

CYBER BLOCKZ

CEH Practical Lab — Find the Flags

FLAG FORMAT
CEH{...}

CHALLENGES
10 independent flags

🔪 You can submit these flags in any order in the course assignment section.

1

SCANNING

A custom port banner has flag scan the port properly to get the flag.

FLAG: _____

2

INFORMATION GATHERING — FTP

Find your second flag via ftp server.

FLAG: _____

3

INFORMATION GATHERING — WEB RECON

A web server is running on this host. Find the hidden directory that isn't linked anywhere on the site. Find it to get the flag.

FLAG: _____

4

ENCRYPTION & CRACKING — CIPHER

Download **notes.txt** from the web server's. Its contents are double encoded — decode it to reveal the flag.

FLAG: _____

5

ENCRYPTION & CRACKING — STEGANOGRAPHY

There's an **staff_portrait** image in the website that hides more than it shows. It's password protected — extract the hidden data to get the flag.

FLAG: _____

6

ENCRYPTION & CRACKING — HASH CRACKING

A leaked file in the web page contains a password hash. Crack it and submit the flag eg if you crack the hash and got password as password123 then submit as **CEH{password123}**.

FLAG: _____

7

ENCRYPTION & CRACKING — ZIP CRACKING

A password-protected ZIP in the downloads page holds a flag file inside. Crack the password and extract it.

FLAG: _____

8

INFORMATION GATHERING — METADATA / OSINT

A image file in the web page contains more than meets the eye. Inspect it more to find the flag.

FLAG: _____

9

VULNERABILITY RESEARCH

find the vulnerable server which has a rce vulnerability and submit it version as the flag eg: software is log4shell 4.3.10 then submit flag as **CEH{4.3.10}**

FLAG: _____

10

EXPLOITATION

Use the above vulnerable server to get access to system and find out the flag in **/home/ctfuser/user.txt**

FLAG: _____