

OverTheWire – Leviathan Lab Walkthrough (Levels 0–7)

Proof of Concept Report

Team Contributors

- Piyush Babele – 386
- Sristi Dutta – 387

This report documents the detailed step-by-step solutions of the OverTheWire Leviathan wargame (Levels 0–7). The lab was completed collaboratively by both team members, working together on each level from start to finish. As beginners, we often referred to online resources for guidance, especially to understand Linux commands, their functions, and practical usage. The report not only reflects our progress in solving the challenges but also highlights how teamwork, exploration, and external references helped us strengthen our foundation in Linux fundamentals, binary exploitation, and privilege escalation techniques.

Level 0

Username: leviathan0

Password: leviathan0

Port: ssh 2223

Host: leviathan.overthewire.org

Level 0 → Level 1

Tools Used: `ls`, `cat`, `grep`

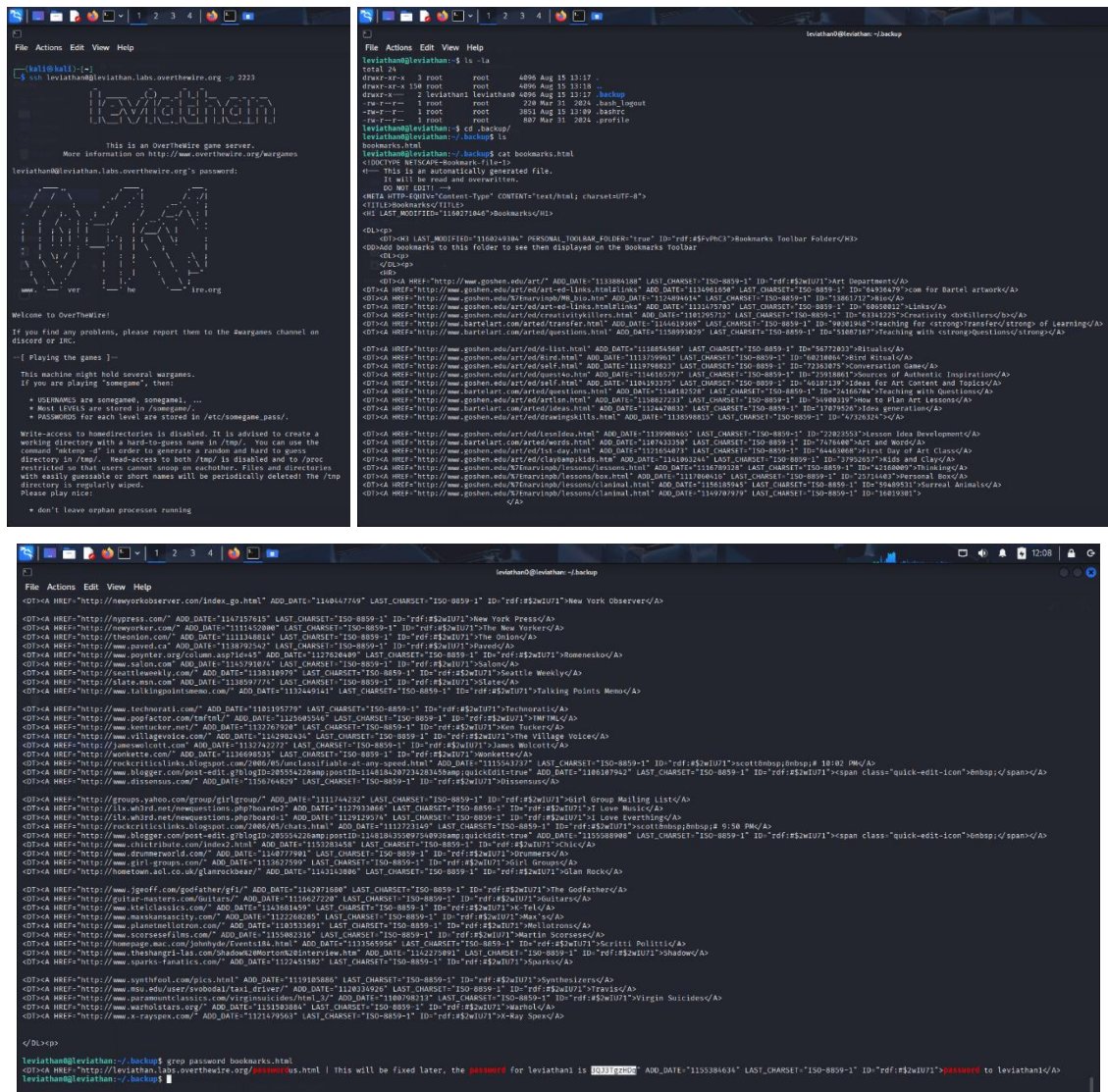
Objective: Extract password from backup HTML file.

Steps Followed:

1. Logged in as leviathan0 with default password.
2. Ran `ls -la` and found hidden `.backup` file.
3. Viewed contents with `cat bookmark.html`, which pointed to `bookmark.html`.
4. Searched for the keyword using `grep password bookmark.html`.
5. Retrieved the password for leviathan1.

Flag: 3QJ3TgzHDq

Conclusion: Learned to inspect hidden files and extract sensitive data from backups.



Level 1 → Level 2

Tools Used: `ltrace`, `./binary`

Objective: Analyze binary execution to uncover a hardcoded password.

Steps Followed:

1. Found a binary named `check`.
2. Running it without arguments asked for a password.
3. Executed with `ltrace ./check` to trace function calls.
4. Observed a `strcmp()` comparison with the string `sex`.
5. Ran `./check sex` and successfully obtained the password.

Flag: `NsN1HwFoyN`

Conclusion: Learned how to use `ltrace` to reveal hidden binary logic.

```
File Actions Edit View Help
--[ kali@kali:~ ]--
$ ssh leviathan@leviathan.labs.overthewire.org -p 2223

leviathan

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

leviathan@leviathan.labs.overthewire.org's password:

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the game ]--

This machine might hold several wargames.
If you are playing "somegame", then:
  * USERWORDS are somegame, somegame1, ...
  * Most LEVELS are stored in /somegame/.
  * PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:
  * don't leave orphan processes running
```

```
File Actions Edit View Help
--[ kali@kali:~ ]--
$ ssh leviathan@leviathan.labs.overthewire.org -p 2223

leviathan

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:
  * gef (https://github.com/hugsy/gef) in /opt/gef/
  * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
  * gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
  * pwntools (https://github.com/Gallopsled/pwntools)
  * radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

leviathan@leviathan:~$ ls -la
total 36
drwxr-xr-x  2 root  root   4096 Aug 15 13:17 .
drwxr-xr-x 150 root  root   4096 Aug 15 13:18 ..
-rw-r--r--  1 root  root    228 Mar 31 2024 .bash_logout
-rw-r--r--  1 root  root   3851 Aug 15 13:09 .bashrc
-rw-r--r--  1 leviathan leviathan1 1580 Aug 15 13:17 .bashrc
-rw-r--r--  1 root  root    807 Mar 31 2024 .profile
leviathan@leviathan:~$ ./check
-bash: ./check: no such file or directory
leviathan@leviathan:~$ ./check
password: null
Wrong password, Good Bye ...
leviathan@leviathan:~$ ltrace ./check
_libc_start_main@0x004080ed, 1, 0xfffff0d4, 0 unfinished ...>
printf@0, 0, 0x786573, 0x046f0: password: null
getchar@0, 0, 0x786573, 0x046f0:
getchar@0, 110, 0x786573, 0x046f0:
getchar@0, 0x7865, 0x786573, 0x046f0:
strcpy@0, 0, 0x786573, 0x046f0:
puts@0, 0, 0x786573, 0x046f0:
leviathan@leviathan:~$ ./check
password: sex
$ ls
check
$ cat /etc/leviathan_pass/leviathan2
null
leviathan@leviathan:~$
```

Level 2 → Level 3

Tools Used: ltrace, command injection

Objective: Exploit insecure command usage inside a binary.

Steps Followed:

1. Found the binary `printfile`.
2. Running with `/etc/leviathan_pass/leviathan3` returned “you can’t have that file.”
3. Using `ltrace`, discovered it calls the `cat` command.
4. Created a malicious filename `/tmp/file;bash` to inject commands.
5. Executed binary with this input, escalated privileges, and accessed `/etc/leviathan_pass/leviathan3`.

Flag: f0n8h2iWLP

Conclusion: Gained experience in exploiting command injection vulnerabilities.

```
File Actions Edit View Help
--[ kali@kali:~ ]--
$ ssh leviathan2@leviathan.labs.overthewire.org -p 2223

leviathan2

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

leviathan2@leviathan.labs.overthewire.org's password:

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the game ]--

This machine might hold several wargames.
If you are playing "somegame", then:
  * USERWORDS are somegame, somegame1, ...
  * Most LEVELS are stored in /somegame/.
  * PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:
  * don't leave orphan processes running
  * don't leave exploit-files laying around
```

```
File Actions Edit View Help
--[ kali@kali:~ ]--
$ ssh leviathan2@leviathan.labs.overthewire.org -p 2223

leviathan2

Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:
  * gef (https://github.com/hugsy/gef) in /opt/gef/
  * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
  * gdbinit (https://github.com/gdbinit/gdbinit) in /opt/gdbinit/
  * pwntools (https://github.com/Gallopsled/pwntools)
  * radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

leviathan2@leviathan2:~$ ls -la
total 36
drwxr-xr-x  2 root  root   4096 Aug 15 13:17 .
drwxr-xr-x 150 root  root   4096 Aug 15 13:18 ..
-rw-r--r--  1 root  root    228 Mar 31 2024 .bash_logout
-rw-r--r--  1 root  root   3851 Aug 15 13:09 .bashrc
-rw-r--r--  1 leviathan2 leviathan2 1582 Aug 15 13:17 .bashrc
-rw-r--r--  1 root  root    807 Mar 31 2024 .profile
leviathan2@leviathan2:~$ ./printfile
Usage: ./printfile filename
leviathan2@leviathan2:~$ ./printfile /etc/leviathan_pass/leviathan2
You can't have that file ...
leviathan2@leviathan2:~$ ./printfile /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
games:x:5:40:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lpr:x:7:7:lpr:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
_ftp:x:14:14:ftp:/var/ftp:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:List Manager:/usr/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/ircd:/usr/sbin/nologin
_apt:x:42:42:apt:/var/cache/apt:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
```



```
File Actions Edit View Help
[ kali@kali:~ ]
$ ssh leviathan@leviathan.labs.overthewire.org -p 2223

leviathan
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

leviathan@leviathan.labs.overthewire.org's password:
Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--
This machine might hold several wargames.
If you are playing "somegame", then:
  * USERNAMES are somegame1, somegame2, ...
  * Most LEVELS are stored in /somegame/.
  * PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and safe to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!
  * don't leave orphan processes running
```

```
File Actions Edit View Help
leviathan@leviathan:~$ ls -la
total 48
drwxr-xr-x  2 root root 4096 Aug 15 13:17 .
drwxr-xr-x 128 root root 4096 Aug 15 13:18 ..
-rw-r--r--  1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root root 3821 Aug 15 13:09 .bashrc
-rw-r--r--  1 leviathan leviathan 3180 Aug 15 13:11 .ssh
-rw-r--r--  1 root root 887 Mar 31 2024 .profile
leviathan@leviathan:~$ ./level3
Enter the password: hello
b2222222ap. WMOG:b2222222ap. WMOG
leviathan@leviathan:~$ ./level3
--libc_start_main@GLIBC_2.1.2--
streq("hello", "hello")
printf("Enter the password: ")
fgets(buf, 256, stdin)
strncpy(buf, "hello", 256)
puts(buf)
*** exited (status 0) ***
leviathan@leviathan:~$ ./level3
Enter the password: b2222222ap
[You've got shell!]
$ ls
level3
$ cat /etc/leviathan_pass/leviathan
WMOG:ICo
$ AC
$
```

Level 4 → Level 5

Tools Used: Hidden file inspection, ASCII conversion

Objective: Decode hidden binary file to extract password.

Steps Followed:

1. Logged in as leviathan4.
2. Searched directories and discovered a hidden `.trash` folder.
3. Found a binary file inside named `bin`.
4. Converted binary content to ASCII using online tools.
5. Extracted the password for leviathan5.

