



Lab 4

CS 5-1 - BSCS – Operating System Lab

Name: Sharaiz Ahmed SAP: 57288

Bandit-0

Learn to connect via SSH and read a file to get the next password.

A screenshot of a Kali Linux desktop environment. A terminal window titled "bandit1@bandit: ~" is open, displaying the following text:

```
bandit1@bandit:~$ cat file
cat: file: No such file or directory
bandit1@bandit:~$ ls
readme
bandit1@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: ZjLjTmM6FvvyRnrb2rfNW0ZOTa6ip5If
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

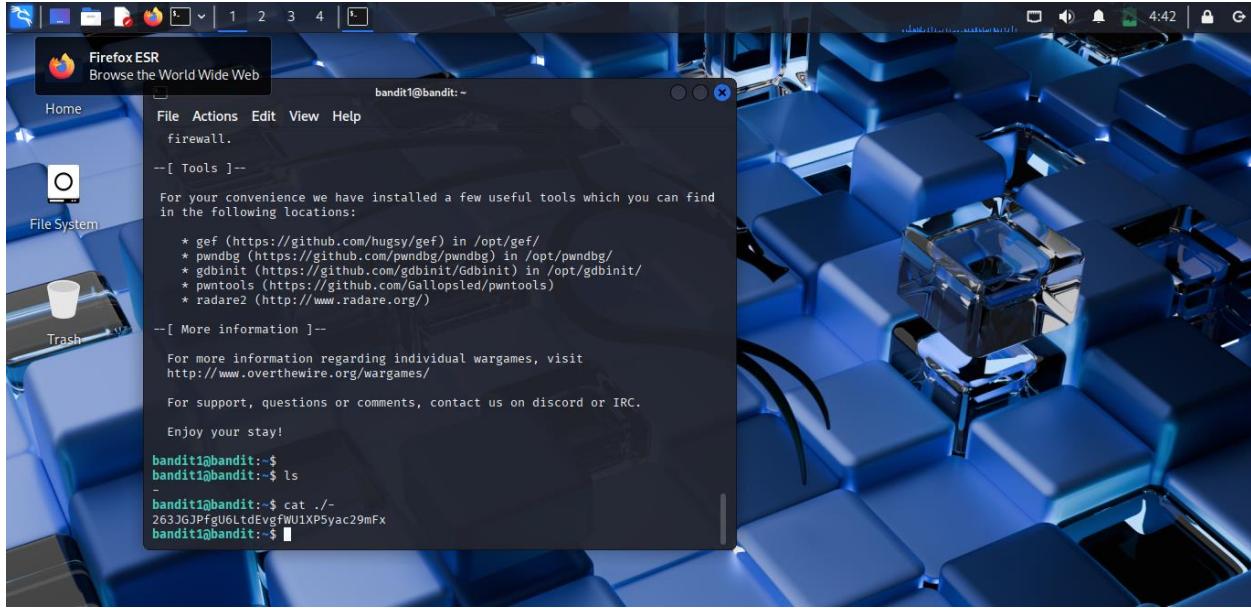
[(kali㉿kali)-[~]]$ ssh -p 2220 bandit1@bandit.labs.overthewire.org
```

The desktop background is a close-up image of a blue keyboard.

Bandit-1

Handle files with tricky names (like -) using proper paths.

