

Sri Lanka Institute of Information technology

2024

System and Networking programming

Lab sheet 01

Year 2, Semester



IT23400368

MMM ARKAM

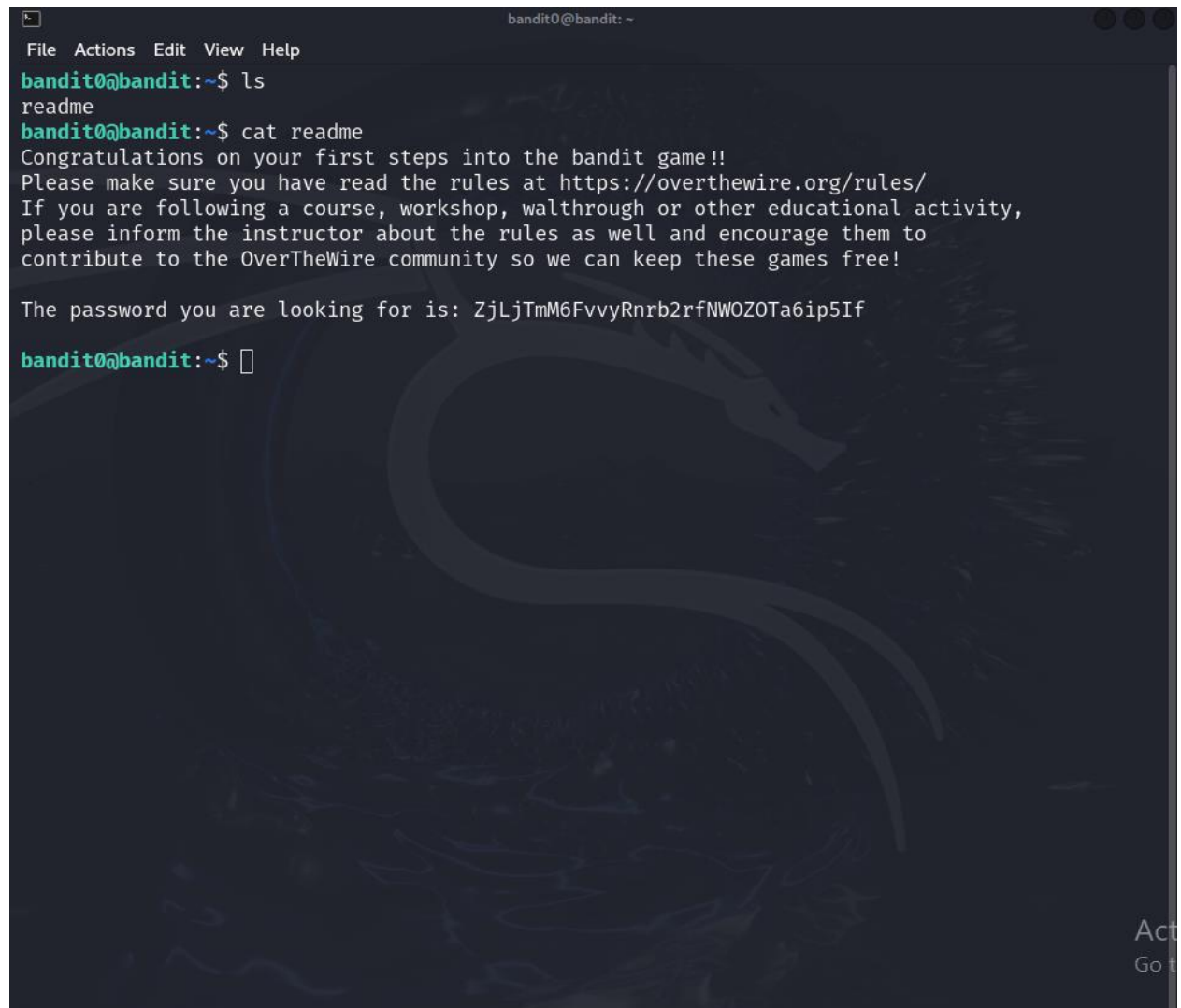
Y2.S1.WD.CS.01.01

MALABE CAMPUS

Introduction.

In this assignment, you'll find a detailed journey through Bandit levels 0 to 20. I've included screenshots and simple explanations for each level, showing how each task was completed. This guide highlights the steps and commands used to solve the challenges, making it easy to understand the problem-solving process at every stage.

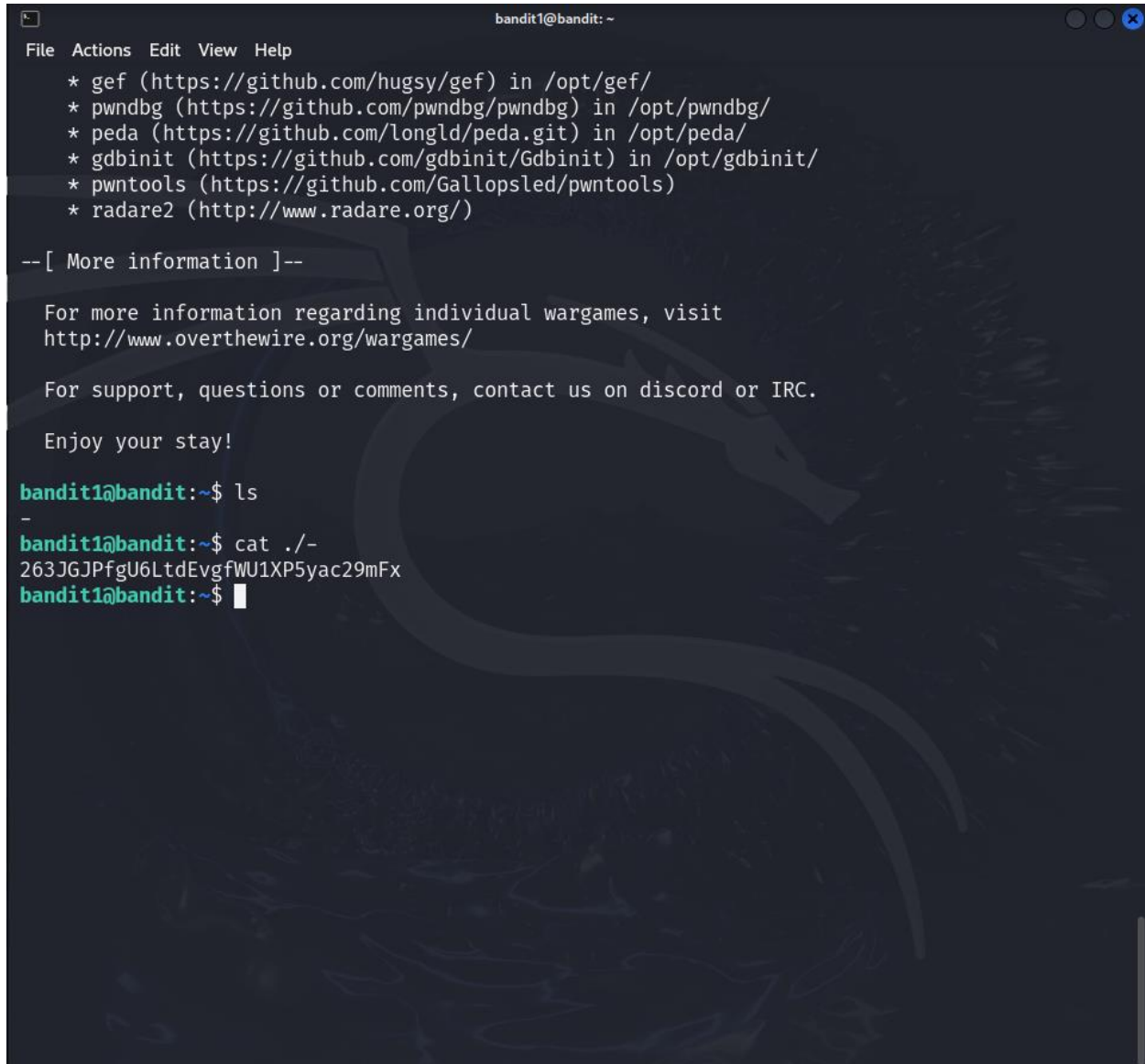
Level 0 - 1

A terminal window titled 'bandit0@bandit: ~' with a menu bar (File, Actions, Edit, View, Help). The user runs 'ls' and sees 'readme'. Then they run 'cat readme' and see a welcome message and a password. The background has a faint dragon watermark.

```
bandit0@bandit: ~  
File Actions Edit View Help  
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: ZjLjTmM6FvvYRnrb2rfNW0Z0Ta6ip5If  
bandit0@bandit:~$
```

Note: using **cat** command to read the file.