Flag: 0dyxT7F4QD

Conclusion: Learned how hidden binary files can store encoded secrets.

```
File Actions Edit View Help
[ kali@kali:~ ]
$ ssh leviathan@leviathan.labs.overthewire.org -p 2223

leviathan
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

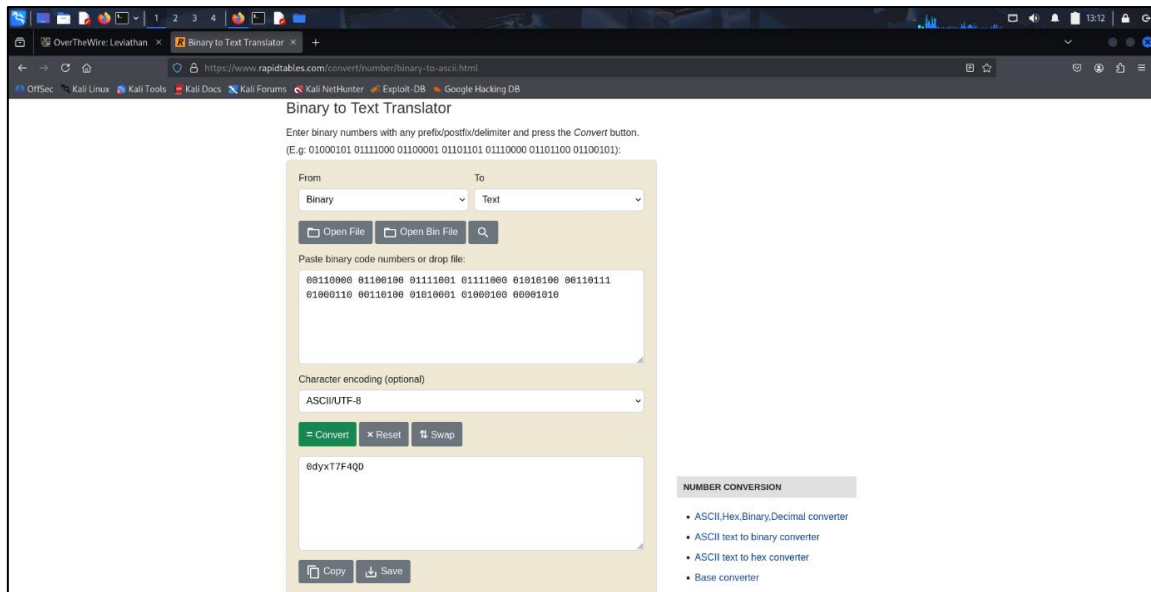
leviathan@leviathan.labs.overthewire.org's password:
Permission denied, please try again.
leviathan@leviathan.labs.overthewire.org's password:
Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--
This machine might hold several wargames.
If you are playing "somegame", then:
  * USERNAMES are somegame1, somegame2, ...
  * Most LEVELS are stored in /somegame/.
  * PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and safe to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice!
```

```
File Actions Edit View Help
leviathan@leviathan:~$ ls -la
total 24
drwxr-xr-x  3 root root 4096 Aug 15 13:17 .
drwxr-xr-x 128 root root 4096 Aug 15 13:18 ..
-rw-r--r--  1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root root 3821 Aug 15 13:09 .bashrc
-rw-r--r--  1 root root 887 Mar 31 2024 .profile
dr-xr-xr-x  2 root leviathan 4096 Aug 15 13:17 .trash
leviathan@leviathan:~$ cd .trash
leviathan@leviathan:~/trash$ ls
bin
leviathan@leviathan:~/trash$ ./bin
0010000 0100100 0111001 0111000 0101010 0100111 0100010 0011000 0101000 0100010 0000100
leviathan@leviathan:~/trash$
```