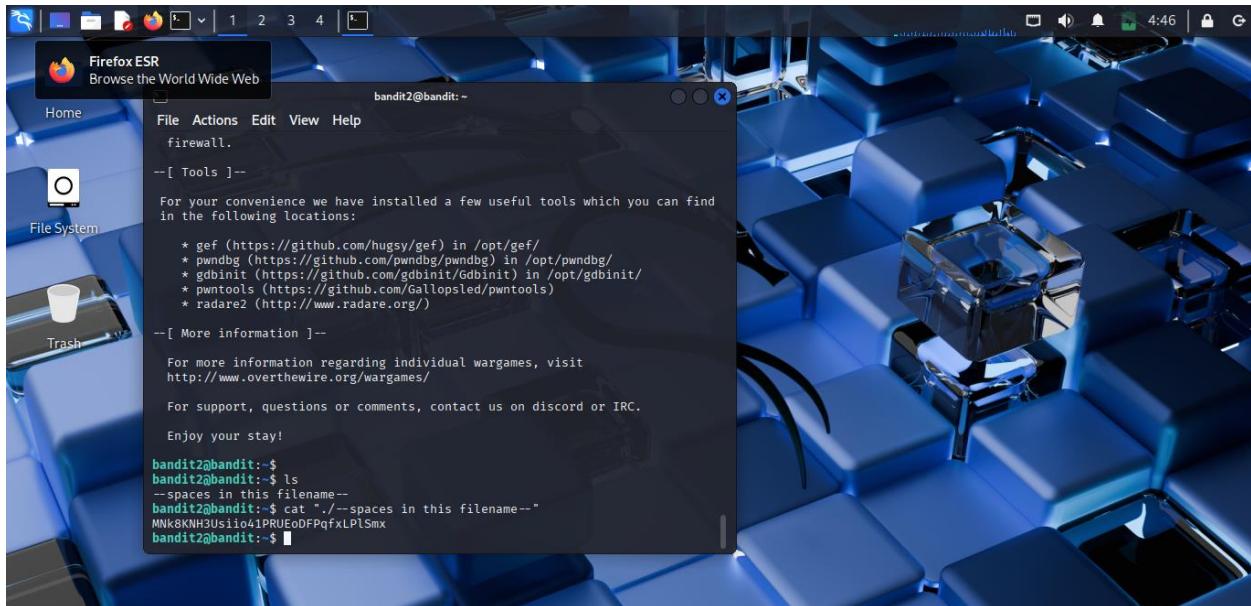
```
cat ./-
```



Bandit-2

Open files with spaces or special characters in their names.

Cat ".--species in this filename--"

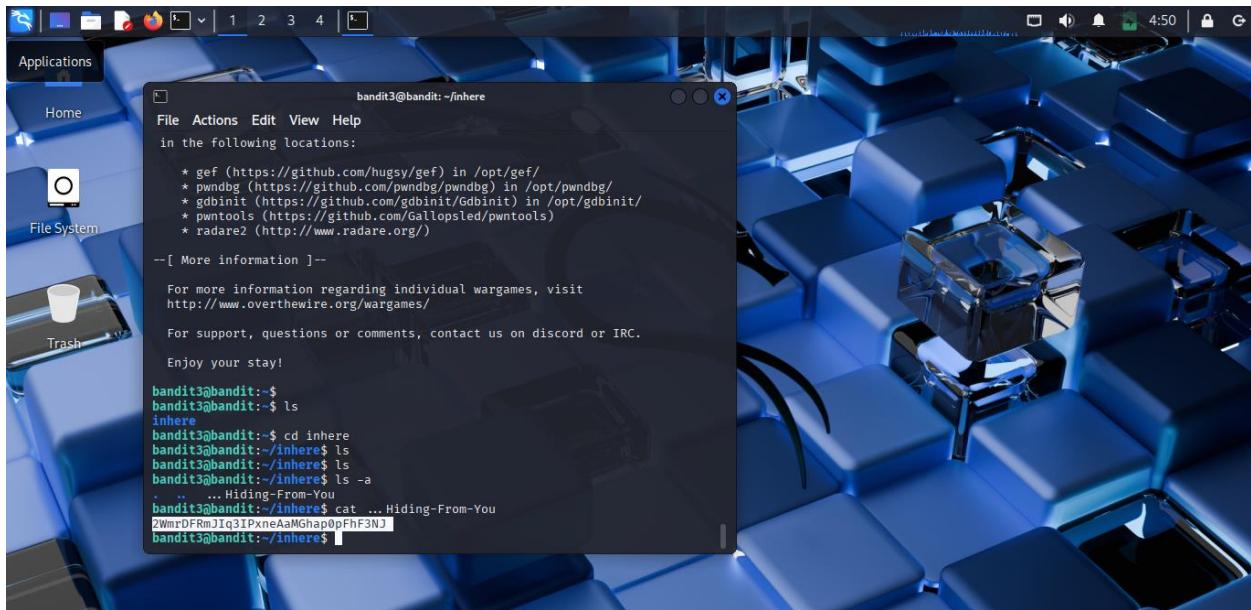


Bandit-3

Discover and read hidden files in a directory.

