

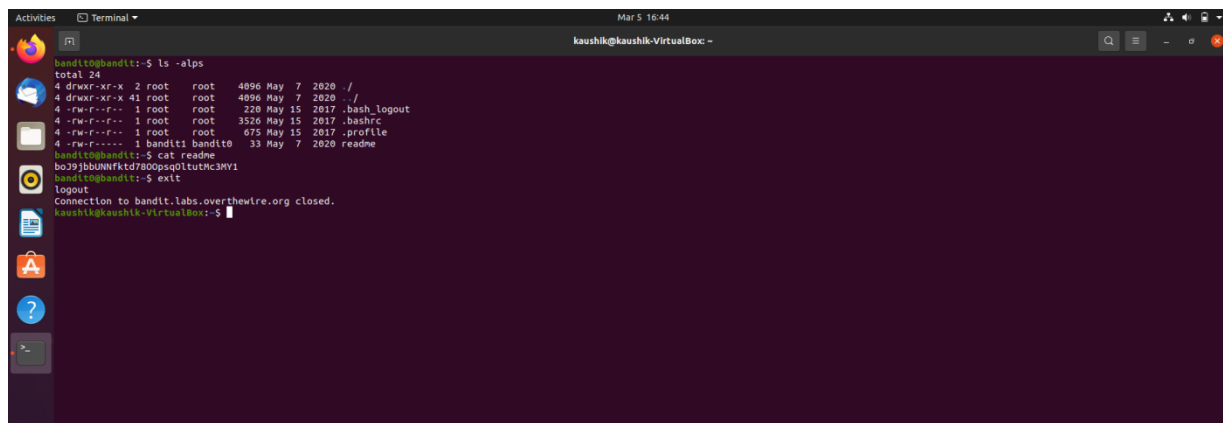
Cognizance [task-7]

Linux games

Level 0:

Password:

boJ9jbbUNNfktd78OOpsqOltutMc3MY1

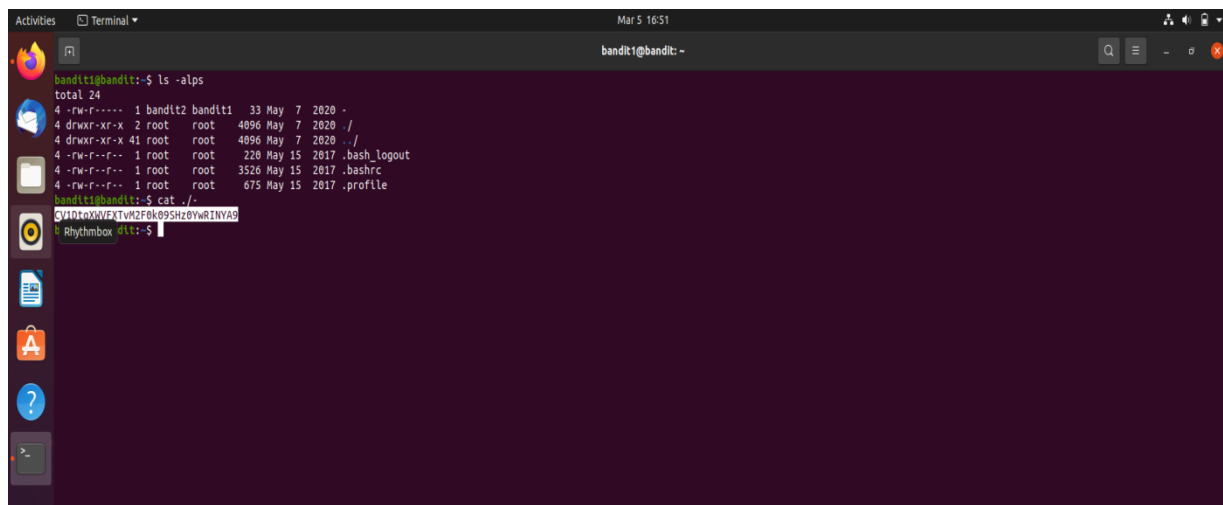
A terminal window titled 'kaushik@kaushik-VirtualBox: ~' showing the execution of 'ls -alps' and 'cat readme'. The output of 'ls -alps' lists files in the current directory, including 'readme'. The output of 'cat readme' shows the password 'boJ9jbbUNNfktd78OOpsqOltutMc3MY1'. The terminal also shows the user logging out and the connection to bandit.labs.overthewire.org closing.

```
bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 2 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
4 -rw-r----- 1 bandit1 bandit0 33 May 7 2020 readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
kaushik@kaushik-VirtualBox:~$
```

Level 1:

Password:

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

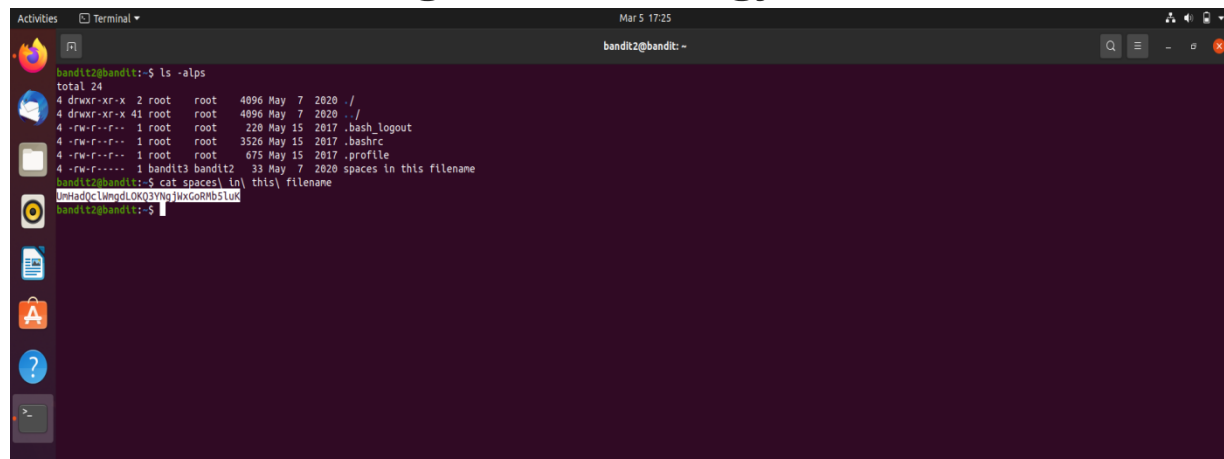
A terminal window titled 'bandit1@bandit: ~' showing the execution of 'ls -alps' and 'cat ./'. The output of 'ls -alps' lists files in the current directory, including 'readme'. The output of 'cat ./' shows the password 'CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9'. The terminal also shows the user logging out and the connection to bandit.labs.overthewire.org closing.

```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r----- 1 bandit2 bandit1 33 May 7 2020 -
4 drwxr-xr-x 2 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
bandit1@bandit:~$ cat ./
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
kaushik@kaushik-VirtualBox:~$
```