Level 1 - 2

A screenshot of a terminal window titled 'bandit1@bandit: ~'. The terminal shows a list of tools to be installed: gef, pwndbg, peda, gdbinit, pwntools, and radare2, each with its source URL and installation path. Below this, there is a section for more information, including a link to 'http://www.overthewire.org/wargames/' and contact information for support. The user then runs 'ls' and 'cat ./-' commands, which output a long alphanumeric string: '263JGJPfgU6LtdEvgfWU1XP5yac29mFx'.

```
bandit1@bandit: ~
File Actions Edit View Help
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* 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.

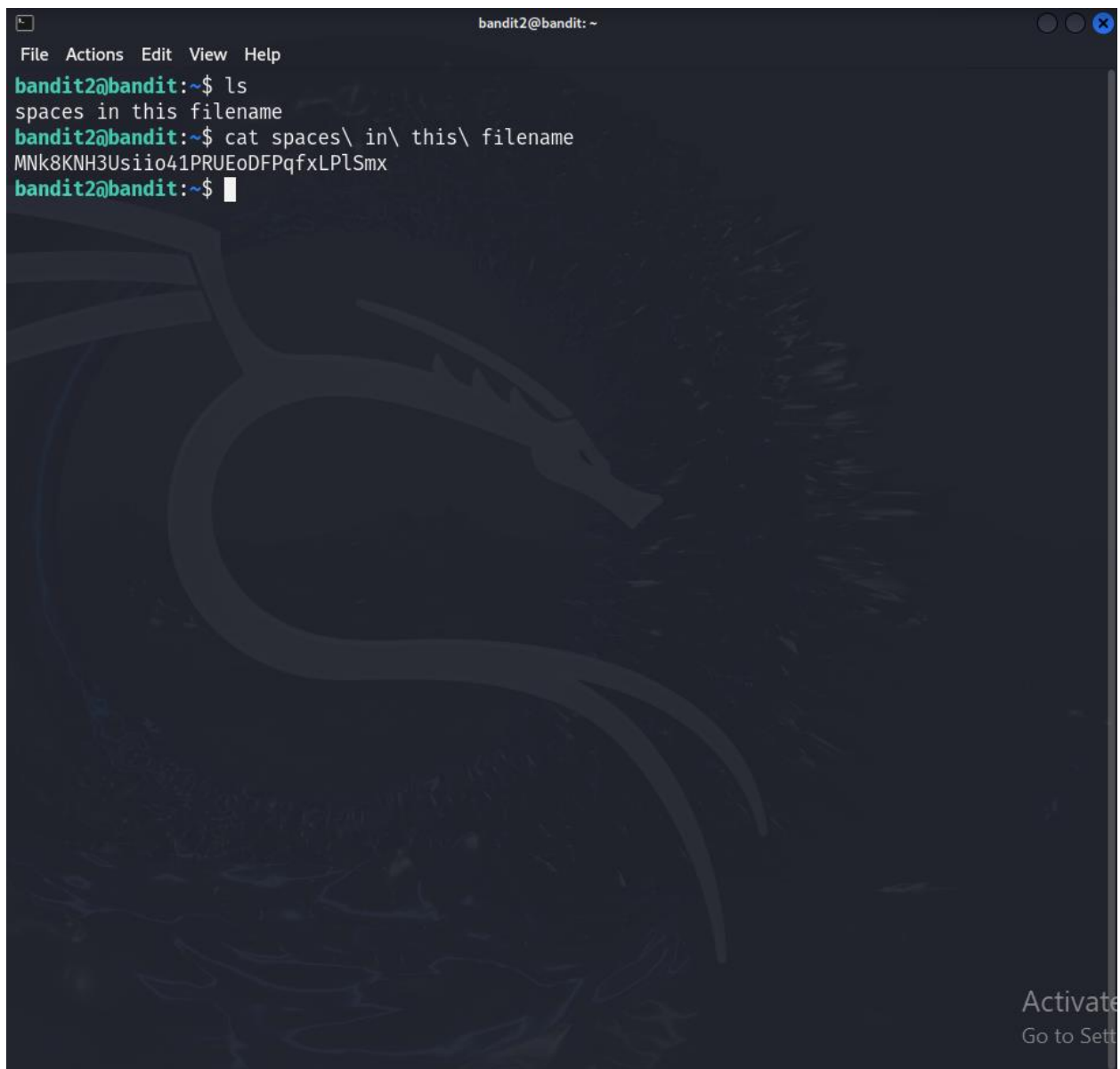
Enjoy your stay!

bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
bandit1@bandit:~$
```

Note:

Using the command **cat -** does not return anything. So, we add the path and write (**cat ./-**) .

Level 2 - 3

A terminal window titled 'bandit2@bandit: ~' with a menu bar (File, Actions, Edit, View, Help) and a dark background featuring a faint dragon illustration. The terminal shows the following commands and output:

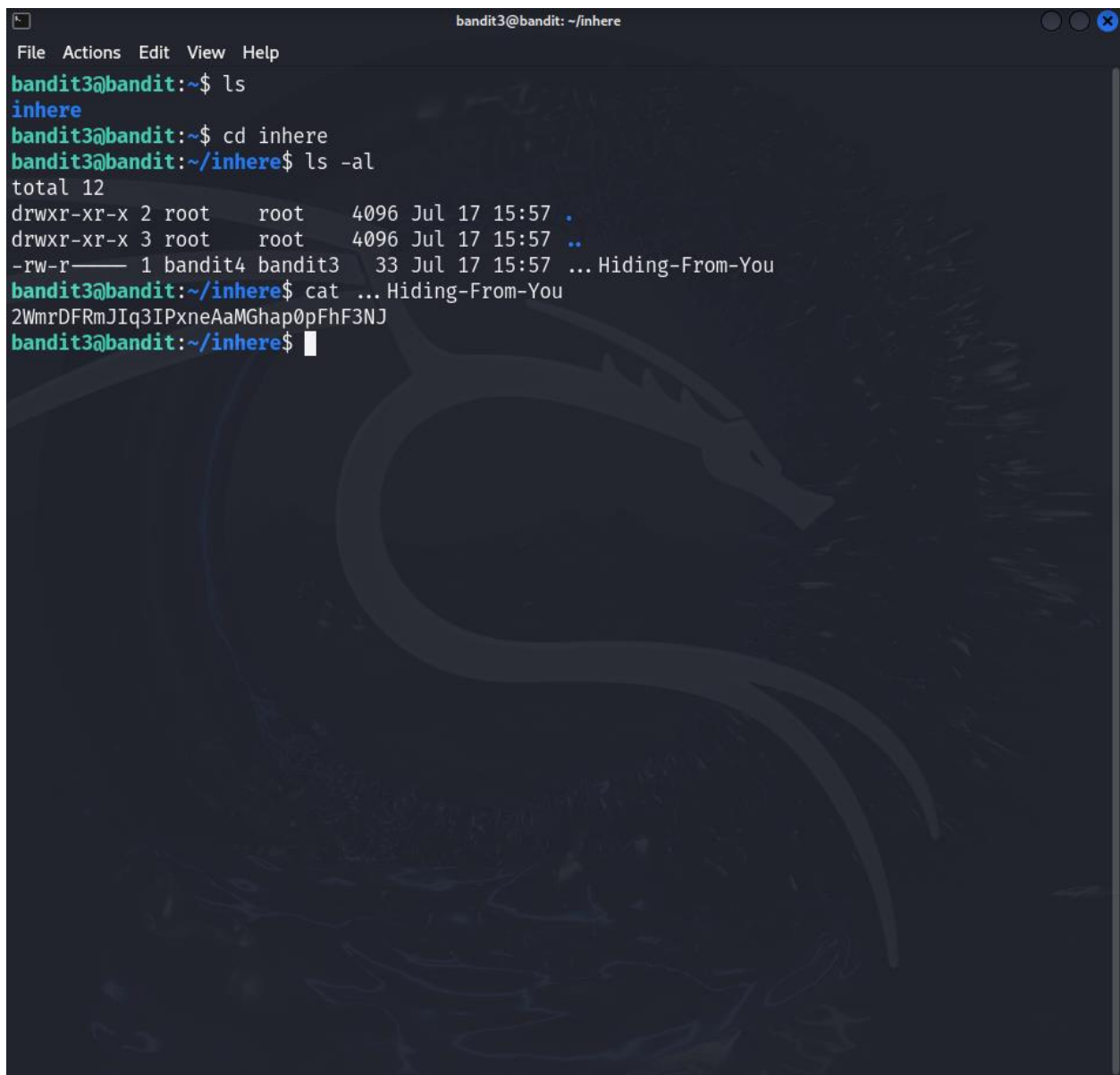
```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
bandit2@bandit:~$
```

Note:

Using \ for each space to indicate that all of it belongs to one file.

Backslash is an escape.

