DigiSuraksha Wargame internship Task

Team Members: 1. Durvaas More

2. Janvi Sonavale

3. Atul Prajapati

Leviathan Report

Level 0 → Level 1

Objective:

Analyze the check binary and find the hardcoded password.

Steps Followed:

1. Listed files in the home directory of leviathan0 and found the check binary.
2. Ran strings check to reveal readable strings inside the binary.
3. Found a hardcoded password.
4. Executed the binary with the found password
5. Got the password for leviathan1.

Level 1 → Level 2

Objective:

Use the printfile binary to access the password file for leviathan2.

Steps Followed: 1.

Found a binary named printfile.

2. Tried different file paths like /etc/passwd, etc.
3. Successfully ran: ./printfile /etc/leviathan_pass/leviathan2
4. Password was printed on the screen.

Level 2 → Level 3

Objective:

Bypass filename filtering using symbolic links.

Steps Followed:

1. printfile may restrict filenames.
2. Created a symlink: ln -s /etc/leviathan_pass/leviathan3 mylink
3. Ran: ./printfile mylink
4. Retrieved the password for leviathan3.

Level 3 → Level 4

Objective:

Find a 4-digit PIN to reveal the next password.

Steps Followed:

1. Ran the level3 binary — it asked for a 4-digit pin.
2. Used a brute-force loop: for i in {0000..9999}; do ./level3 $i; done
3. Found correct pin and received password in output.

Level 4 → Level 5

Objective:

Find and exploit a SUID binary.

Steps Followed:

1. Ran: f ind / -user leviathan4 -perm -4000 2>/dev/null
2. Located the binary and executed it.
3. It executed whoami or id, revealing useful environment or privilege info.
4. The binary gave access to the password for leviathan5.

Level 5 → Level 6

Objective:

Trace the binary to find how it compares input to a password.

Steps Followed:

1. Ran: ltrace ./leviathan5
2. Saw that it uses strcmp() to compare input with a hardcoded string.
3. Found the correct password in ltrace output or by trying strings found inside.

4. Logged in with password.

Level 6 → Level 7

Objective:

Use a binary that relies on environment or paths to run external commands.

Steps Followed:

1. Ran the binary — it attempted to execute a program like echo or ls.

2. Changed the $PATH environment to point to a custom script: echo "/bin/sh" > /tmp/echo chmod +x /tmp/echo export PATH=/tmp:$PATH ./leviathan6

3. Binary executed /tmp/echo which launched a shell as leviathan7.

4. Read the password from /etc/leviathan_pass/leviathan7.