Level 2:

Password:

UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

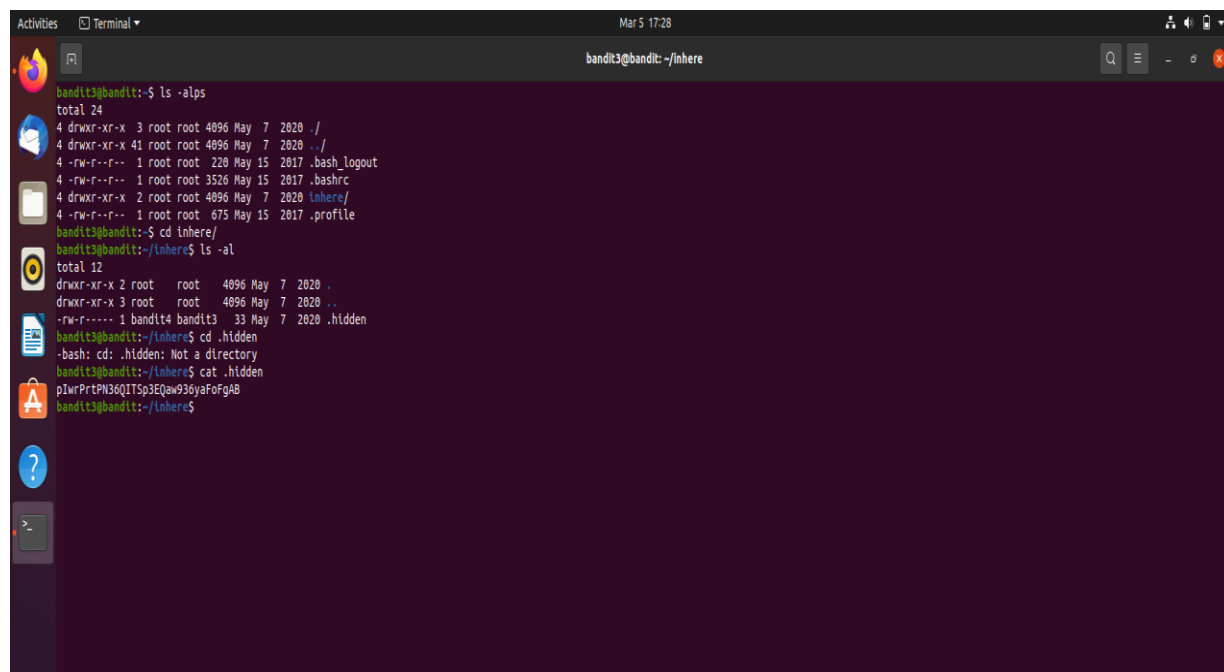
A terminal window titled 'bandit2@bandit: ~' showing the command 'ls -alps' and its output. The output lists files in the current directory, including a file named 'spaces' which contains the password 'UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK'.

```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 2 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
4 -rw-r----- 1 bandit3 bandit2 33 May 7 2020 spaces in this filename
bandit2@bandit:~$ cat spaces | tr '\n' '\0'
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$
```

Level 3:

Password:

plwrPrtPN36QITSp3EQaw936yaFoFgAB

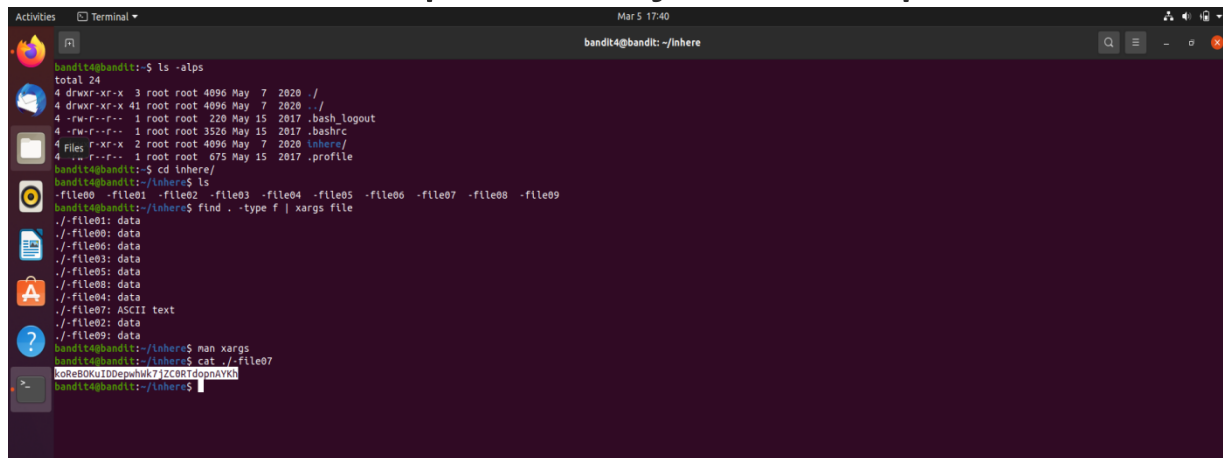
A terminal window titled 'bandit3@bandit: ~/inhere' showing the command 'ls -alps' and its output. The output lists files in the current directory, including a file named 'hidden' which contains the password 'plwrPrtPN36QITSp3EQaw936yaFoFgAB'.

```
bandit3@bandit:~/inhere$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 drwxr-xr-x 2 root root 4096 May 7 2020 inhere/
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
bandit3@bandit:~/inhere$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 May 7 2020 .
drwxr-xr-x 3 root root 4096 May 7 2020 ..
-rw-r----- 1 bandit4 bandit3 33 May 7 2020 .hidden
bandit3@bandit:~/inhere$ cd .hidden
-bash: cd: .hidden: Not a directory
bandit3@bandit:~/inhere$ cat .hidden
plwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

Level 4:

Password:

koReBOKuIDDepwhWk7jZC0RTdopnAYKh

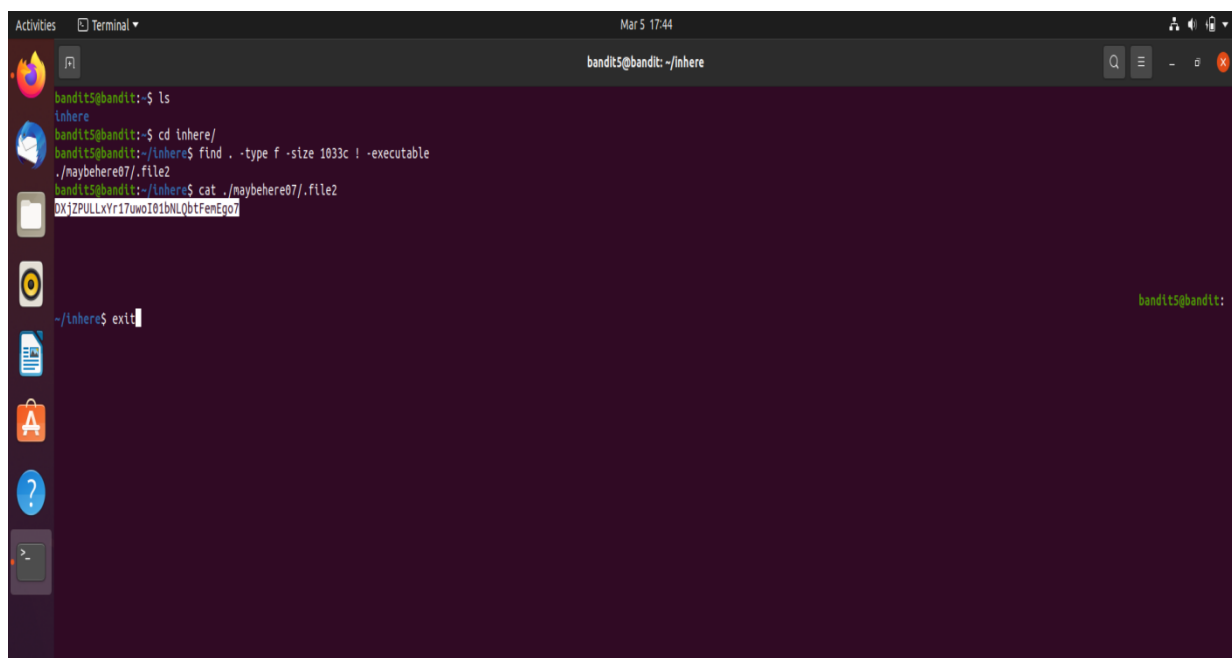
A terminal window titled 'bandit4@bandit: ~/lnhere' showing the process of solving Level 4. The user runs 'ls -alps' to list files, then 'cd lnhere/' to enter the 'lnhere' directory. They run 'ls' again to see files named -file00 through -file09. Then, they use 'find . -type f | xargs file' to identify the files, discovering that -file07 is an ASCII text file. Finally, they run 'cat ./-file07' to reveal the password: 'koReBOKuIDDepwhWk7jZC0RTdopnAYKh'.

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 files -r-xr-x 2 root root 4096 May 7 2020 lnhere/
4 --r--r-- 1 root root 675 May 15 2017 .profile
bandit4@bandit:~$ cd lnhere/
bandit4@bandit:~/lnhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/lnhere$ find . -type f | xargs file
./-file01: data
./-file00: data
./-file06: data
./-file03: data
./-file05: data
./-file08: data
./-file04: data
./-file07: ASCII text
./-file02: data
./-file09: data
bandit4@bandit:~/lnhere$ man xargs
bandit4@bandit:~/lnhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/lnhere$
```

Level 5:

Password:

