

How to to access bandit

bandit1

Notes:

* Special characters in Unix: <http://tldp.org/LDP/abs/html/special-chars.html>
* To exit to the prompt type: exit

Level 0 → Level 1

Pass: boJ9jbbUNNfktd78OOpsqOltutMc3MY1

Notes: cat is to open a file with a name. Ex: cat readme

Level 1 → Level 2:

Pass: CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

Notes: cat can open - file. Ex: cat <-

Command (cat) can create a text file and to EXIT it press Ctrl+C

Level 2 → Level 3

Pass: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

Notes: to open a file with spaces between them with command (cat).

Ex: File name: spaces in this file name

Type in: cat spaces\ in\ this\ file\name

Level 3 → Level 4

Pass: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

ApIwrPrtPN36QITSp3EQaw936yaFoFgAB

Notes: Command (ls) is to list files in a directory. Command (ls -a) is to list hidden files

To open hidden file, type less filename. Ex: less . .. .hidden

Level 4 → Level 5

Pass: koReBOKuIDDepwhWk7jZC0RTdopnAYKh

Notes: same for file name with – Example: type cat <-file00 to view the file

Level 5 → Level 6

Pass: DXjZPULLxYr17uwoI01bNLQbtFemEgo7

Notes: command (find) Options:

-exec CMD: The file being searched which meets the above criteria and returns 0 for as its exit status for successful command execution.

-ok CMD : It works same as -exec except the user is prompted first.

-inum N : Search for files with inode number ‘N’.

-links N : Search for files with ‘N’ links.

-name demo : Search for files that are specified by ‘demo’.

-newer file : Search for files that were modified/created after ‘file’.

-perm octal : Search for the file if permission is ‘octal’.

-print : Display the path name of the files found by using the rest of the criteria.

-empty : Search for empty files and directories.

-size +N/-N : Search for files of ‘N’ blocks; ‘N’ followed by ‘c’can be used to measure size in characters; ‘+N’ means size > ‘N’ blocks and ‘-N’ means size < 'N' blocks.

-user name : Search for files owned by user name or ID ‘name’.

\(expr \) : True if ‘expr’ is true; used for grouping criteria combined with OR or AND.

! expr : True if ‘expr’ is false.

If want to open a file with a location after using find. Ex: cat ~/inhere/maybeinhere07/.file2

Level 6 → Level 7

Pass: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

Notes: the dot (.) = everything. Ex: find . -user bandit7 -group bandit6 -size 33c

That find command means find everything that belongs to the user of the group with the size of 33c because (.) means every thing

When listing file 2>/dev/null will eliminate all the file with denied permission

Level 7 → Level 8

Pass: cvX2JJa4CFALtqS87jk27qwqGhBM9plV

Notes: command (grep) options:

**-c** : This prints only a count of the lines that match a pattern

**-h :** Display the matched lines, but do not display the filenames.

**-i :** Ignores, case for matching

**-l :** Displays list of a filenames only.

**-n :** Display the matched lines and their line numbers.

**-v :** This prints out all the lines that do not matches the pattern

**-e exp :** Specifies expression with this option. Can use multiple times.

**-f file :** Takes patterns from file, one per line.

**-E :** Treats pattern as an extended regular expression (ERE)

**-w :** Match whole word

**-o :** Print only the matched parts of a matching line,

with each such part on a separate output line.

Ex: **$grep -i "UNix" geekfile.txt**

Output: unix is great os. unix is opensource. unix is free os.

Unix linux which one you choose.

uNix is easy to learn.unix is a multiuser os.Learn unix .unix is a powerful.

Level 8 → Level 9

Pass: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

Notes: command(sort) will sort the file

Command(uniq) will reports or filters out the repeated lines in a file. Options:

-c – -count : It tells how many times a line was repeated by displaying a number as a prefix with the line.

-d – -repeated : It only prints the repeated lines and not the lines which aren’t repeated.

-D – -all-repeated[=METHOD] : It prints all duplicate lines and METHOD can be any of the following:

none : Do not delimit duplicate lines at all. This is the default.

prepend : Insert a blank line before each set of duplicated lines.

separate : Insert a blank line between each set of duplicated lines.

-f N – -skip-fields(N) : It allows you to skip N fields(a field is a group of characters, delimited by whitespace) of a line before determining uniqueness of a line.

-i – -ignore case : By default, comparisons done are case sensitive but with this option case insensitive comparisons can be made.

-s N – -skip-chars(N) : It doesn’t compares the first N characters of each line while determining uniqueness. This is like the -f option, but it skips individual characters rather than fields.

-u – -unique : It allows you to print only unique lines.

-z – -zero-terminated : It will make a line end with 0 byte(NULL), instead of a newline.

-w N – -check-chars(N) : It only compares N characters in a line.

– – help : It displays a help message and exit.

– – version : It displays version information and exit.

Level 9 → Level 10

Pass: truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

Notes: command (strings) prints the strings of printable characters in files or readable for humans with a binary file

Level 10 → Level 11

Pass: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

Notes: [Base64 on Wikipedia](http://en.wikipedia.org/wiki/Base64)

Base64 is a group of [binary-to-text encoding](https://en.wikipedia.org/wiki/Binary-to-text_encoding) schemes that represent [binary data](https://en.wikipedia.org/wiki/Binary_data) in an [ASCII](https://en.wikipedia.org/wiki/ASCII) string format by translating it into a [radix](https://en.wikipedia.org/wiki/Radix)-64 representation. The term Base64 originates from a specific [MIME content transfer encoding](https://en.wikipedia.org/wiki/MIME#Content-Transfer-Encoding). Each Base64 digit represents exactly 6 bits of data. Three 8-bit bytes (i.e., a total of 24 bits) can therefore be represented by four 6-bit Base64 digits.

Common to all binary-to-text encoding schemes, Base64 is designed to carry data stored in binary formats across channels that only reliably support text content. Base64 is particularly prevalent on the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web)[[1]](https://en.wikipedia.org/wiki/Base64#cite_note-1) where its uses include the ability to embed [image files](https://en.wikipedia.org/wiki/Image_files) or other binary assets inside textual assets such as [HTML](https://en.wikipedia.org/wiki/HTML) and [CSS](https://en.wikipedia.org/wiki/CSS) files.

Base64 is also a command in Unix/Linux. There are a few options for it, yet this challenge we only need to use –decode

Level 11 → Level 12

Pass: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

Notes: [Rot13 on Wikipedia](http://en.wikipedia.org/wiki/Rot13)

<https://www.geeksforgeeks.org/tr-command-in-unix-linux-with-examples/>

Level 12 → Level 13

Pass: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

Notes: hex dump files and how to unzip it

Level 13 → Level 14

Pass: 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

Notes: ssh -i ./sshkey.private bandit14@localhost is the command to switch to another section without asking the password.

ssh -i ./sshkey.private is the standard

bandit14@localhost is provided

Level 14 → Level 15

Pass: BfMYroe26WYalil77FoDi9qh59eK5xNr

Notes: the echo command is to talk back with the localhost

Command nc is to send raw data over a network connection

Ex: nc localhost 30000 localhost is us, but 30000 is the port number

Level 15 → Level 16

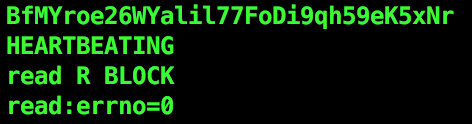
Pass: cluFn7wTiGryunymYOu4RcffSxQluehd

Notes: This time we need to connect through SSL(Secure Sockets Layer) which basically means encrypted communication. We need to use the openssl command.

openssl s\_client -ign\_eof -connect localhost:30001

Here s\_client implements a generic SSL/TLS client which can establish a transparent connection to a remote server speaking SSL/TLS. For more information use man s\_client. s\_server on the other hand implements a generic SSL/TLS server which accepts connections from remote clients speaking SSL/TLS(analogous to the nc -l <port\_number> command).

ign\_eof is to be used as mentioned in the description other wise we get this



What ign\_eof does is it prevents the server from closing down the connection when the end of file is reached in our input(when we press the enter key after submitting the password).

connect host:port specifies the host and optional port to connect to. If not specified then an attempt is made to connect to the local host on port 4433.

Note that -ign\_eof and -connect host:port flags are under man s\_clientand not man openssl.

Level 16 → Level 17

Pass: xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn