs in the real world is at your own risk.

Sandbox

- Use sandbox environment for the CTF tasks. Open it with *Open sandbox* button. Sandbox will open to a new tab and you can do all the CTF tasks in there. You do not need to open the sandbox again; you can do all the tasks in the same sandbox.

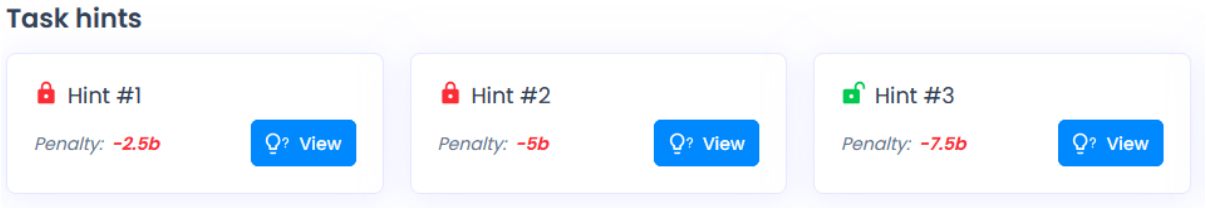
- If the sandbox connection is lost, or it **asks you to login**, use *Refresh connection* button to refresh the connection.
- In most CTFs, the Sandbox environment is Kali Linux. Your username usually is **kali** and password is **kali**. You are **not** logged in as a root user, so you need the password, for example, with `sudo` commands.

CTF tasks

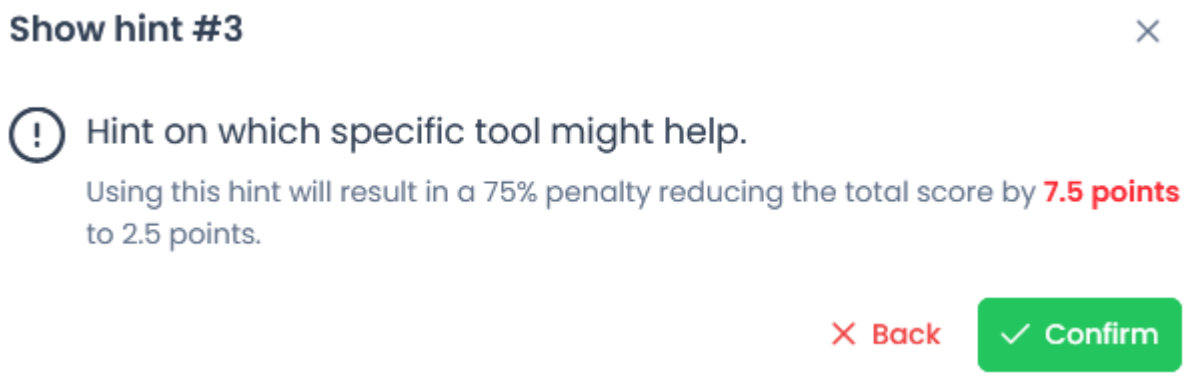
- Each task has its own FLAG as an answer; write it in the task solution and submit. The game proceeds after the correct flag is given. CTF flags can have different formats, such as FLAG(this is the flag), CTF{ThisIsTheFlag}, this is the flag. Follow the CTF's instructions about formatting.

- Some tasks have attachment(s) that can serve as supporting documents. **Use them!**
- You can also use various online tools or Google during tasks. Remember Linux man pages, for example, `man sudo`, or commands' help option, for example, `nmap -h`

- Use **Task hints** if you don't know how to proceed with the task.



Hints show in their description what the hint is about. Use *View* button to see the hint description. If you think the hint could be useful, *Confirm* the usage, this reveals the actual hint. Note that the usage of hints costs points. You can select only the hints that you think could help you. Just viewing the hint description does not cost points. In each task, there is one hint that reveals the correct flag.



- **Manage your time.** CTF playtime is usually around two hours, so do not spend too long on one task. You can see playtime top right of the screen.

Linux essentials

Navigating the filesystem, managing files/directories:

```
ls [OPTS] <PATH> # list files/directories; opts: -a all, -l
   ↪long, -h human-readable format
cd <PATH> # change directory (dir)
    ~ is equivalent to home dir
    / root dir
    .. one dir higher
    . current dir
    - previous dir
    * all files in the current dir
mkdir -p <PATH> # make directories defined in path
pwd  # print working directory
mv <SOURCE> <DEST> # move
cp [OPTS] <SOURCE> <DEST> # copy; opts: -r recursive
rm [OPTS] <PATH> # remove; opts: -rf recursive+force (for
   ↪directories)
find <PATH> -name <NAME> [-type d] # find file recursively in
   ↪ path (eq /), specify "type d" for searching dirs only
cat <FILE> # print the file
less <FILE> # open the file for reading; use "q" to exit
### searching in opened file ###
    /<PATTERN> # start searching forwards
        n  # move to the next matching pattern
        <SHIFT+N> # move to the previous matching pattern
        gg  # move to the beginning of file
        <SHIFT+G> # move to the end of file
```

Useful shell shortcuts:

```
<TAB+TAB> # automatic completion of command or PATH, list
   ↪options
<CTRL+R><PATTERN> # search in shell history
<UP> or <DOWN> # reuse commands from history
```

Users, shell:

```
su <USERNAME> # switch user (create new shell for different
   ↪user)
sudo <COMMAND> # execute command by root without creation of
   ↪new shell
whoami  # print current user
<CTRL+D> # Exit shell
```

Networking, file transfer/download:

```
ip a  # print all interfaces
ip route # print routes
netstat -pultn # print active network connections
ssh <USER>@<IP> # connect to the server via SSH
scp -pr <USER>@<IP>:<PATH> <LOCAL_PATH> # copy directories/
   ↪files from remote server to the local path
curl -O <URL> # download a file from Internet with given URL
```

Managing packages in Debian-based distributions:

```
apt-get update # update package repositories
apt-cache search <CMD> # search which packages provides
   ↪specified command
apt-get install [package] # install package
```

A package is a compressed file containing all the necessary components (binaries, libraries, configuration files and metadata) for software. It is designed for easy distribution, installation and management.

Edit a file:

```
nano <PATH> # open file using nano editor
    <CTRL+O> # save changes
    <CTRL+X> # exit file
    # follow the bottom panel for more shortcuts/instructions
    ^=<CTRL>; M=<ALT>
```

Redirections:

```
[CMD] > [FILE] # output of command to the file
[CMD] >> [FILE] # output of command to the end of file
echo "TEXT" >> test.txt # put TEXT at the end of text.txt
[CMD1] | [CMD2] # output of command1 to input of command2
ls -alh | less # example
```

Getting help:

```
man <PACKAGE> # show manual page
whatis <PACKAGE> # display one-line manual page descriptions
info  # all info in 1 file; press U to go 1 level UP, press L
   ↪ to return previous location
<PACKAGE> --help # short help in command line
whereis # find where a command binary (or manual) is located
```