Level 5 → Level 6

Tools Used: `ln -s`, symbolic links

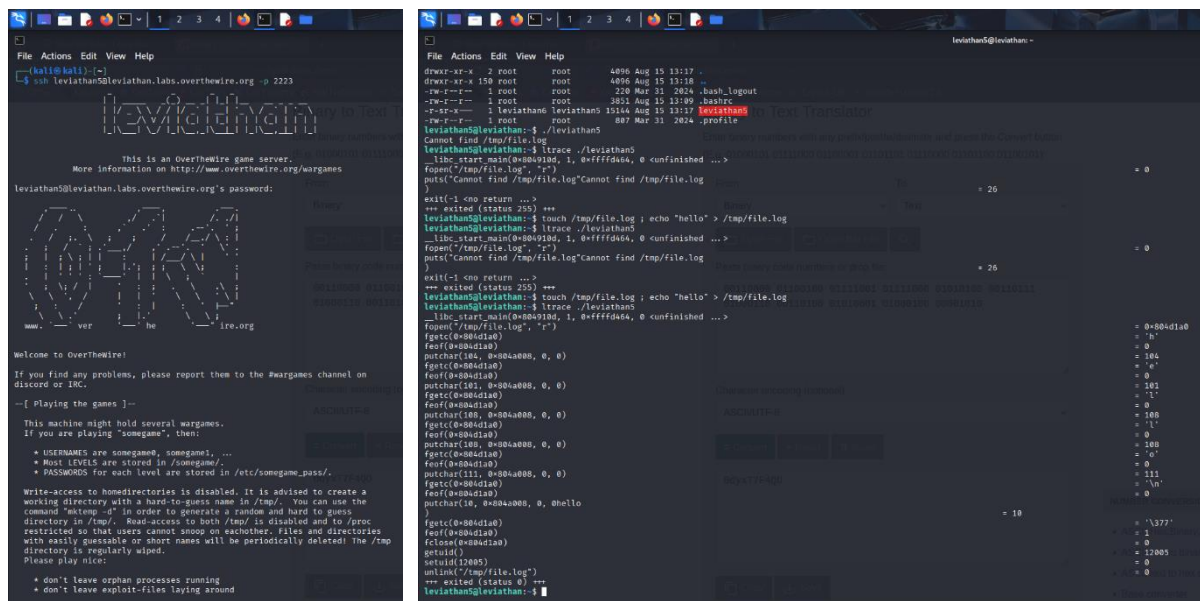
Objective: Exploit SUID binary with symlink trick.

Steps Followed:

1. Found a binary that attempted to use `/tmp/file.log`.
2. Created a symbolic link:
3. `ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log`
4. Ran the binary, which printed the contents of the password file.
5. Retrieved the password for leviathan6.

Flag: `szo7HDB88w`

Conclusion: Gained understanding of symlink attacks against SUID binaries.



Level 7 (Final)

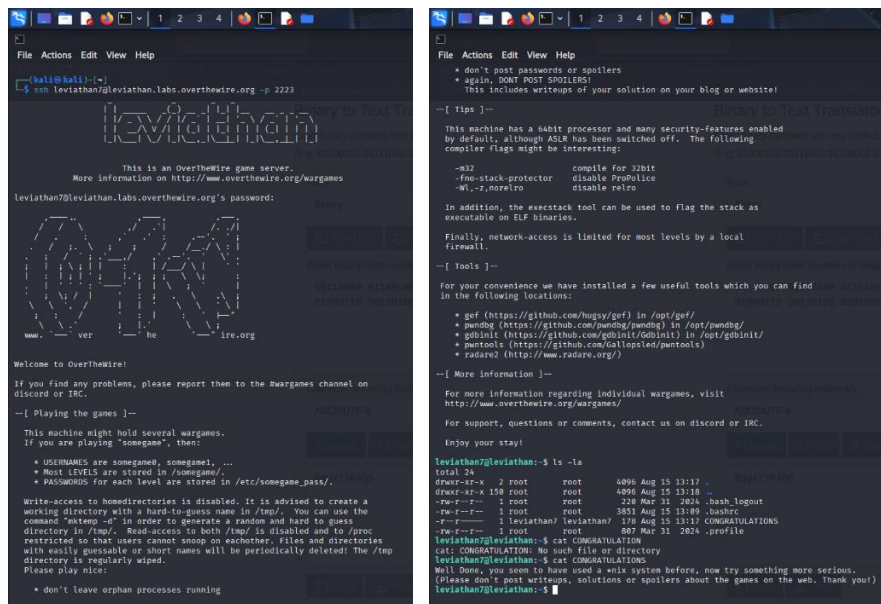
Tools Used: File inspection

Objective: Verify game completion.

Steps Followed:

1. Logged in as leviathan7.
2. No files were visible in the home directory.
3. Found and opened the file congratulations.
4. The file confirmed successful completion of Leviathan.

