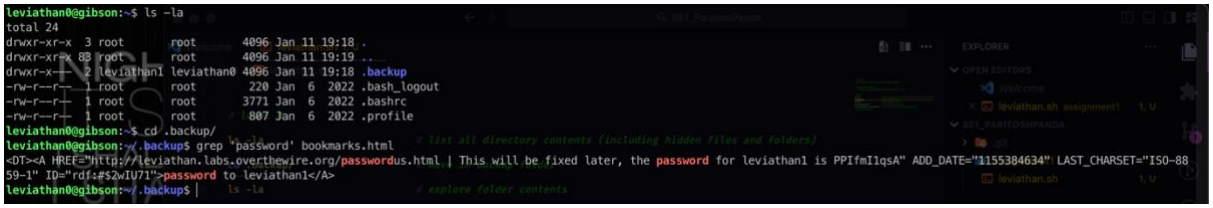
Wargame Leviathan: Report

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.

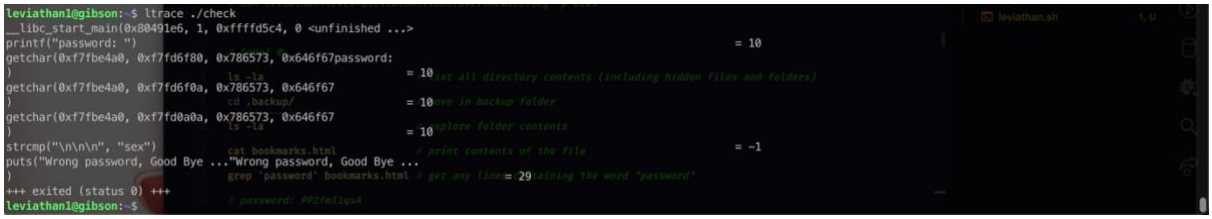


Level 1

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 “secrf” 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.



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*.

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.

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.

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.

Level 4

Checking the contents of the home directory, I saw there was a hidden *.trash* directory. Changing into that and seeing it's 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.

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.

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 $out"
fi
done
done
done
done
' > test.sh
leviathan6@gibson:/tmp/tmp.ZyCDrdH9nP$ ./test.sh


^Cleviathan6@gibson:/tmp/tmp.ZyCDrdH9nP$ ~/leviathan6 7123
$ cat /etc/leviathan_pass/leviathan7
8GpZ5f8Hze
$

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
-r--r----- 1 leviathan7 leviathan7 178 Jan 11 19:18 CONGRATULATIONS
-rw-r--r-- 1 root root 807 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:~$