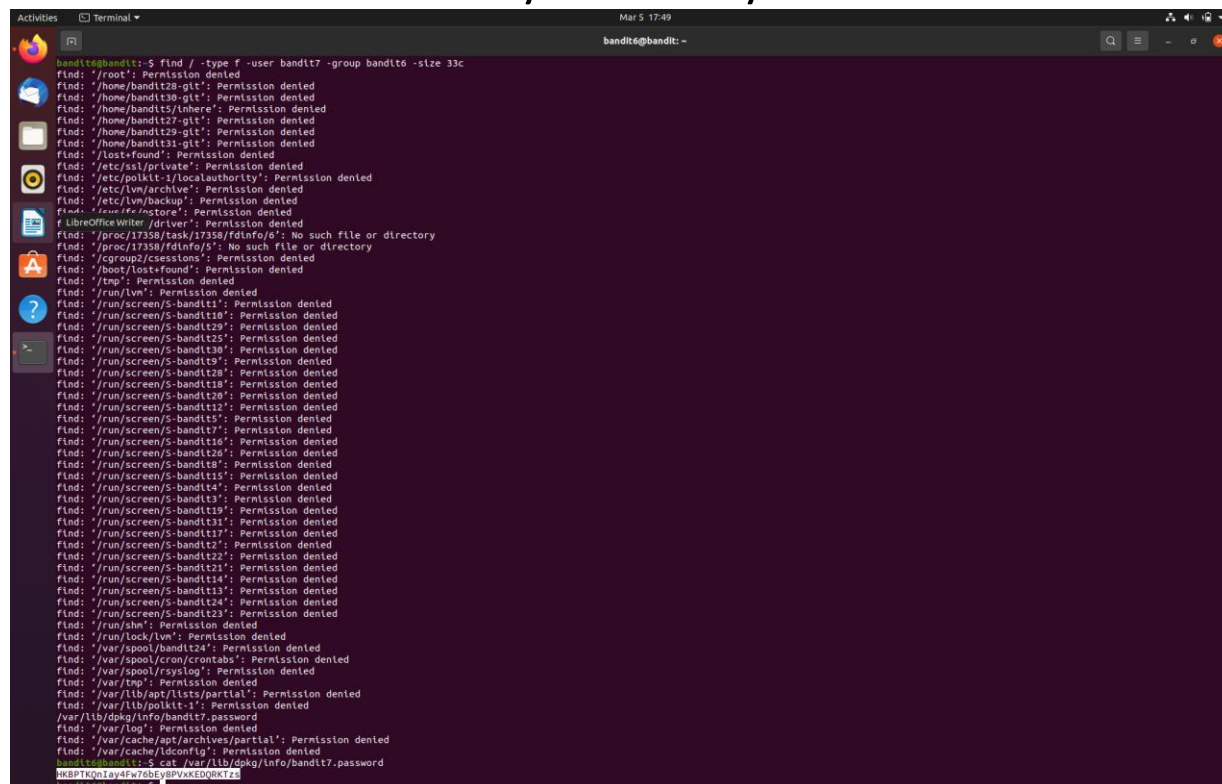
DXjZPULLxYr17uwoIO1bNLQbtFemEgo7

A terminal window titled 'bandit5@bandit: ~/lnhere' showing the process of solving Level 5. The user runs 'ls' to see the 'lnhere' directory. Then, they run 'cd lnhere/' and 'find . -type f -size 1033c ! -executable' to find a file. They discover './maybehere07/.file2'. Finally, they run 'cat ./maybehere07/.file2' to reveal the password: 'DXjZPULLxYr17uwoIO1bNLQbtFemEgo7'.

```
bandit5@bandit:~$ ls
lnhere
bandit5@bandit:~$ cd lnhere/
bandit5@bandit:~/lnhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/lnhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoIO1bNLQbtFemEgo7
bandit5@bandit:~/lnhere$ exit
```

Level 6:

Password: HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs

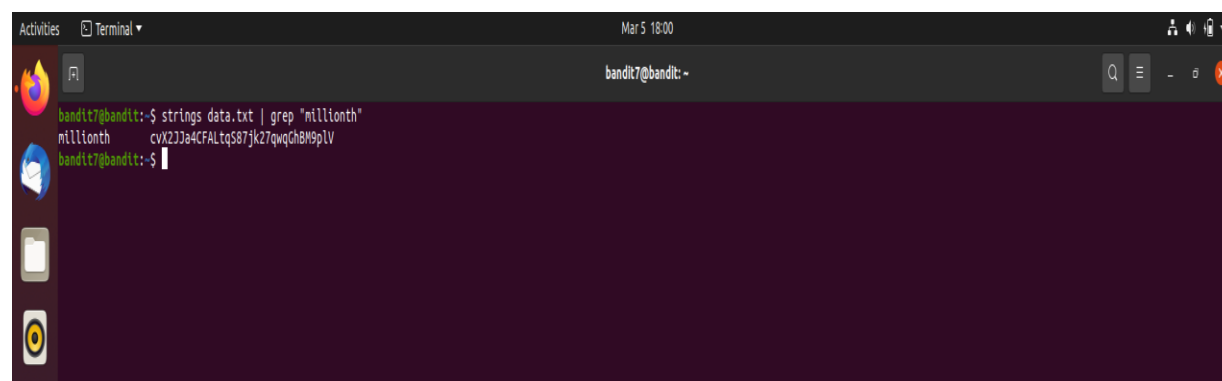


A terminal window titled "bandit6@bandit: -" showing the execution of a find command. The command is: `bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c`. The output lists numerous files and directories across the system, all of which are denied access with the message "Permission denied". The files include system directories like /root, /home, /etc, /var, and /usr, as well as specific files like /etc/passwd and /etc/shadow. The terminal window has a dark background and a light-colored text.

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/home/bandit6-git': Permission denied
find: '/home/bandit60-git': Permission denied
find: '/home/bandit6/inhere': Permission denied
find: '/home/bandit62-git': Permission denied
find: '/home/bandit69-git': Permission denied
find: '/home/bandit63-git': Permission denied
find: '/lost+found': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/archive': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/usr/lib/instore': Permission denied
find: '/LibreOfficeWriter/driver': Permission denied
find: '/proc/17358/task/17358/fdinfo/0': No such file or directory
find: '/proc/17358/fdinfo/5': No such file or directory
find: '/cgroup2/csessions': Permission denied
find: '/boot/lost+found': Permission denied
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit1': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit6': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tnp': Permission denied
find: '/var/lib/polkit-1/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/dpkg/info/bandit7.password'
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Level 7:

Password: cvX2JJJa4CFaLtqS87jk27qwqGhBM9plV



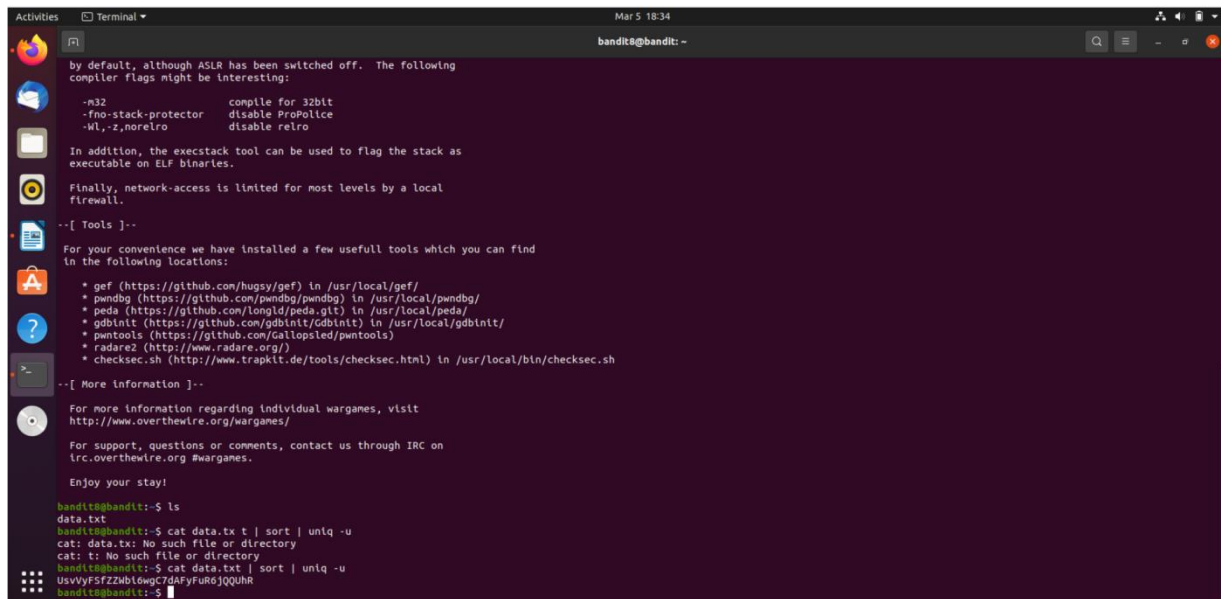
A terminal window titled "bandit7@bandit: -" showing the execution of a strings command. The command is: `bandit7@bandit:~$ strings data.txt | grep "millionth"`. The output shows the password: `cvX2JJJa4CFaLtqS87jk27qwqGhBM9plV`. The terminal window has a dark background and a light-colored text.

```
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth  cvX2JJJa4CFaLtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

Level 8:

Password:

UsvVyFSfZZwbi6wgC7dAFYFur6jQQUhr



A terminal window titled 'bandit8@bandit: ~' showing instructions for Level 8. The text includes information about ASLR, compiler flags, the execstack tool, and a list of installed tools like gef, pwndbg, peda, gdbint, pwn2tools, radare2, and checksec.sh. It also provides links for more information and support.