Conclusion: Completed all Leviathan levels successfully.



Summary Table

Level	Approach	Key Command / Method
0	Backup file inspection	<code>grep password bookmark.html</code>
1	Binary tracing with ltrace	<code>./check sex</code>
2	Command injection in filename	<code>/tmp/file;bash</code>
3	Hardcoded password via ltrace	<code>./level3 snlprintf</code>
4	Hidden binary decoding	ASCII conversion (using any site of conversion in website)
5	Symlink attack on temp file	<code>ln -s /etc/leviathan_pass/leviathan6 ...</code>
6	Brute-force PIN with loop	Bash brute force <code>for i in {0000..9999}; do echo \$i; ./leviathan6 \$i; done;</code>
7	Completion check	<code>cat CONGRATULATIONS</code>

Conclusion

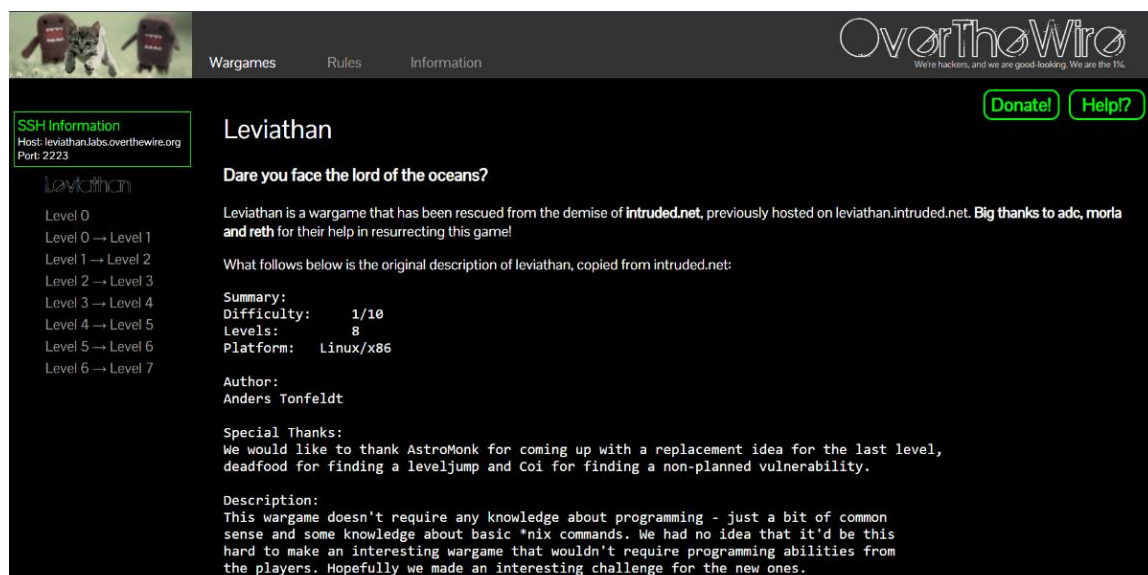
Through the successful completion of the OverTheWire Leviathan wargame (Levels 0–7), we gained valuable hands-on experience in Linux system navigation, privilege escalation, and binary exploitation. Each level introduced us to different aspects of cybersecurity problem-solving; from inspecting hidden files and analyzing binaries, to exploiting SUID programs, command injection, symbolic links, and brute-force techniques.

Working together as a team allowed us to share ideas, troubleshoot errors collaboratively, and develop a structured approach to solving challenges. As beginners, we enhanced our understanding of Linux commands and their practical applications with the help of online references, which further deepened our confidence in applying theoretical knowledge to real-world scenarios.

Learning Outcomes

- Improved proficiency in **basic Linux commands** and their functional uses.
- Practical exposure to **binary analysis tools** such as `ltrace`, `strings`, etc.
- Understanding of **command injection** and symlink exploitation.
- Hands-on practice with **SUID binaries** and privilege escalation.
- Developed skills in **automation and brute-force scripting** using Bash.
- Strengthened teamwork, research ability, and problem-solving mindset.

This project not only helped us clear the Leviathan lab but also built a solid foundation for advancing further in Capture The Flag (CTF) challenges and cybersecurity learning.



OverTheWire Website Interface