Level 3 - 4



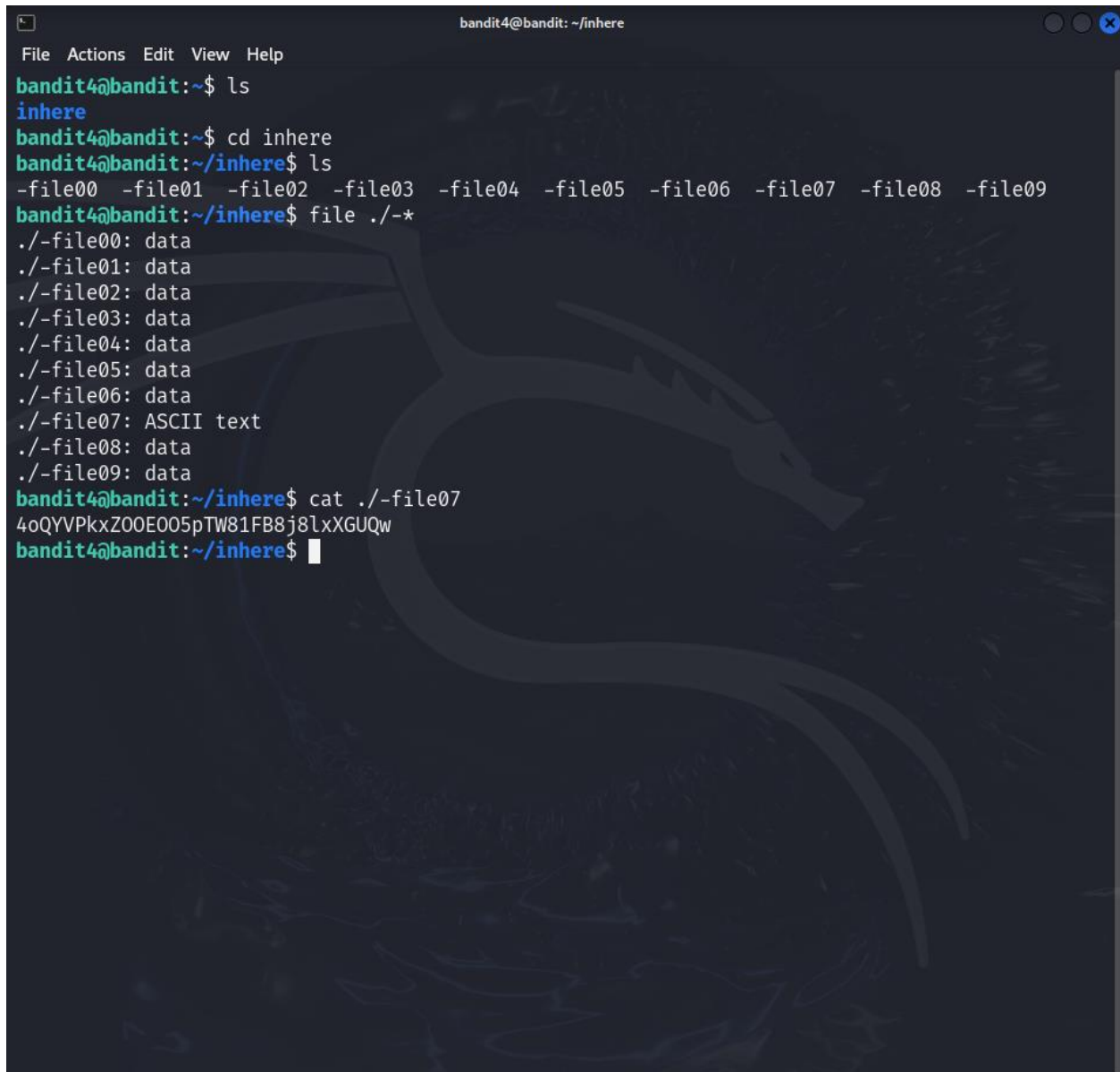
```
bandit3@bandit: ~/inhere
File Actions Edit View Help
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Jul 17 15:57 .
drwxr-xr-x 3 root root 4096 Jul 17 15:57 ..
-rw-r----- 1 bandit4 bandit3 33 Jul 17 15:57 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$
```

Note:

Using **-al** option for **ls** command. It shows all the hidden files.

After finding the file read it with **cat** command.

Level 4 - 5

A terminal window titled 'bandit4@bandit: ~/inhere' with a menu bar (File, Actions, Edit, View, Help). The user runs 'ls' in the home directory, then 'cd inhere'. In the 'inhere' directory, 'ls' shows files '-file00' through '-file09'. The user then runs 'file ./-*', which lists the file types: data for files 00-06 and 08-09, and ASCII text for file 07. Finally, the user runs 'cat ./-file07', displaying the alphanumeric string '4oQYVPkxZ00E005pTW81FB8j8lxXGUQw'.

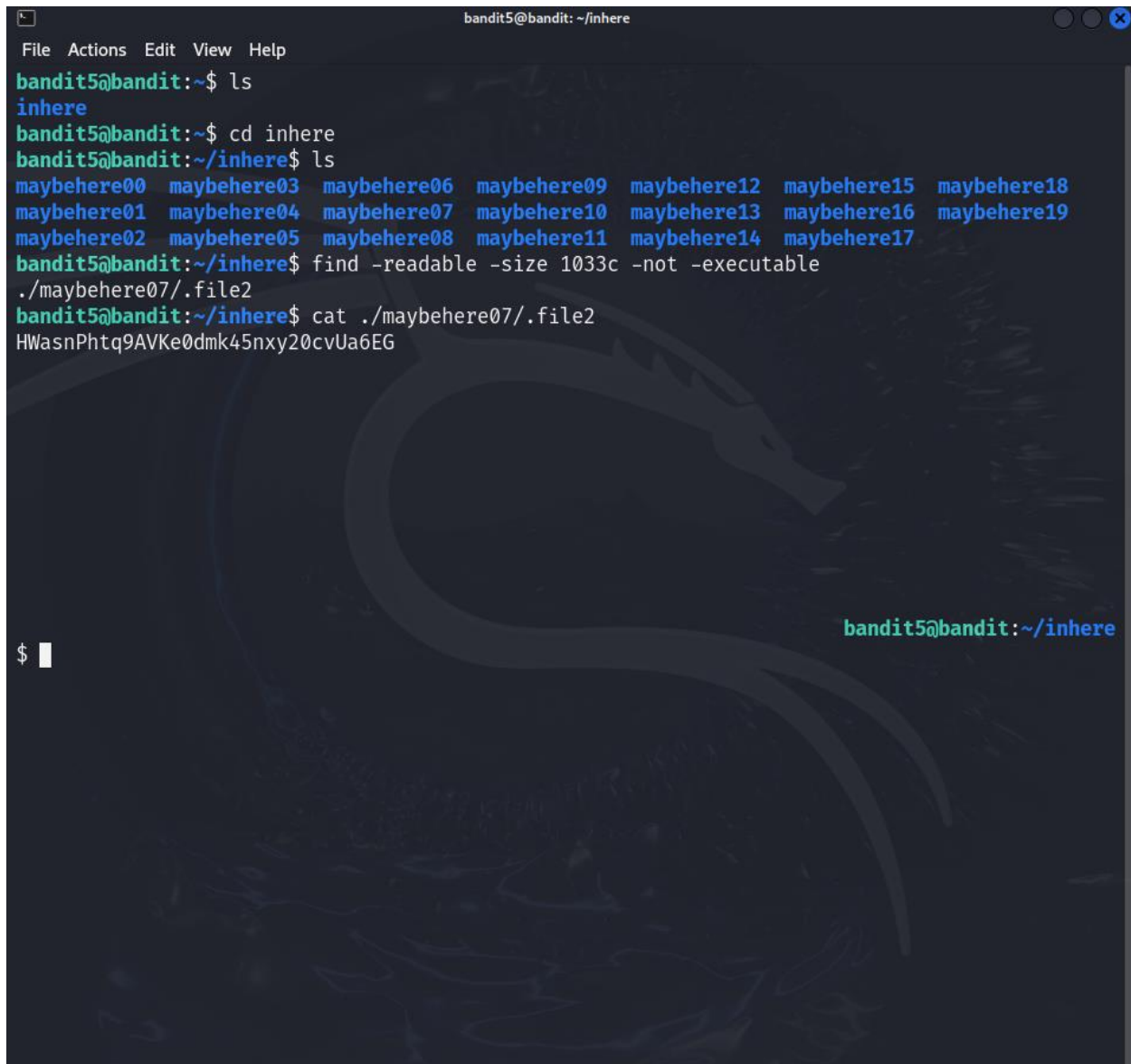
```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ file ./-*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

Note:

The **file** command is used for finding the file type of a file.

After moving to the directory, we should find the file type of each file. So, we use **file ./-*** to find the all file starting with ./- .

Level 5 - 6



```
bandit5@bandit: ~/inhere
File Actions Edit View Help
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00 maybehere03 maybehere06 maybehere09 maybehere12 maybehere15 maybehere18
maybehere01 maybehere04 maybehere07 maybehere10 maybehere13 maybehere16 maybehere19
maybehere02 maybehere05 maybehere08 maybehere11 maybehere14 maybehere17
bandit5@bandit:~/inhere$ find -readable -size 1033c -not -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWAsnPhtq9AVKe0dmk45nxy20cvUa6EG
bandit5@bandit:~/inhere
```

Note:

We use **find** command to find the file with given properties.

It looks for files that can be read but not executed and are exactly 1033 bytes in size.

Level 6 – 7