```
by default, although ASLR has been switched off. The following
compiler flags might be interesting:

-m32                compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro       disable relro

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 usefull tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/longld/peda.git) in /usr/local/peda/
* gdbint (https://github.com/gdbint/gdbint) in /usr/local/gdbint/
* pwn2tools (https://github.com/Gallopsled/pwn2tools)
* radare2 (http://www.radare.org/)
* checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

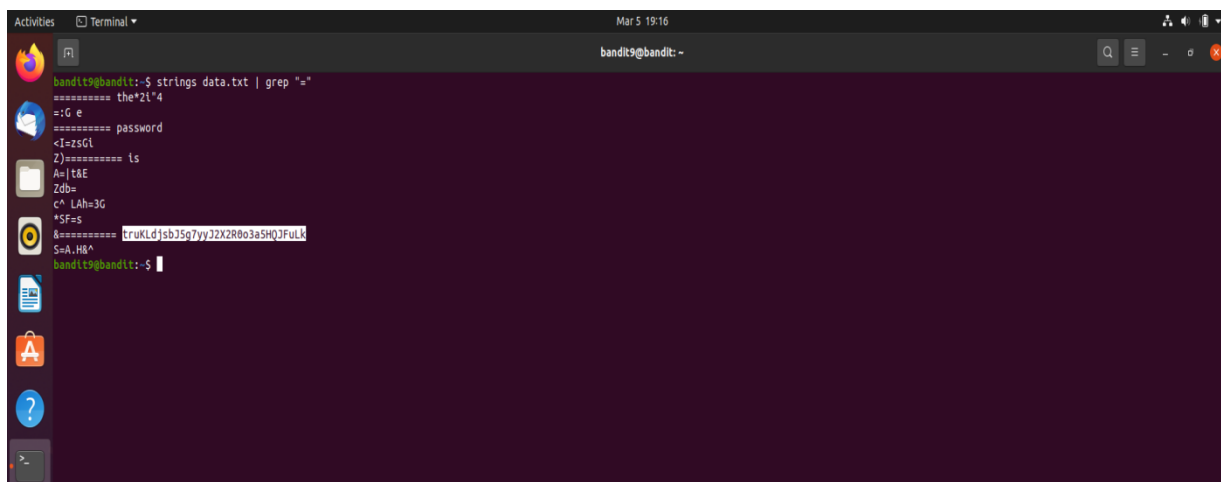
Enjoy your stay!

bandit8@bandit:~$ ls
data.txt
bandit8@bandit:~$ cat data.txt | sort | uniq -u
cat: data.txt: No such file or directory
cat: t: No such file or directory
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZwbi6wgC7dAFYFur6jQQUhr
bandit8@bandit:~$
```

Level 9:

Password:

truKLdJsbj5g7yyJ2X2R0o3a5HqJFuLK



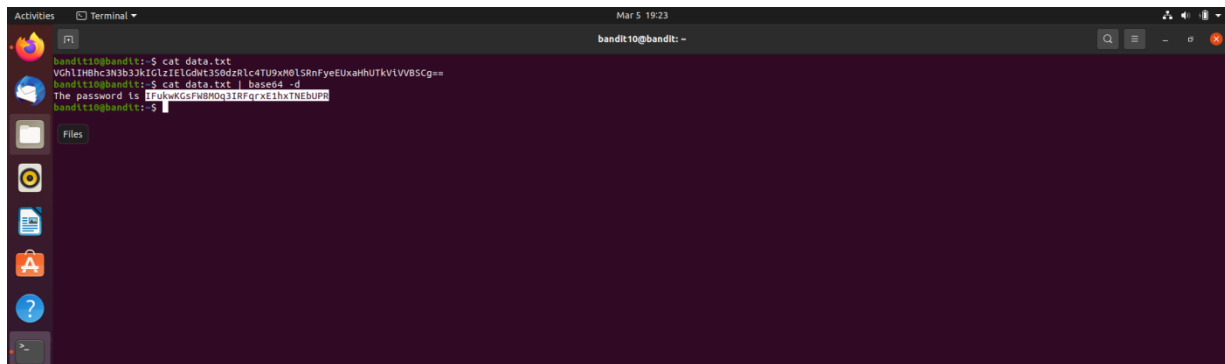
A terminal window titled 'bandit9@bandit: ~' showing the process of extracting the password from data.txt using the strings command and grep. The output shows the password 'truKLdJsbj5g7yyJ2X2R0o3a5HqJFuLK'.

