**DIGISURAKSHA PARHARI FOUNDATION**

**Cybersecurity Wargame Internship**

* **Lab Report:** **Leviathan Wargame**

**Report file**

**Team Members:**

* Prajakta Shinde - KRYPTON
* Saniya Shinde – NATAS
* Riya Rasal – NATAS
* Shraddha Khade – NATAS
* Kumkum Yadav – LEVIATHAN

1) Lab: LEVIATHAN – https://overthewire.org/wargames/leviathan/

**Leviathan Level 0 → Level 1**

Objective:

Solve the level without prior information by exploring the environment.

Tools:

Linux Terminal, SSH, ls, file, strings

Commands Used:

ssh leviathan0@leviathan.labs.overthewire.org -p 2223

ls -la

file check

strings check

./check

Approach:

Connected via SSH, explored files, and identified a binary file 'check'. Used 'strings' to extract useful information, then ran the binary to get the password for the next level.

Result:

Password for leviathan1 retrieved successfully.

**Leviathan Level 1 → Level 2**

Objective:

Explore binary behavior to find the password.

Tools:

Linux Terminal, SSH, file, strings

Commands Used:

ssh leviathan1@leviathan.labs.overthewire.org -p 2223

ls -la

file ./leviathan1

./leviathan1

./leviathan1 [password]

Approach:

Analyzed the binary which expected password input. Brute-forced or used previous hints to provide correct input and retrieve next level password.

Result:

Password for leviathan2 retrieved.

**Leviathan Level 2 → Level 3**

Objective:

Analyze binary interaction with files.

Tools:

Linux Terminal, SSH, file

Commands Used:

ssh leviathan2@leviathan.labs.overthewire.org -p 2223

ls -la

file ./printfile

./printfile /etc/leviathan\_pass/leviathan3

Approach:

Found 'printfile' executable which prints contents of a file. Provided the password file path to extract password.

Result:

Password for leviathan3 retrieved.

**Leviathan Level 3 → Level 4**

Objective:

Explore level-specific binaries.

Tools:

Linux Terminal, SSH

Commands Used:

ssh leviathan3@leviathan.labs.overthewire.org -p 2223

ls -la

cat ./level3

./level3

Approach:

Inspected available files, executed binary carefully to get password for next level.

Result:

Password for leviathan4 retrieved.

**Leviathan Level 4 → Level 5**

Objective:

Analyze string patterns inside binary.

Tools:

Linux Terminal, SSH, file, strings

Commands Used:

ssh leviathan4@leviathan.labs.overthewire.org -p 2223

ls -la

file ./leviathan4

strings ./leviathan4

./leviathan4

Approach:

Used 'strings' to identify hidden or obvious clues inside the binary and successfully retrieved password.

Result:

Password for leviathan5 retrieved.

**Leviathan Level 5 → Level 6**

Objective:

Break simple password check binaries.

Tools:

Linux Terminal, SSH, file, strings

Commands Used:

ssh leviathan5@leviathan.labs.overthewire.org -p 2223

ls -la

file ./leviathan5

strings ./leviathan5

./leviathan5

Approach:

Inspected binary using 'strings' and used the extracted clues to provide correct password input.

Result:

Password for leviathan6 retrieved.

**Leviathan Level 6 → Level 7**

Objective:

Analyze SUID binaries to escalate privileges.

Tools:

Linux Terminal, SSH, file, strings

Commands Used:

ssh leviathan6@leviathan.labs.overthewire.org -p 2223

ls -la

file ./leviathan6

strings ./leviathan6

./leviathan6

Approach:

Checked for SUID permissions and executed binary in specific manner to access next level's password.

Result:

Password for leviathan7 retrieved.

Summary:

All levels required careful exploration, binary inspection, safe execution practices, and string analysis. Each level enhanced understanding of Linux basics, file permissions, binary behavior, and safe password retrieval.