```
bandit6@bandit: ~  
File Actions Edit View Help  
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c  
find: '/sys/kernel/tracing': Permission denied  
find: '/sys/kernel/debug': Permission denied  
find: '/sys/fs/pstore': Permission denied  
find: '/sys/fs/bpf': Permission denied  
find: '/snap': Permission denied  
find: '/run/lock/lvm': Permission denied  
find: '/run/systemd/inaccessible/dir': Permission denied  
find: '/run/systemd/propagate/systemd-udev.service': Permission denied  
find: '/run/systemd/propagate/systemd-resolved.service': Permission denied  
find: '/run/systemd/propagate/systemd-networkd.service': Permission denied  
find: '/run/systemd/propagate/systemd-logind.service': Permission denied  
find: '/run/systemd/propagate/irqbalance.service': Permission denied  
find: '/run/systemd/propagate/chrony.service': Permission denied  
find: '/run/systemd/propagate/polkit.service': Permission denied  
find: '/run/systemd/propagate/ModemManager.service': Permission denied  
find: '/run/systemd/propagate/fwupd.service': Permission denied  
find: '/run/lvm': Permission denied  
find: '/run/cryptsetup': Permission denied  
find: '/run/multipath': Permission denied  
find: '/run/screen/S-bandit22': Permission denied  
find: '/run/screen/S-bandit20': Permission denied  
find: '/run/screen/S-bandit21': Permission denied  
find: '/run/screen/S-bandit19': Permission denied  
find: '/run/screen/S-bandit0': Permission denied  
find: '/run/screen/S-bandit25': Permission denied  
find: '/run/screen/S-bandit24': Permission denied  
find: '/run/screen/S-bandit18': Permission denied  
find: '/run/screen/S-bandit5': Permission denied  
find: '/run/screen/S-bandit12': Permission denied  
find: '/run/screen/S-bandit14': Permission denied  
find: '/run/screen/S-bandit10': Permission denied  
find: '/run/screen/S-bandit16': Permission denied  
find: '/run/screen/S-bandit13': Permission denied  
find: '/run/screen/S-bandit15': Permission denied  
find: '/run/screen/S-bandit29': Permission denied  
find: '/run/screen/S-bandit8': Permission denied  
find: '/run/screen/S-krypton3': Permission denied  
find: '/run/sudo': Permission denied  
find: '/run/user/11012': Permission denied  
find: '/run/user/11020': Permission denied  
find: '/run/user/11013': Permission denied  
find: '/run/user/11000': Permission denied  
find: '/run/user/11023/systemd': Permission denied  
find: '/run/user/11023/bus': Permission denied  
find: '/run/user/11023/gnupg': Permission denied  
find: '/run/user/11023/pk-debconf-socket': Permission denied  
find: '/run/user/11023/snapd-session-agent.socket': Permission denied  
find: '/run/user/11023/dbus-1': Permission denied  
find: '/run/user/11025': Permission denied  
find: '/run/user/11014': Permission denied  
find: '/run/user/11027': Permission denied  
find: '/run/user/11016': Permission denied
```

Note:

The find command looks for files that has user as bandit7 group as bandit6 and 33 bytes file.

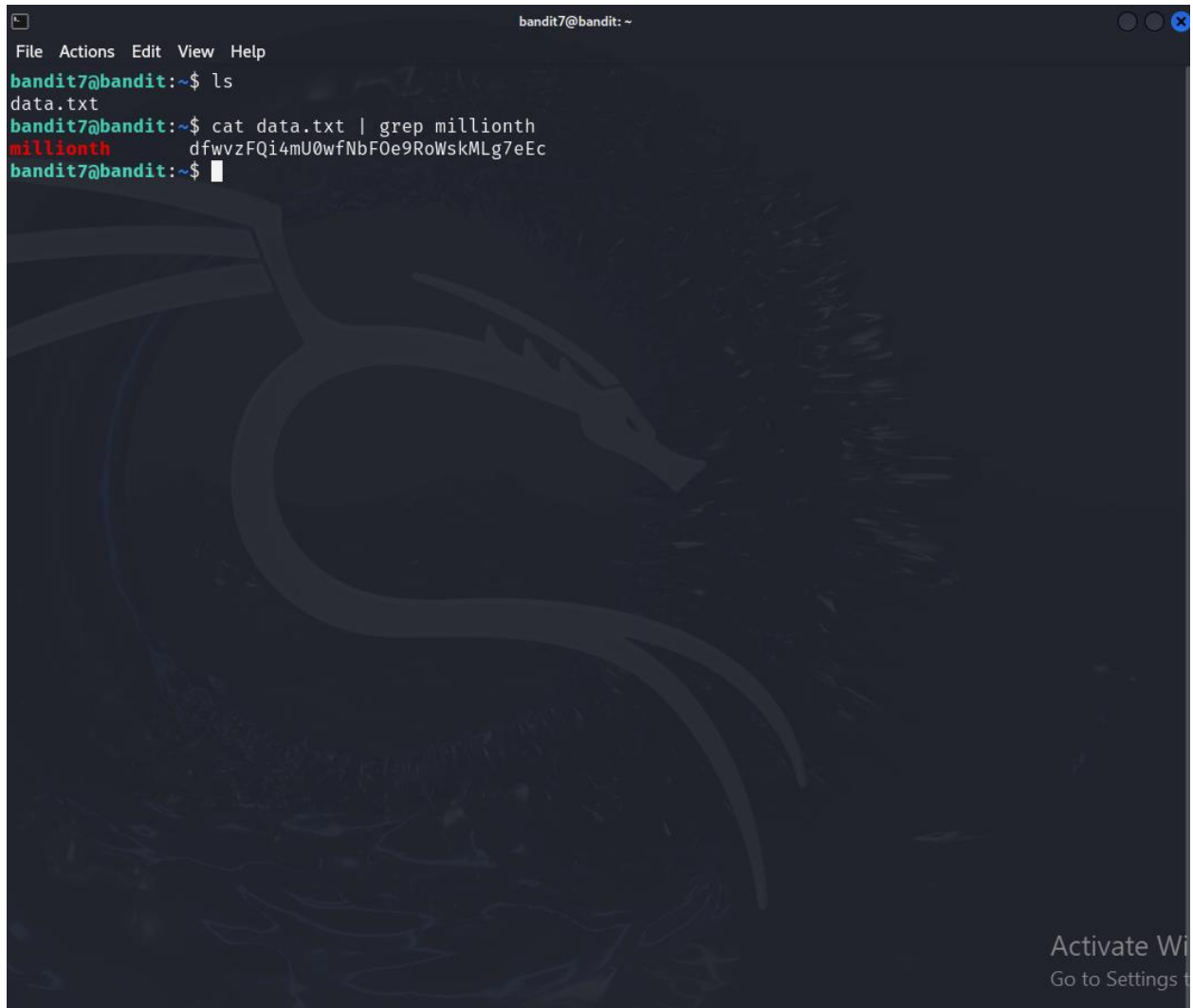
Level 6 – 7

```
bandit6@bandit: ~  
File Actions Edit View Help  
find: '/etc/multipath': Permission denied  
find: '/etc/sudoers.d': Permission denied  
find: '/etc/credstore.encrypted': Permission denied  
find: '/etc/ssl/private': Permission denied  
find: '/etc/credstore': Permission denied  
find: '/etc/xinetd.d': Permission denied  
find: '/etc/polkit-1/rules.d': Permission denied  
find: '/root': Permission denied  
find: '/tmp': Permission denied  
find: '/lost+found': Permission denied  
find: '/dev/shm': Permission denied  
find: '/dev/mqueue': Permission denied  
find: '/var/spool/bandit24': Permission denied  
find: '/var/spool/rsyslog': Permission denied  
find: '/var/spool/cron/crontabs': Permission denied  
find: '/var/lib/udisks2': Permission denied  
/var/lib/dpkg/info/bandit7.password  
find: '/var/lib/snapd/void': Permission denied  
find: '/var/lib/snapd/cookie': Permission denied  
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied  
find: '/var/lib/private': Permission denied  
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied  
find: '/var/lib/amazon': Permission denied  
find: '/var/lib/chrony': Permission denied  
find: '/var/lib/apt/lists/partial': Permission denied  
find: '/var/lib/polkit-1': Permission denied  
find: '/var/log/unattended-upgrades': Permission denied  
find: '/var/log/private': Permission denied  
find: '/var/log/amazon': Permission denied  
find: '/var/log/chrony': Permission denied  
find: '/var/tmp': Permission denied  
find: '/var/cache/private': Permission denied  
find: '/var/cache/ldconfig': Permission denied  
find: '/var/cache/pollinate': Permission denied  
find: '/var/cache/apt/archives/partial': Permission denied  
find: '/var/cache/apparmor/baad73a1.0': Permission denied  
find: '/var/cache/apparmor/2425d902.0': Permission denied  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIlUc0ymOdMaLn0LFVAaj  
bandit6@bandit:~$
```

Note:

Every file is showing permission denied except one file.
we should find it manually and read it.

Level 7 – 8



```
bandit7@bandit: ~  
File Actions Edit View Help  
bandit7@bandit:~$ ls  
data.txt  
bandit7@bandit:~$ cat data.txt | grep millionth  
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc  
bandit7@bandit:~$
```

Note:

Command **grep** helps you find specific words or patterns in files.

We can use **grep** to find the password because it is on the same line as the word 'millionth'.

“|” this symbol tells what should output do.

Level 8 – 9