```
bandit9@bandit:~$ strings data.txt | grep "="
===== the*2l*4
=:G e
===== password
<I=zsG!
Z)====== ls
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&===== truKLdJsbj5g7yyJ2X2R0o3a5HqJFuLK
S=A,HA^
bandit9@bandit:~$
```

Level 10:

Password:

IfukwKGsFW8MOq3IRFqrxETNEbUPR

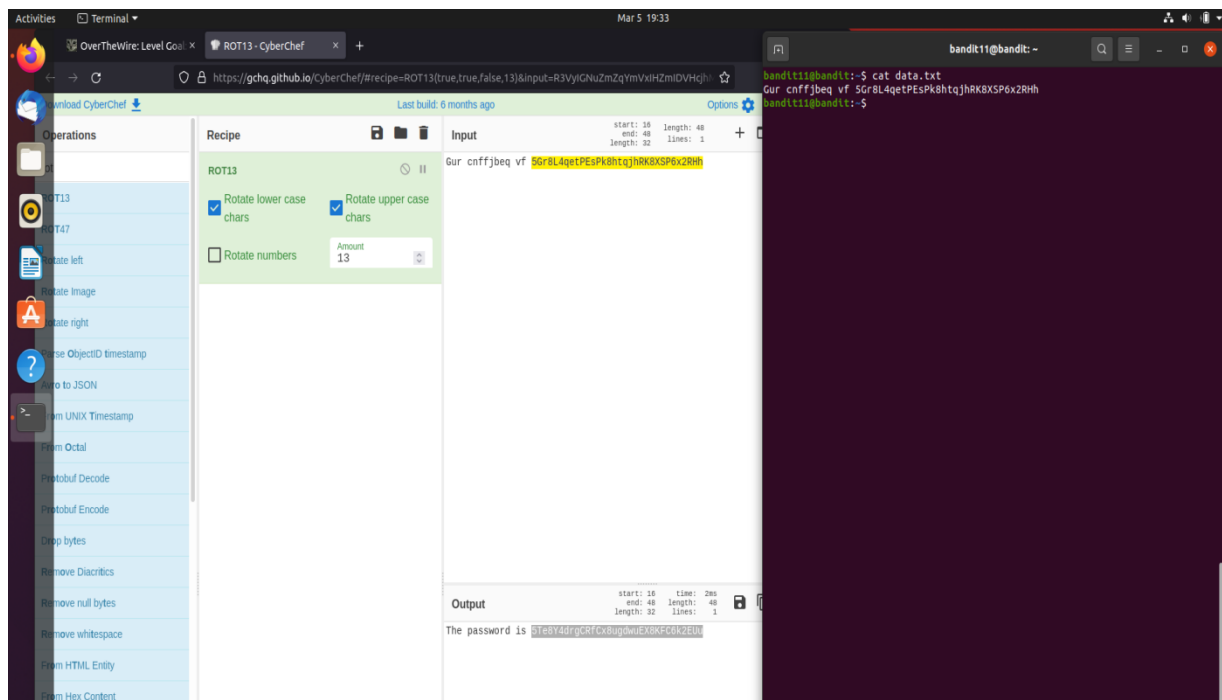
A terminal window titled 'bandit10@bandit: ~' showing the following commands and output:

```
bandit10@bandit:~$ cat data.txt
Vch1IH0hc3N3b3JkIGZlZlElGdWt3S0dzRlc4TU9xM0lSRnFyeEUXahhUTkVlVVB5Cg==
bandit10@bandit:~$ cat data.txt | base64 -d
The password is IfukwKGsFW8MOq3IRFqrxETNEbUPR
bandit10@bandit:~$
```

Level 11:

Password:

5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH

A screenshot showing the CyberChef web application and a terminal window. The CyberChef interface has the 'Recipe' set to 'ROT13' with 'Rotate lower case chars', 'Rotate upper case chars', and 'Amount' set to '13'. The 'Input' field contains the text 'Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH'. The 'Output' field shows the result: 'The password is 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH'. The terminal window on the right shows the following commands and output:

```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHH
bandit11@bandit:~$
```

Level 12:

Password:

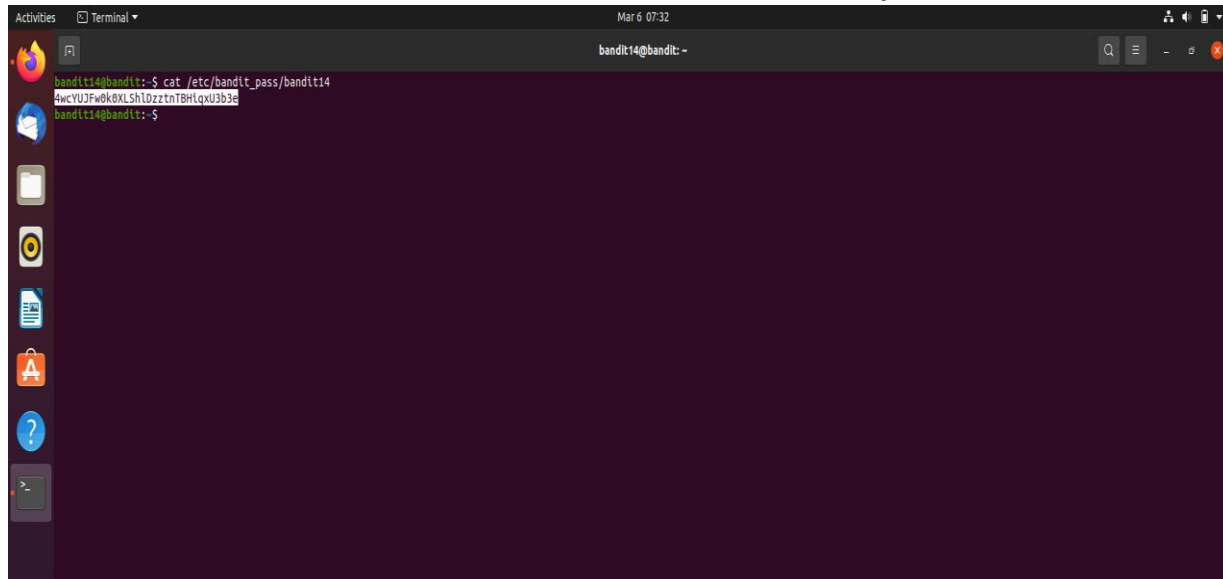
8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL

```
Activities Terminal Mar 6 07:25 bandit12@bandit: /tmp/kaushik

bandit12@bandit:/tmp/kaushik$ xxd -r data.txt > data
bandit12@bandit:/tmp/kaushik$ ls
data data.txt
bandit12@bandit:/tmp/kaushik$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/kaushik$ man gzip
bandit12@bandit:/tmp/kaushik$ mv data file.gz
bandit12@bandit:/tmp/kaushik$ gzip -d file.gz
bandit12@bandit:/tmp/kaushik$ ls
data.txt file
bandit12@bandit:/tmp/kaushik$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/kaushik$ file
Usage: file [-bchiklmprsvzO] [--apple] [--extension] [--mime-encoding] [--mime-type]
[-e testname] [-F separator] [-f namefile] [-m magicfiles] file ...
file -C [-m magicfiles]
file [--help]
bandit12@bandit:/tmp/kaushik$ mv file file.bz2
bandit12@bandit:/tmp/kaushik$ man bzip2
bandit12@bandit:/tmp/kaushik$ bzip2 -d file.bz2
bandit12@bandit:/tmp/kaushik$ ls
data.txt file
bandit12@bandit:/tmp/kaushik$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/kaushik$ mv file file.gz
bandit12@bandit:/tmp/kaushik$ gzip -d file.gz
bandit12@bandit:/tmp/kaushik$ ls
data.txt file
bandit12@bandit:/tmp/kaushik$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kaushik$ mv file file.tar
bandit12@bandit:/tmp/kaushik$ tar xf file.tar
bandit12@bandit:/tmp/kaushik$ ls
data5.bin data.txt file.txt
bandit12@bandit:/tmp/kaushik$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kaushik$ rm file.tar
bandit12@bandit:/tmp/kaushik$ rm data
rm: cannot remove 'data': No such file or directory
bandit12@bandit:/tmp/kaushik$ rm data.txt
bandit12@bandit:/tmp/kaushik$ ls
data5.bin
bandit12@bandit:/tmp/kaushik$ file file
file: cannot open 'file' (No such file or directory)
bandit12@bandit:/tmp/kaushik$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kaushik$ mv data5.bin data.tar
bandit12@bandit:/tmp/kaushik$ tar xf data.tar
bandit12@bandit:/tmp/kaushik$ ls
data6.bin data.tar
bandit12@bandit:/tmp/kaushik$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/kaushik$ mv data6.bin data.bz2
bandit12@bandit:/tmp/kaushik$ bzip2 -d data.bz2
bandit12@bandit:/tmp/kaushik$ ls
data data.tar
bandit12@bandit:/tmp/kaushik$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/kaushik$ mv data data.tar
bandit12@bandit:/tmp/kaushik$ ls
data.tar
bandit12@bandit:/tmp/kaushik$ tar xf data.tar
bandit12@bandit:/tmp/kaushik$ ls
data8.bin data.tar
bandit12@bandit:/tmp/kaushik$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:/tmp/kaushik$ mv data8.bin data.gz
bandit12@bandit:/tmp/kaushik$ gzip -d data.gz
bandit12@bandit:/tmp/kaushik$ ls
data data.tar
bandit12@bandit:/tmp/kaushik$ file data
data: ASCII text
bandit12@bandit:/tmp/kaushik$ cat data
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a10RpYL
bandit12@bandit:/tmp/kaushik$
```

Level 13:

Password:4wcYUJw0k0XLShlDzztnTBHlqxU3b3e

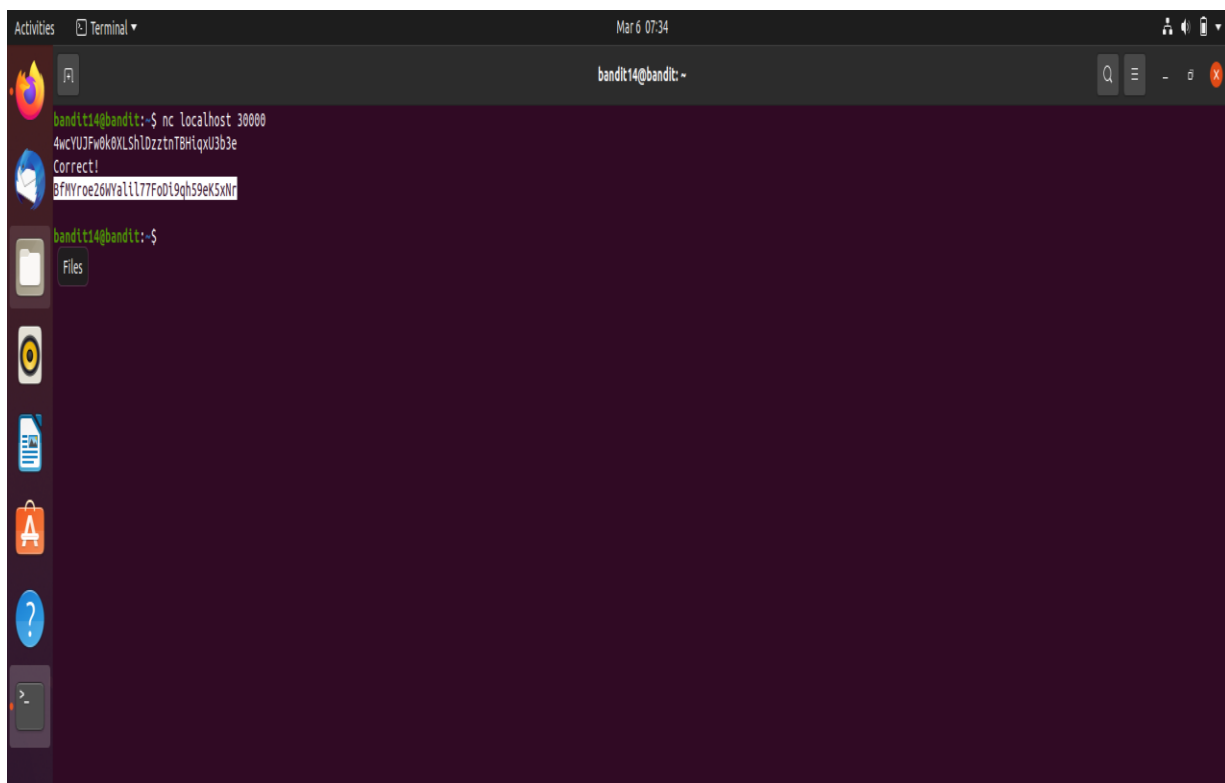
A terminal window titled 'bandit14@bandit: ~' showing the command 'cat /etc/bandit_pass/bandit14' and its output '4wcYUJw0k0XLShlDzztnTBHlqxU3b3e'.

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJw0k0XLShlDzztnTBHlqxU3b3e
bandit14@bandit:~$
```