Cd inhere

Cat ...Hiding-From-You



A terminal window titled "bandit3@bandit: ~/inhere" is displayed. The window shows the following text:

```
File Actions Edit View Help
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/

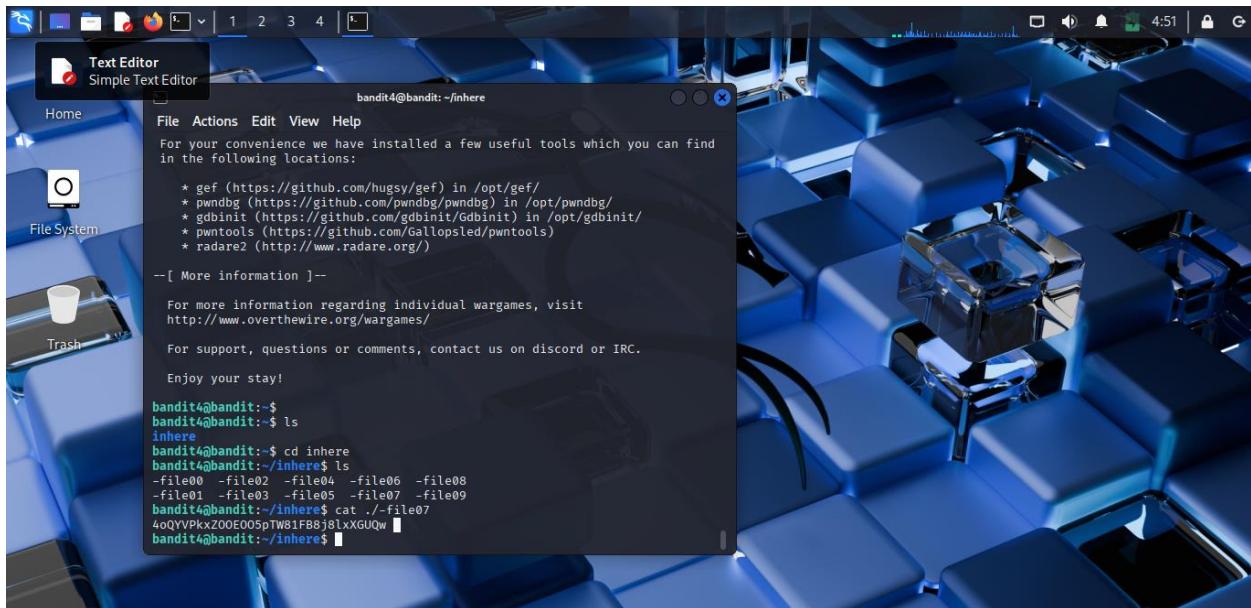
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
inhere
bandit3@bandit:~/inhere$ ./... Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJJtq3IPxneAaMGhap0pFhF3N]
bandit3@bandit:~/inhere$
```

Bandit-4

Search directories to find files with specific properties.



A terminal window titled "bandit4@bandit: ~/inhere" is displayed. The window shows the following text:

```
File Actions Edit View Help
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.

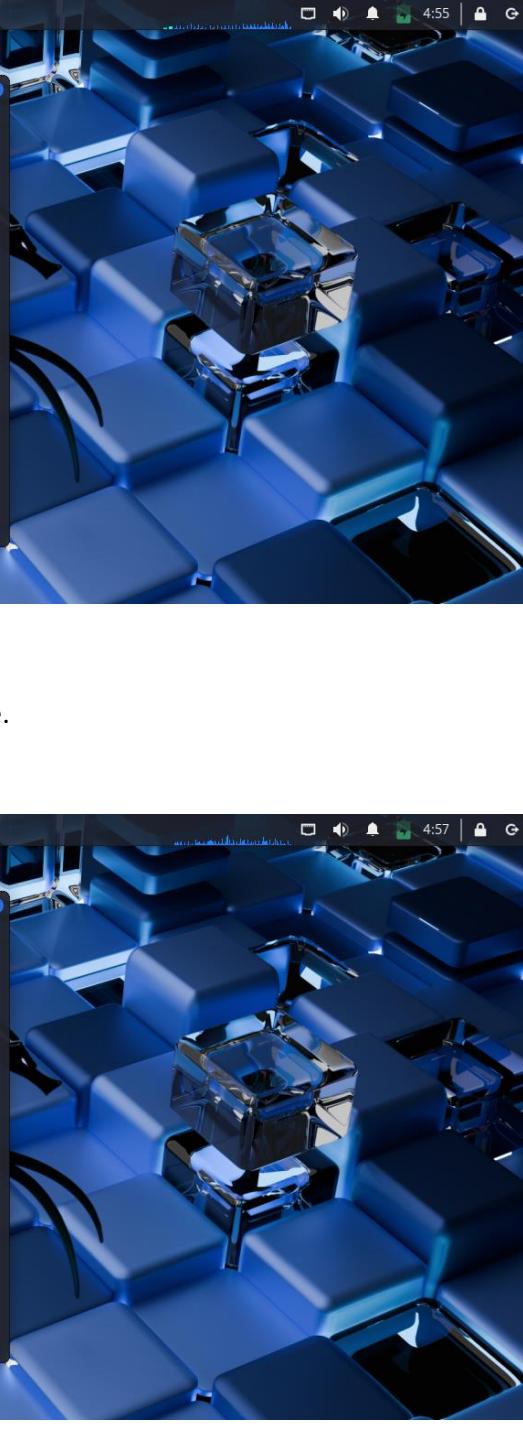
Enjoy your stay!

bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls
inhere
bandit4@bandit:~/inhere$ ./file00 -file02 -file04 -file06 -file08
-file01 -file03 -file05 -file07 -file09
bandit4@bandit:~/inhere$ cat ./file07
4oQVVPkxZ0OE005tW81F88jblxGUQW
bandit4@bandit:~/inhere$
```