```
bandit8@bandit: ~  
File Actions Edit View Help  
bandit8@bandit:~$ ls  
data.txt  
bandit8@bandit:~$ cat data.txt | sort | uniq -c  
10 0KCctkqCfY7BIOwqoLXsHDaboXVTkZ49  
10 1SKCEfQ151hW0x9JkeIAmOQdXiC813h1  
10 3hHLoFjM7m3sdyiKJF5QsMqvEIfFh5b1  
10 3hW8tLnDV8acjhTQi44CKXEzHsJb3sqz  
10 3nUXvAjKo7yu6fYykYu7nGGKDMuNMWZf  
10 42qjuz5hdLLItNwdJYsDRpkbbvoEYiWK  
1 4CKMh1JI91bUIZZPXQdGanal4xvAg0JM  
10 5g2sV40okwqDv29Pfo6C7twjKc0k4WQV  
10 5YlL2xxyEUqV6tF0P6NoHt8LOY2EGEc0  
10 6lMDNhQjl0oCOZ5F8ULK2g0uT0rCdnOQ  
10 6z7GGjobj2JASCjNYt0oavrTPCA1GVLc  
10 7f32a50fHRuHaW6lD7l5swMZjK5dKH0t  
10 8H8AWnIimy3xpF9RY7wkOpBxFLK70dHm  
10 9fTezZmzh16K70LBunAd3k0Mor9RIsDv  
10 AiNdScFDXFSBnLNzveDQHAENckqrrJsk  
10 B5mH15Q1FvDMnz0QdREdTRGHtHU6mYqc  
10 BNZFkNcXh3nSE1dEqqBYZKiDAsJj7W4K  
10 bsi00xcFo9wde7ENABAd12ZikWzHfmZa  
10 bT4i2z3wfpWTwImrUrBUzAzqN7MYvi0U  
10 BTuibb63I0yqDgkVyVbu0X8Ma5j4f2ki  
10 bWRXANhoA9ckBDYCPiZU80C23Iwj0NAz  
10 bziGsgFgtBJS2eEiYqWztHPs4ysYaBeP  
10 CJDmZTjXG6TosJ6YFPQ3BhefqB0zzPCq  
10 cJDU7Zp88KXORADTXygR6sQ0KceHRxYn  
10 CkhRsGGr50LPJm0BiSzPUwFLcuaiENBY  
10 c09lpNeUyU9T4FPNVvaejCiUejPTSzlw  
10 cVw919gMWBntrI1oQqEfRGtZGjGUftCu  
10 d2rLG6LAvhW0TXFaER051wqQ3Cb7gyLU  
10 d77bGY1DLZPKdkIvij7EqKy51b5olgiW  
10 DCMmVLsNG2jhnggB59DfFqVH1Yqe3TKr  
10 dLS3M0umsdFIkQNAxp10x6UE09hXcmTg  
10 dW9Vv1sbgSMbKqstgICWbwbZSWyczGrK  
10 DWBLXSfkBJPNCV092M9hWSzpyIH8WVXr  
10 dXmpp5K2sMrKsbGjqoS5EE4jrBaP0kdF  
10 EkIk0LInZr2E0gdW8Ulk0vCK3Ys6xqjI  
10 ekTd8FrXagu5mb8JSGz3ILUGoMy53srx  
10 fA9kkjNN2w5ucHzehI7KL2eOWwGYu68y  
10 fcIDERLIVL2YN3ZoJJz55LgjWYqGV4EQ  
10 fRKpp1s1s9Db7GoQRgcLtgaohzV7ym0w
```

Note:

This command reads data.txt, sorts the lines in ascending order, and then counts and shows unique lines with their frequency. It helps summarize repeated entries in the file.

Password repeated only once.

Level 9 – 10

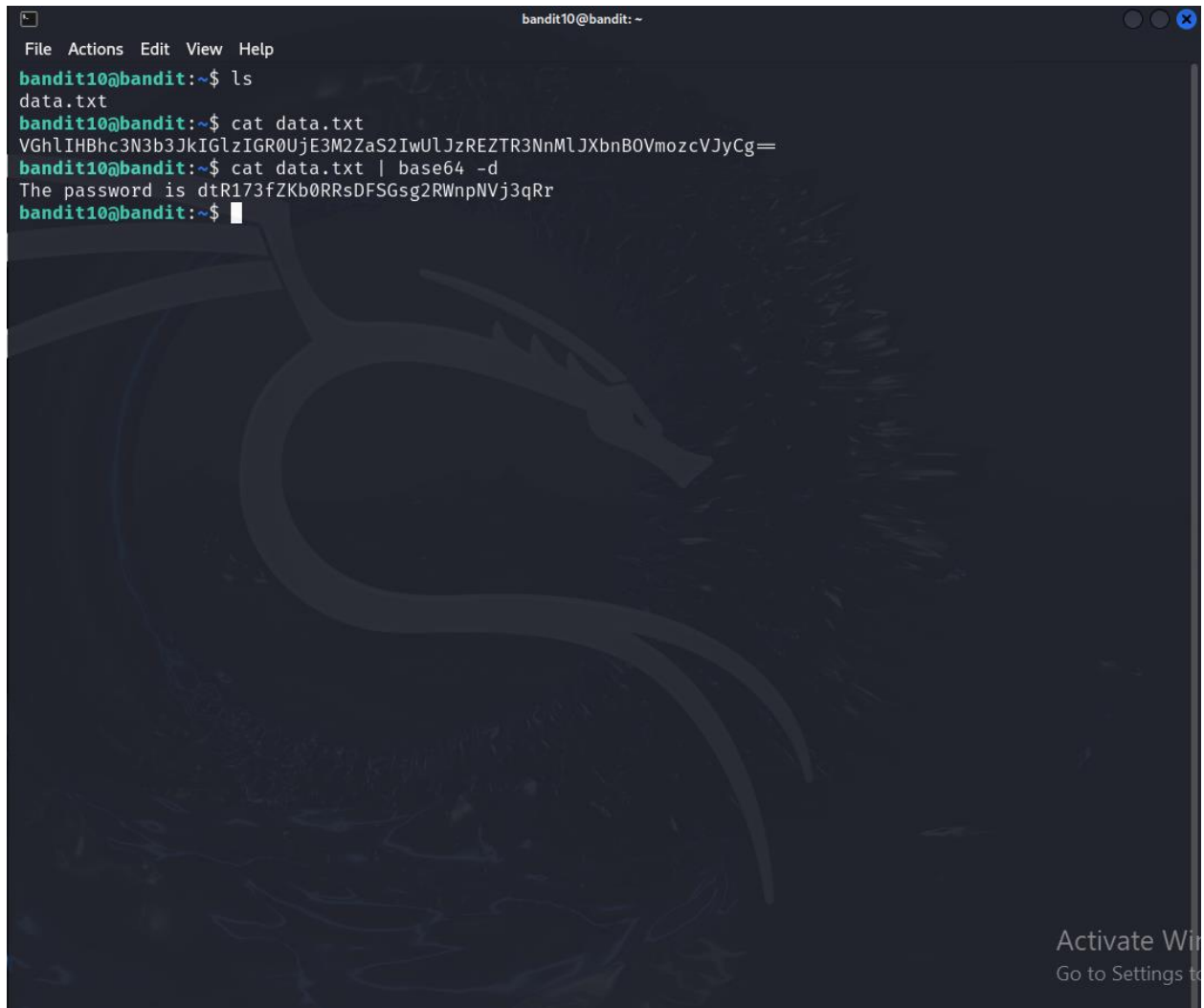


```
bandit9@bandit: ~  
File Actions Edit View Help  
bandit9@bandit:~$ ls  
data.txt  
bandit9@bandit:~$ cat data.txt | strings | grep =  
=aA"f  
\a!;===== the  
PWAf=1  
M),\}=  
2Y6=  
G';?e=  
===== passwordf  
===== isc  
*=N6  
m=</  
E=Bty  
=sw  
"M1=  
===== FGUW5illVJrxX9kMYMmLN4MgbpfMiqey  
!&-u84$  
*XA=  
bandit9@bandit:~$
```

Note:

This command filters out readable text, and then looks for lines with =. It helps identify specific patterns within the file.

Level 10 – 11



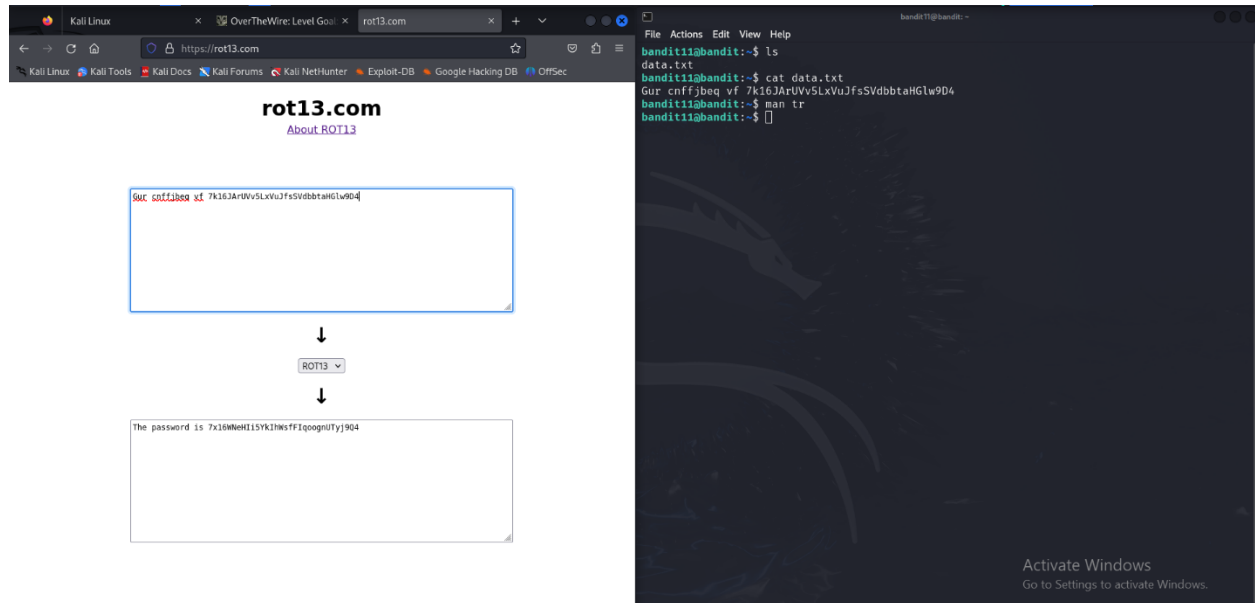
```
bandit10@bandit: ~  
File Actions Edit View Help  
bandit10@bandit:~$ ls  
data.txt  
bandit10@bandit:~$ cat data.txt  
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==  
bandit10@bandit:~$ cat data.txt | base64 -d  
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr  
bandit10@bandit:~$
```

Note:

This command decodes its Base64 content and displays the result. It's useful for converting encoded data back into its original form.

Level 11 – 12

Note: ROT13 decoding shifts letters 13 places in the alphabet, reversing the encoding.



Level 12 – 13

```
bandit12@bandit: /tmp/gm12
data9.bin: ASCII text
bandit12@bandit: /tmp/gm12$ cat data9.bin
The password is F05dWfSc0cbaiiH0h832eUks2vdTDwAn
bandit12@bandit: /tmp/gm12$ history
1 clear
2 ls
3 cd /tmp
4 mkdir gm12
5 cd
6 cp data.txt gm12
7 cd ..
8 cd
9 cd /tmp
10 cp data.txt gm12
11 ls
12 cd /tmp/gm12
13 ls
14 mv data.txt data1.txt
15 ls
16 -xxd -r data1.txt compressed_data
17 xxd -r data1.txt compressed_data
18 ls
19 file compressed_data
20 mv compressed_data data2.bin.gz
21 ls
22 file data2.bin.gz
23 gunzip data2.bin.gz
24 ls
25 file data2.bin
26 mv data2.bin data2.bin.bz2
27 ls
28 file data2.bin.bz2
29 bzip2 -d data2.bin.bz2
30 ls
31 file data2.bin
32 mv data2.bin data4.bin.gz
33 file data4.bin.gz
34 gunzip data4.bin.gz
35 ls
36 file data4.bin
37 man tar
38 tar -xf data4.bin
39 ls
40 file data5.bin
41 tar -xf data5.bin
42 ls
43 file data6.bin
44 mv data6.bin data6.bin.bz2
45 bzip2 -d data6.bin.bz2
46 bzip2 -d data6.bin.bz2
47 ls
48 file data6.bin
49 tar -xf data6.bin
50 ls
51 file data8.bin
52 mv data8.bin data9.bin.gz
53 gunzip data9.bin.gz
54 ls
55 file data9.bin
56 cat data9.bin
57 history
bandit12@bandit: /tmp/gm12$
```

Note:

1. Creating directory in /tmp and moving file.
2. Reverting hexdump of the file using xxd.
3. Repeatedly decompress the file using gunzip for gzip file and bzip2 -d for bz2 file.
4. After finding tar file we should extract it. -xf (extract file).
5. Repeat it until finding ASCII TEXT file.

Level 13 – 14

[illegible]

Note:

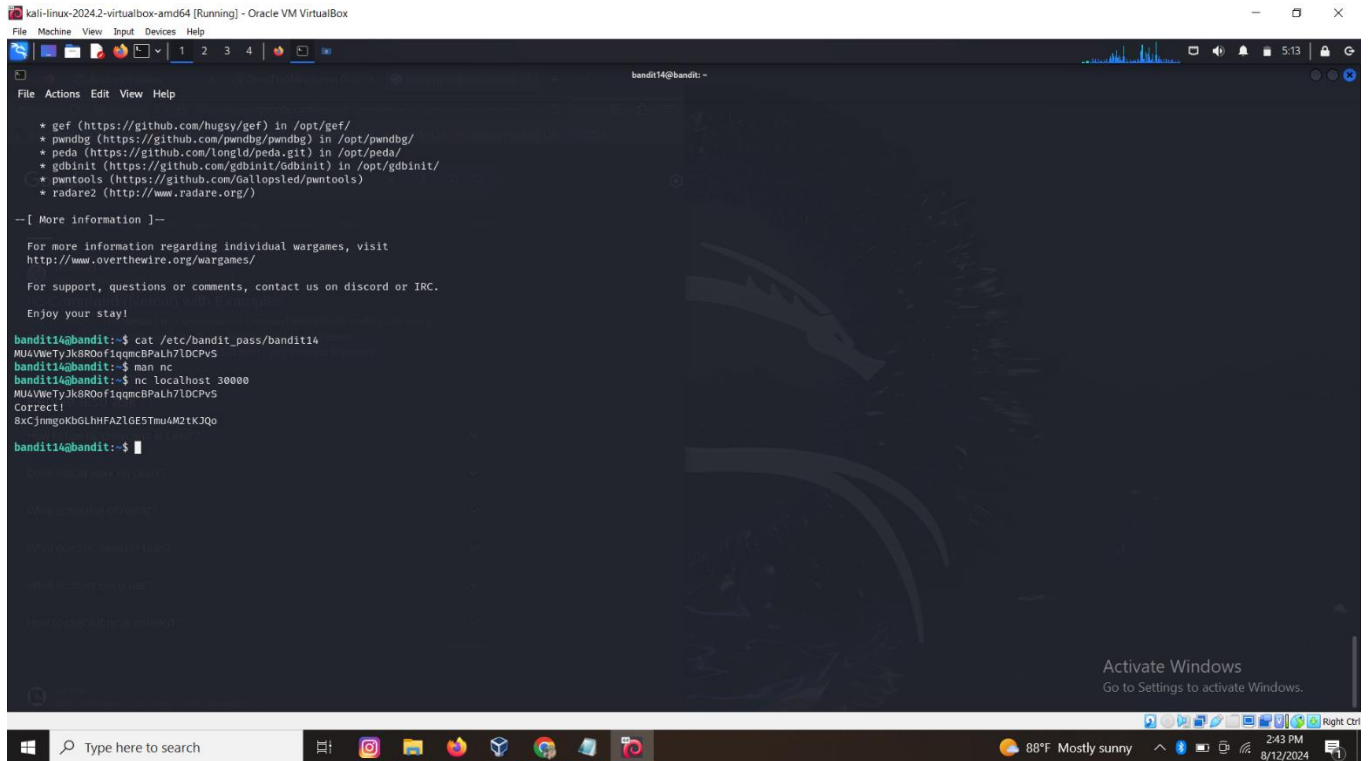
Scp command mean secure file copy.

This command securely copies the file `sshkey.private` from a remote server to our local machine. It connects to the server on port 2220 using `scp`, which is a secure file transfer protocol.

After saving the file we can move into the next level with that private key file.

Option -i with ssh command is used for private key.

Level 14 – 15



```
kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
bandit14@bandit: ~
File Actions Edit View Help

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* 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!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MUA4WeTy3k8R0ofiqmc8PaLh7LDCPvS
bandit14@bandit:~$ man nc
bandit14@bandit:~$ nc localhost 30000
MUA4WeTy3k8R0ofiqmc8PaLh7LDCPvS
Correct!
8xCJnmg0KbGLHFAZ1GE5Tmu4M2tK3Qo

bandit14@bandit:~$
```

Note:

Reading the current password in `/etc/bandit_pass/bandit14`.
This **nc** command connects to a local server on port 30000.
It allows us to read and write data over a network connection.
we need to submit the password to port 30000 on localhost.

Level 15 – 16

