search Windows Feature On and Off

open Ubuntu and you will be prompted to set usernames and password

Install PuTTY too

An **SSH** (Secure Shell) client is a software application that enables a user to connect to a remote server securely over an encrypted communication channel. SSH is a protocol that provides a secure way to remotely access and manage network devices, servers, and systems. It is commonly used for remote command-line access, file transfers, and tunnelling network connections.

In the Bandit Wargrame, in level 0, you will see they have provided the IP address and the port name

**Level 0 :**

username - type bandit0 and

password - bandit0

**Level 1 :**

password - NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

**ls** - list files

**cat** - concatenate files and print on the standard output

**More** - writting contents of file

**ls** -a for hidden files

**Level 2 :**

cat "spaces in this filename" or cat spaces\ in\ this\ filename

password - rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi

**Level 3 :**

Ls

file filename

cat filename

Password - aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG

Level 4 :

*find . -type f -exec file {} \;*

Finds the file type recursively

Password – 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe

Level 5 :

cd inhere

ls

file \*

cat filename

Password – lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR

Level 6 :

find / -type f -size 33c -user bandit7 -group bandit6 2>/dev/null

find /: Starts the search from the root directory (/).

-type f: Searches for files.

-size 33c: Looks for files with a size of 33 bytes. Adjust the size based on the level description.

-user bandit7 -group bandit6: Filters files owned by user bandit7 and group bandit6.

2>/dev/null: Redirects errors to /dev/null to avoid displaying permission-denied errors.

cat /path/to/password\_file

Password – P4L4vucdmLnm8I7Vl7jG1ApGSfjYKqJU

Level 7 :

Use the grep command to filter out lines that contain the word "millionth":

grep "millionth" \*

Password – z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S

Level 8 :

cat data.txt

cat data.txt | grep millionth

Password – TESKZC0XvTetK0S9xNwm25STk5iWrBvP

Level 9 :

cat data.txt

cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

The tr command translates characters based on the ROT13 cipher. Running this command will decode the text from ROT13 to plain text.

Password – EN632PlfYiZbn3PhVK3XOGSlNInNE00t

Level 10 :

cat data.txt

Use the base64 command to decode the file's contents:

base64 -d data.txt

Password – G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s

Level 11 :

Locate and examine the data.txt file. This file contains the password encoded with Base64 multiple times.

base64 -d data.txt

The -d flag tells base64 to decode the file. Running this command will decode the contents of data.txt.

Repeat Base64 Decoding:

After decoding once, you might find that the output is still in Base64 format. If so, the password has been encoded multiple times.

Continue decoding until the output is no longer in Base64 format. You can use a loop in the terminal or script it based on the number of times you need to decode.

For example, to decode multiple times in the terminal:

bash

base64 -d data.txt | base64 -d | base64 -d | base64 -d | ...

Keep adding | base64 -d to the command until the output is human-readable or not in Base64 format.

Password – 6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM

Level 12 :

Locate and examine the data.txt file. This file contains the encoded data that needs to be decoded to retrieve the password.

xxd -r data.txt > decoded\_data (Use the xxd command to reverse the transformation (from hex to binary) of the file )

file decoded\_data

cat decoded\_data

Password – JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv

Level 13 :

use scp (Secure Copy) to transfer the password file from the Bandit server to your local machine.

Password – wbWdlBxEir4CaE8LaPhauuOo6pwRmrDw

Level 14 :

telnet localhost 30000

After executing the telnet command, the connection to the service on port 30000 will be established. The service might require some interaction or input.

Password – fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq

Level 15 :

Echo “fGrHPx402xGC7U7rXKDaxiWFTOiF0ENq” | nc localhost 30000

Password - jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt