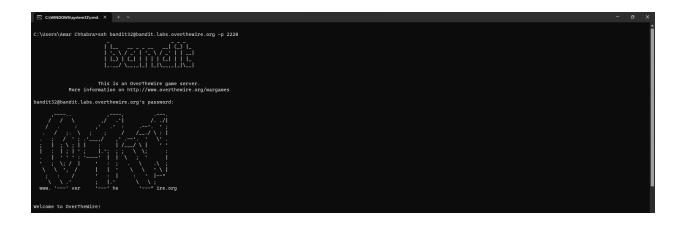
Bandit Level 32 -> Level 33

SSH Parameters			
Server:	bandit.labs.overthewire.org		
Port:	2220		

Website URLs				
Level 32—>33	OverTheWire: Bandit Level 32 → Level 33			
Level 33—>34	OverTheWire: Bandit Level 33 → Level 34			

Passwords				
Level	User Name	Password		
Level 32>33	bandit32	rmCBvG56y58BXzv98yZGdO7ATVL5dW8y		
Level 33>34	bandit33	odHo63fHiFqcWWJG9rLiLDtPm45KzUKy		





WELCOME TO THE UPPERCASE SHELL

Upon authentication, to Level 32, we are receive a message stating "WELCOME TO The UPPERCASE SHELL". Post input of command, "Is", an sh and the command [converted to upper case] is returned with permission denied. sh indicates the dash shell is invoked per the sh man page. The command is not being processed, and permission denied, because the script run converts it to uppercase before processing. Additionally, the command [LS] is proceeded by a 1. This indicates that the Is command is the second item processed by the script. The first item is the shell, denoted by the "sh" command, indicating positional parameters are being utilized.

Positional parameters are a special kind of variable. Rather than a variable that is identified inside the bash script, a positional parameter is specified when you run the script. In this case the positional parameter [Is] is preceded by the su command which invokes the script.

To invoke the first positional parameter in position 0, sh, we input key sequence \$0. This gets us command line/shell access. To verify identity we invoke the id && whoami commands. Next we execute the pwd and Is -la commands to view the contents of the bandit32 home directory for password related information.

We noted the usershell file is set user ID (SETUID) file. This is denoted by the third character [s] in the permissions of the uppershell file permissions. It enables the current user to execute files/commands as bandit33 [logged in as bandit32]. This is denoted in the ls -la file permissions for the uppershell file.

Per execution of Is -la, on the /etc/bandit_pass/bandit33, access is restricted to bandit33. We will be able to read this file, as bandit32, since the bandit32 user ID leverages the SUID permissions described above.

To get the Level 33 password we input the key sequence, "cat /etc/bandit_pass/bandit33" and the password is output.

```
C:\WINDOWS\system32\cmd. × + v
WELCOME TO THE UPPERCASE SHELL
sh: 1: LS: Permission denied
>>
>> $0
$
$ id && whoami
uid=11033(bandit33) gid=11032(bandit32) groups=11032(bandit32)
bandit33
$ pwd && ls -la
/home/bandit32
total 36
drwxr-xr-x 2 root
                              root
                                           4096 Apr 23 18:04 .
drwxr-xr-x 70 root
                              root
                                           4096 Apr 23 18:05 ..
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_logot
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
-rwsr-x--- 1 bandit33 bandit32 15128 Apr 23 18:04 uppershell
                                           220 Jan 6 2022 .bash_logout
3771 Jan 6 2022 .bashrc
807 Jan 6 2022 .profile
$ ls -la /etc/bandit_pass/bandit33
     ------ 1 bandit33 bandit33 33 Apr 23 18:04 /etc/bandit_pass/bandit33
$ cat /etc/bandit_pass/bandit33
odHo63fHiFqcWWJG9rLiLDtPm45KzUKy
```

Level 33 —> Level 34 Password

odHo63fHiFqcWWJG9rLiLDtPm45KzUKy