Level 14:

Password:

BfMYroe26WYalil77FoDi9qh59eK5xNr

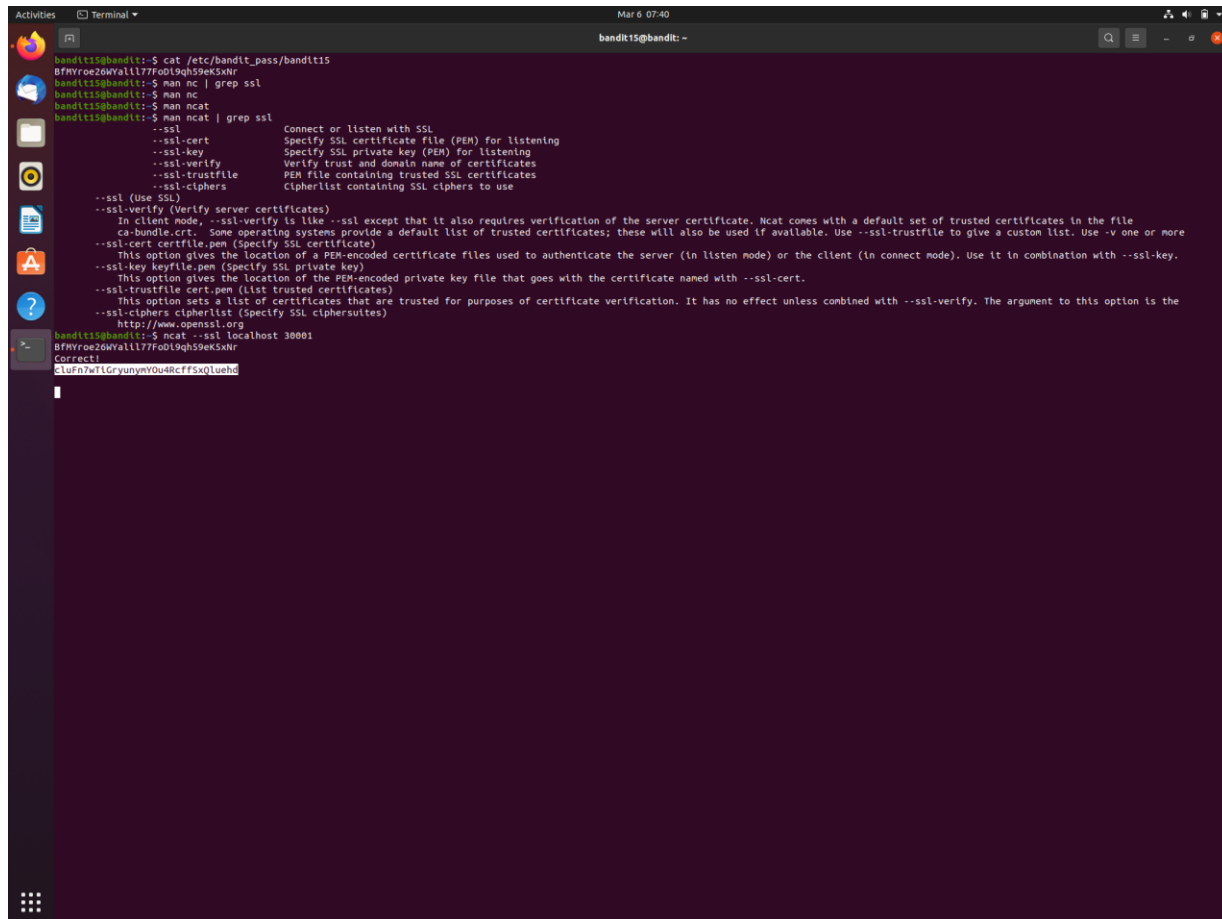
A terminal window titled 'bandit14@bandit: ~' showing a netcat listener on port 30000. It receives a connection from '4wcYUJw0k0XLShlDzztnTBHlqxU3b3e' with the message 'Correct!'. The user then enters the password 'BfMYroe26WYalil77FoDi9qh59eK5xNr' and the prompt returns to '\$'.

```
bandit14@bandit:~$ nc localhost 30000
4wcYUJw0k0XLShlDzztnTBHlqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit14@bandit:~$
```


Level 15:

Password:

clFn7wTiGryunymYOu4RcffSxQluehd



A terminal window titled "Terminal" with a dark background. The user is in a shell as "bandit15@bandit:". The terminal shows the following commands and output:

```
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BfMYroe26WVallll777FoDl9qH59eK5xNr
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ man ncat | grep ssl
--ssl                  Connect or listen with SSL
--ssl-cert             Specify SSL certificate file (PEM) for listening
--ssl-key              Specify SSL private key (PEM) for listening
--ssl-verify           Verify trust and domain name of certificates
--ssl-trustfile        PEM file containing trusted SSL certificates
--ssl-ciphers          Cipherlist containing SSL ciphers to use
--ssl (Use SSL)
--ssl-verify (Verify server certificates)
    In client mode, --ssl-verify is like --ssl except that it also requires verification of the server certificate. Ncat comes with a default set of trusted certificates in the file
    ca-bundle.crt. Some operating systems provide a default list of trusted certificates; these will also be used if available. Use --ssl-trustfile to give a custom list. Use -v one or more
--ssl-cert certfile.pem (Specify SSL certificate)
    This option gives the location of a PEM-encoded certificate files used to authenticate the server (in listen mode) or the client (in connect mode). Use it in combination with --ssl-key.
--ssl-key keyfile.pem (Specify SSL private key)
    This option gives the location of the PEM-encoded private key file that goes with the certificate named with --ssl-cert.
--ssl-trustfile cert.pem (List trusted certificates)
    This option sets a list of certificates that are trusted for purposes of certificate verification. It has no effect unless combined with --ssl-verify. The argument to this option is the
--ssl-ciphers cipherlist (Specify SSL ciphersuites)
    http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 38001
BfMYroe26WVallll777FoDl9qH59eK5xNr
Correct!
clFn7wTiGryunymYOu4RcffSxQluehd
```