```
bandit15@bandit: ~  
File Actions Edit View Help  
bandit15@bandit:~$ openssl s_client -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:PKKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256  
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT  
-----  
Server certificate  
-----BEGIN CERTIFICATE-----  
MIIFBzCCAu+gAwIBAgIU8L7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL  
BQAwEzERMA8GA1UEAwYIU25ha2VPaWwwHhcNMjQ0MjUwMjUwMjUwMjUwMjUw  
MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAIwDQYJKoZIhvcNAQEBBQAD  
ggIPADCCAgQCGgIBANI+P5QXm9Bj21FIPsQqbqZrB5XmSZZJYaam7EIJ16Fxedf+  
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0LAfN33h+RMTjRoMb8yBsZsC063MLfXck4p+  
09gtGP7BS6Iy5XdmfY/fPHvA3JDEscdLDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/  
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE4OzoSrt5+bZVLvODWUFWinB0fLaGRk  
GmI0r5EU0Ud7HpYyoIQbiNlePGfPpHRKnmdXTTEZEoxeWWAAm1VhPGqfrB/Pnca+  
vAJX7iB0b3KHinmfVOScsG/YAUR94wSELeY+ULEWJaELVUntrJ5HeRDiTChiVQ++  
wnnjNbepaW6shopybUF3XXfhIb4NvwLWpvoKFXVtcVjL0ujF0snVvpE+MRT0wacy  
tHtjZs7Ao7GYxDz6H8AdBLKJW67uQon37a4MI260ADFMS+2vEAbNSFP+f6ii5mrB  
18cY64ZaF6oU8bjGK7BARdx56bRc3WFyUBIGWAFHEuB948BcshXY7baf5jjzPmgz  
mq1zdRthQB31MOM2ii6vuTkheAvKff+llH4M9SnES4NSF2hj9NnHga9V08wfhYc  
x0W6qu+S8HudVF+V23yTvUNgz4Q+UoGs4sHSDEsIBFqNvInnpUmtNgcR2L5PAGMB  
AAGjUzBRMB0GA1UdDgQWB8TPo8kfze4P9EgxNuyk7+xDGfTAYzAFBgNVHSMEGDAW  
gBTPo8kfze4P9EgxNuyk7+xDGfTAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3  
DQEBCwUAA4ICAQAKHomtmCGqyiLnhziLe97Mq2+Su15QgYVwfx/KY0Xxv2T8ZmcR  
Ae9XFhZT4jsA0UDK10Xx9aZgDGJHJLNEVTe9zWv10NFFNxEBxQgP7hhdBWDtj6d  
taqEW/Jp06X+08BtNtYK9NZsvDg2YRcvOHConEjwvEL7tQK0m+GVyQfLYg6jnrhx  
egH+abucTKxabFcWSE+Vx0uJYMqcbXvB4WNKz9vj4V5Hn7/DN4xIjFko+nREw60a  
/AUFjNnO/FPjap+d68H1LdzMH3PSS+yjGid+6Zx9FCnt9qZydW13Miqg3nDnODXw  
+Z682mQFjVLGPCA5ZOQbyMKY4tNazG2n8qy2famQT3+jF8Lb6a4NGbnpeWnLMkIu  
jWLIkA9MlbdNXuajjPNVYyIK9gdoBzbfakwoOfSsLxEqlf8rio1GGcEV5HlZ5S2  
txwI0xdW9MWeGwoilBzSbRjH4TIBFFtoBG0LoEJi0C+UPwS8CDngJB4TyrZqEld3  
rH87W+Et1t/Nepoc/Eoaux9PFp5VPXP+qwQGmhir/hv7OsgBhrkYuhkxjZ8+1uk7  
tUWC/XM0mpLoxsq6vVL3AJaJe1ivdA9xLytsuG4iv02Juc593HXyR8yOpow0Eq2T  
U5EyuFg5RXYwAPi7ykw1PW7zAPL4MlonEVz+QXOSx6eyhimp1VZC11SCg==  
-----
```

Activate Windows
Go to Settings to activate Windows.

Note:

openssl s_client is the implementation of a simple client that connects to a server using SSL/TLS.

Level 15 – 16

```
bandit15@bandit: ~  
File Actions Edit View Help  
—  
read R BLOCK  
—  
Post-Handshake New Session Ticket arrived:  
SSL-Session:  
  Protocol : TLSv1.3  
  Cipher   : TLS_AES_256_GCM_SHA384  
  Session-ID: D6D8767D26D4F863CF374E9C92853EA58F1DBC470632F31FBB717C9A142E8436  
  Session-ID-ctx:  
  Resumption PSK: 3EC11190775A117886532C1B5D7D0DC211E014452FB8B2BF68FF07342BA2A8EEE4BB4B6289D795EE2FA  
10B864326EF86  
  PSK identity: None  
  PSK identity hint: None  
  SRP username: None  
  TLS session ticket lifetime hint: 300 (seconds)  
  TLS session ticket:  
0000 - e0 1f e7 ec fb 63 73 2a-fc 3f d4 40 de 78 4c d8 .....cs*..?.@.xL.  
0010 - 89 c0 e8 78 55 88 45 3b-73 fb dd 85 70 d9 91 13 ...xU.E;s...p...  
0020 - fb 74 11 10 07 2e 5e ca-0e d5 4a 07 09 45 1f 81 .t....^...J..E..  
0030 - 6f de 02 5d 8a 43 35 6f-f8 34 97 ef 91 ac 50 56 o..].C5o.4....PV  
0040 - 04 48 0f fa d8 36 64 64-a4 e1 f3 7d 39 2b 96 fd .H...6dd...}9+..  
0050 - 0b 19 81 e1 cf 0c f1 ab-ee 19 2d c4 14 53 1b 78 .....-..S.x  
0060 - 7e 33 a9 9c 18 7f 9d 5a-ff ec 2e 76 56 7b 6f 40 ~3.....Z...vV{o@  
0070 - ad 03 7c b3 fa cb 98 5b-01 1e 61 e0 43 1b 20 d7 ..|....[..a.C. .  
0080 - 74 72 e9 ae a1 da 41 48-1d 8d 17 72 29 f7 93 e1 tr....AH...r)...  
0090 - db be 6f a5 dd 06 2c 4d-69 f1 39 f2 9f 3d 60 0e ..o... ,Mi.9..='.  
00a0 - 8a 99 83 f4 aa aa 5b ca-64 f9 dc bb 1b 74 c7 10 .....[.d....t..  
00b0 - 02 4e 42 5b 9c 9c dd 82-9b cd 22 84 6e a1 1c ae .NB[.....".n...  
00c0 - 1b a6 b8 e4 93 aa 76 22-96 0e 61 0e 27 f2 8b 59 .....v"...a..'..Y  
00d0 - c9 19 3b 16 c9 8a c5 59-cd 83 38 71 62 95 6a 7d ..;....Y..8qb.j}  
  
Start Time: 1723456702  
Timeout : 7200 (sec)  
Verify return code: 18 (self-signed certificate)  
Extended master secret: no  
Max Early Data: 0  
—  
read R BLOCK  
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo  
Correct!  
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRY0Dx  
  
closed  
bandit15@bandit:~$
```

Note:

I connect to the localhost server with the OpenSSL s_client and send the password from this level. The server then sends back the password for the next level.

Level 16 – 17

```
File Actions Edit View Help
bandit16@bandit:~$ nmap -sV localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 16:22 UTC
Stats: 0:01:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 16:24 (0:00:21 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 16:24 (0:00:00 remaining)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00023s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
31960/tcp  open  echo
1 Service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31790-TCP:V=7.94SVNNT=SSLXI=7XD=8/13RTIME=66888859P=x86_64-pc-linux
SF:x-gnuXr(GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password\.\n")Xr(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password\.\n")Xr(HTTPOptions,32,"Wrong!\
SF:x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")Xr(RTS
SF:Request,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password\.\n")Xr(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password\.\n")Xr(FourOfFourRequest,32,"Wrong!\x20Please\x2
SF:0enter\x20the\x20correct\x20current\x20password\.\n")Xr(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\.\n")
SF:Xr(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password\.\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 146.02 seconds
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lByyCMAGBPvCVTlBfWry0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAymOkulfnMgGHL2YPIOjon61wfbp7c3jx34YkYwqUHS75UdyJ
imZeyGCGtZPGuJUSxL3SWL/otqexheCANTSMLOJf7zBr30BAraxd9Y7YT2BRPQ
Ja0LzB558Yw3FZl87OR10+rwALCDNDlUvLE/GL2GwyuKN0K5lCd5TbtJ2EkQTU
DST2mcNn4rHAL+JFr56o4T6z8WAW18BR6yGmQ7Q/KALHYW30eKePQA2L0VUYDW
JGT165CxbCnzc/w4+mqQyvmzpWtMaz3TzAzQxNbrR2MBGySxDLrjg0LWN6SK7wNX
x0YVZtz/zblKpJfkuIjHs+9EBVnj+D1XF0JuaQ1DAQBAoI8ABagxpMlaolWfvd
KHcj10nqcoBc4oE11aFYQw1k7xFW+Z4PRNUDE6Sfth0ar69jp5RLLWD1NHpx31BL
-----END RSA PRIVATE KEY-----
```

```
bandit17@bandit:~$ nano sshkey17.private
bandit17@bandit:~$ ssh -i sshkey17.private bandit17@bandit.labs.overthewire.org -p 2220

bandit17

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

www. ver he ire.org

Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.