Bandit-5

Use `find` to locate a non-executable file of exact size.

```
find . -type f -size 1033c !-executable
```



A screenshot of a terminal window titled "Text Editor Simple Text Editor" running on a Linux desktop environment. The terminal shows a shell session for user "bandit4" on a host named "inhere". The user runs a command to find files owned by "bandit4" and has a size of 1033c, which matches the current file they are viewing. The terminal also displays a message from the OverTheWire wargame site.

```
--[ 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!  
bandit4@bandit:~$  
bandit4@bandit:~$ ls  
inhere  
bandit4@bandit:~$ cd inhere  
bandit4@bandit:~/inhere$ ls  
-file00 -file02 -file04 -file06 -file08  
-file01 -file03 -file05 -file07 -file09  
bandit4@bandit:~/inhere$ cat ./file07  
4oQVVPkxZOOE005pW81FB8j8lxGUQw  
bandit4@bandit:~/inhere$ find . -type f -size 1033c ! -executable  
bandit4@bandit:~/inhere$ find . -type f -size 1033c ! -executable  
bandit4@bandit:~/inhere$ ls  
-file02 -file04 -file06 -file08  
-file01 -file03 -file05 -file07 -file09  
bandit4@bandit:~/inhere$ find . -type f -size 1033c ! -executable  
bandit4@bandit:~/inhere$ cat ./file07  
4oQVVPkxZOOE005pW81FB8j8lxGUQw  
bandit4@bandit:~/inhere$
```

Bandit-6

Find a file owned by a specific user and group with given size.

```
find . -type f -size 1033c !-executable && cat file
```



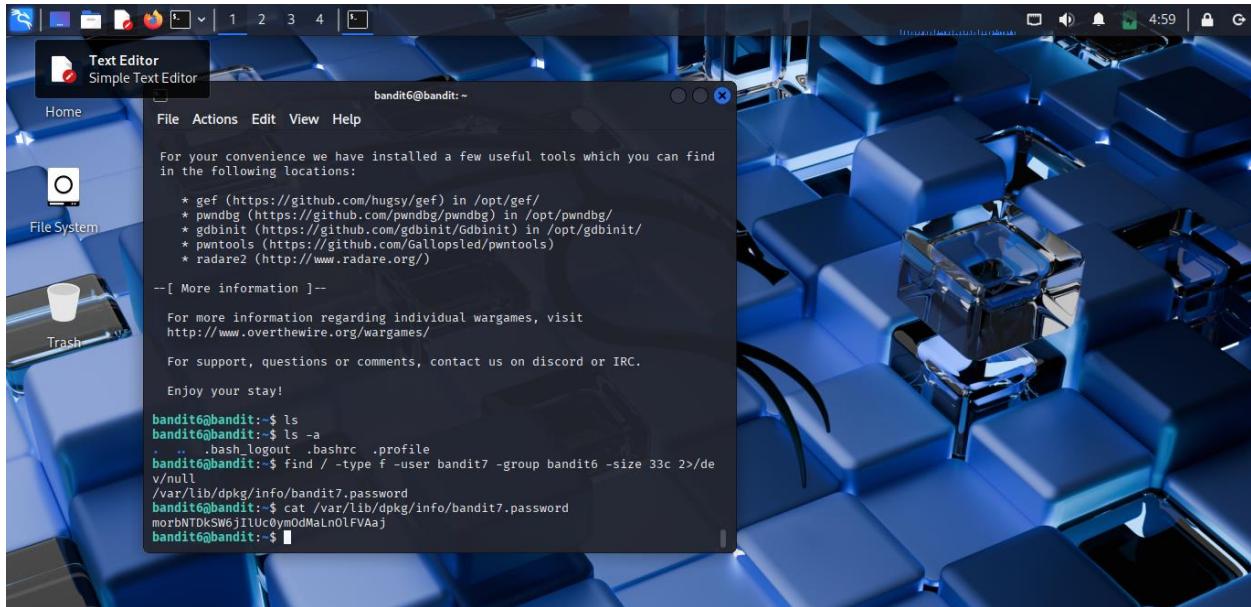
A screenshot of a terminal window titled "Terminal Emulator Use the commandline" running on a Linux desktop environment. The terminal shows a shell session for user "bandit5" on a host named "maybehere07". The user runs a command to find files owned by "bandit5" and has a size of 1033c, which matches the current file they are viewing. The terminal also displays a message from the OverTheWire wargame site.

```
--[ 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!  
bandit5@bandit:~$  
bandit5@bandit:~$ ls  
inhere  
bandit5@bandit:~$ cd inhere  
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable  
.maybehere07/.file2  
bandit5@bandit:~/inhere$ cd maybehere07  
bandit5@bandit:~/inhere/maybehere07$ cat .file2  
HWasnPhtqAVKc0dmk45xy20cvUa6EG
```