--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMES are somegame0, somegame1, ...
* Most LEVELS are stored in /somegame/.
```

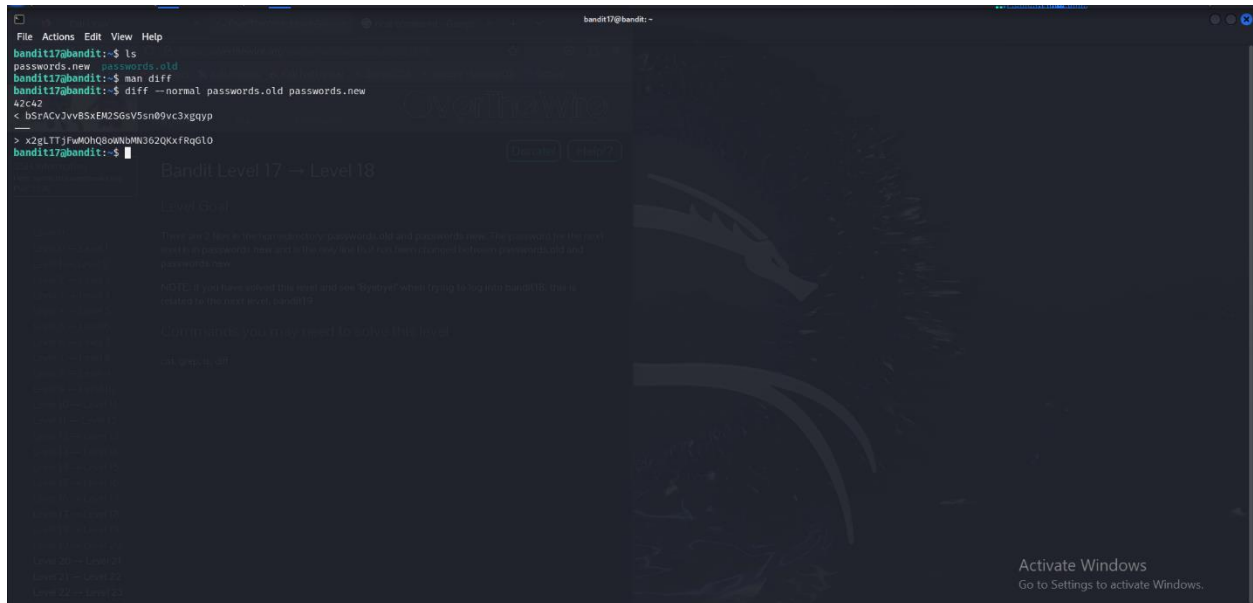
Note:

This command scans ports 31000 to 32000 on your local machine to find open services and their versions. -sV is used for version detection.

Nmap is a network scanner. It can do Host Discovery, Port Scanning, Version Detection etc.

After that connects to local port 31790 using SSL encryption with ncat. And send the password.

Level 17 – 18



```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ man diff
bandit17@bandit:~$ diff --normal passwords.old passwords.new
42c42
< bSrACvJvvBSxEM2SGsV5sn0vc3xgqyp
> x2gLTTFwM0h0S0wWbWJ3Q2QKxfrQ0LO
bandit17@bandit:~$
```

Bandit Level 17 → Level 18

Good job!

You got the base64-encoded passwords.old and passwords.new files. To get the next level, you need to decode the old file and find the password for the new file.

As a hint, you can use the `diff` command to find the differences between the two files.

Good luck!

Note:

After getting private key in previous level, we should save it in our local machine and login to the current level with that key using **ssh -i**.

The **diff --normal** command compares two files, password.old and password.new, and shows the differences between them.

Level 18 – 19

```
kali@kali ~  
File Actions Edit View Help  
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!  
  
Byebye !  
Connection to bandit.labs.overthewire.org closed.  
  
(kali@kali)~  
$ ssh bandit18@bandit.labs.overthewire.org -p 2220 ls  
Connection closed by 13.50.165.192 port 2220  
  
(kali@kali)~  
$ ssh bandit18@bandit.labs.overthewire.org -p 2220 ls  
  
bandit18@bandit.labs.overthewire.org:~  
┌───┴───┐  
│ 0 1 2 3 4 5 6 7 8 9 │  
│ 1 0 1 1 1 1 1 1 1 1 │  
│ 1 0 1 1 1 1 1 1 1 1 │  
│ 1 0 1 1 1 1 1 1 1 1 │  
└───┴───┘  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit18@bandit.labs.overthewire.org's password:  
readme  
  
(kali@kali)~  
$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme  
  
bandit18@bandit.labs.overthewire.org:~  
┌───┴───┐  
│ 0 1 2 3 4 5 6 7 8 9 │  
│ 1 0 1 1 1 1 1 1 1 1 │  
│ 1 0 1 1 1 1 1 1 1 1 │  
│ 1 0 1 1 1 1 1 1 1 1 │  
└───┴───┘  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit18@bandit.labs.overthewire.org's password:  
cGwPmKXVuDUNgPAV3bWYuGHVn9z13j8
```

Note:

.bashrc is a file that is run every time a terminal is loaded.

SSH also allows remote execution of commands.

Instead of logging into the machine with SSH, we just run a command remotely using SSH.

we read the file to find the password.

Level 19 – 20

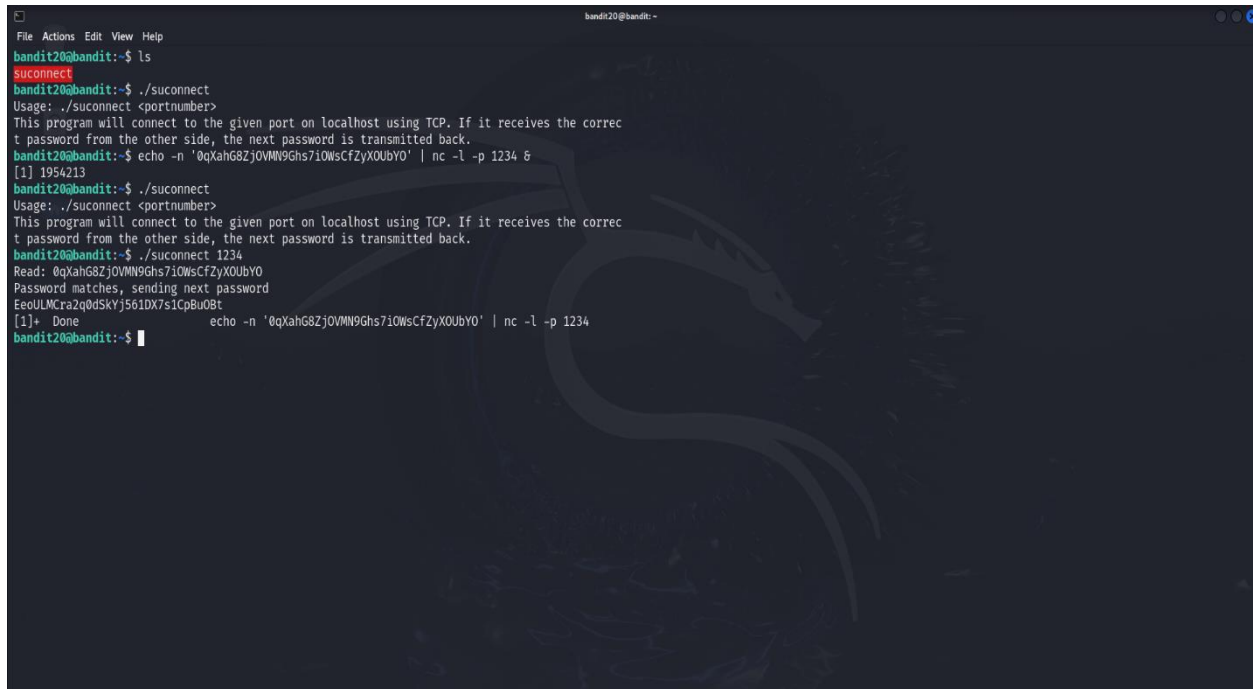
```
bandit19@bandit:~$ cat /etc/bandit_pass/bandit19
c0wPMaxXlv0UngPAV2bWuGwNz13j0
bandit19@bandit:~$ cat /etc/bandit_pass/bandit20
cat: /etc/bandit_pass/bandit20: Permission denied
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ls -l
total 16
-rwsr-x--- 1 bandit20 bandit19 14880 Jul 17 15:57 bandit20-do
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do ls /etc/bandit_pass
bandit0 bandit12 bandit16 bandit2 bandit23 bandit27 bandit30 bandit4 bandit8
bandit1 bandit13 bandit17 bandit20 bandit24 bandit28 bandit31 bandit5 bandit9
bandit10 bandit14 bandit18 bandit21 bandit25 bandit29 bandit32 bandit6
bandit11 bandit15 bandit19 bandit22 bandit26 bandit3 bandit33 bandit7
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXah08Zj0VMpGhs7l0wsCf2yX0Uby0
bandit19@bandit:~$
```

Note:

-rwsr-x--- means the user bandit19 can execute the binary, but the binary is executed as user bandit20.

Executing the binary says it simply executes another command as another user. This means We can access the password file for the user bandit20, but only the bandit20 user is allowed to read it.

Level 20 – 21



```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ ./suconnect
Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it receives the correct password from the other side, the next password is transmitted back.
bandit20@bandit:~$ echo -n '0qXahG8Zj0VMN9Ghs7iOWsCfZyXOUbY0' | nc -l -p 1234 &
[1] 1954213
bandit20@bandit:~$ ./suconnect
Usage: ./suconnect <portnumber>
This program will connect to the given port on localhost using TCP. If it receives the correct password from the other side, the next password is transmitted back.
bandit20@bandit:~$ ./suconnect 1234
Read: 0qXahG8Zj0VMN9Ghs7iOWsCfZyXOUbY0
Password matches, sending next password
EeoULMCraZq0dSKYj561DX7s1CpBu08t
[1]+  Done                  echo -n '0qXahG8Zj0VMN9Ghs7iOWsCfZyXOUbY0' | nc -l -p 1234
bandit20@bandit:~$
```

Note:

Using 'netcat'/nc, we can create a connection in server mode.

The provided command sends the string over **netcat** on port 1234 and runs in the background.

./suconnect 1234 this command runs 'suconnect' program and connects to port 1234 and sends back the password.