Bandit-7

Find a file owned by a specific user and group with given size.

```
find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
```



A terminal window titled "Text Editor" showing a shell session for user "bandit6". The terminal is running on a blue-themed desktop environment. The session starts with a welcome message from the "Simple Text Editor" tool, which includes links to various exploit development tools like gef, pwndbg, gdbinit, pwntools, and radare2. It then shows a standard Linux shell prompt and a command-line session where the user finds a password file in the "/var/lib/dpkg/info/" directory and extracts the password "morbNTDKSw6IIUC0ym0dMaLn0LFVAaj".

```
bandit6@bandit: ~
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/

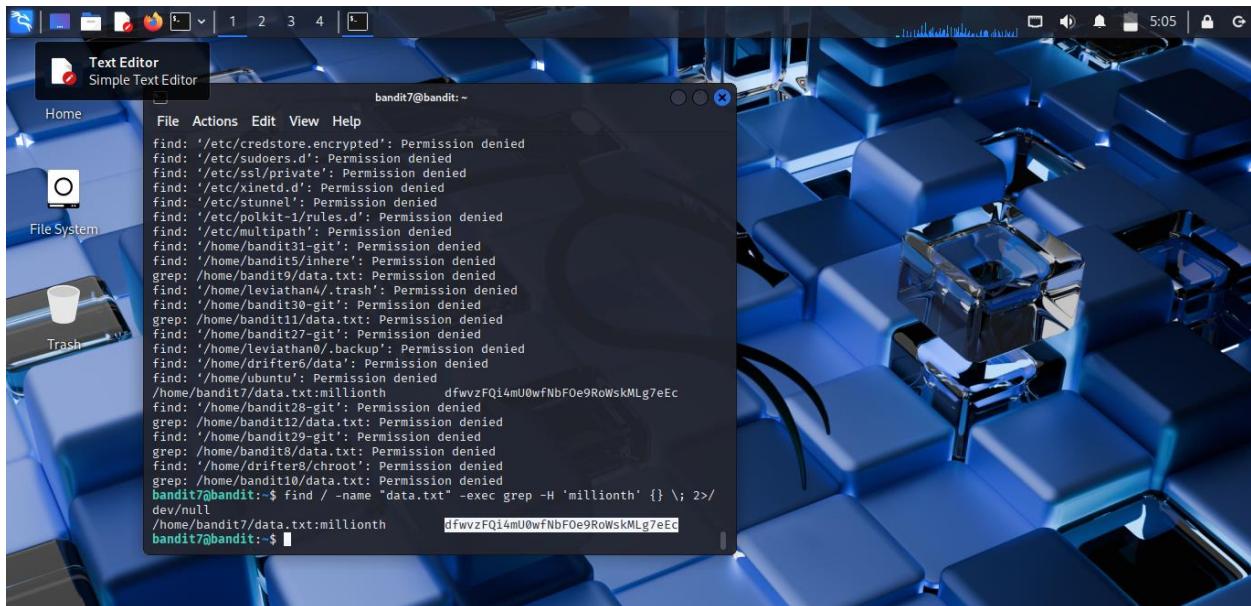
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit6@bandit:~$ ls
bandit6@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
morbNTDKSw6IIUC0ym0dMaLn0LFVAaj
bandit6@bandit:~$
```

Bandit-8

Search a text file for a line containing the keyword millionth.



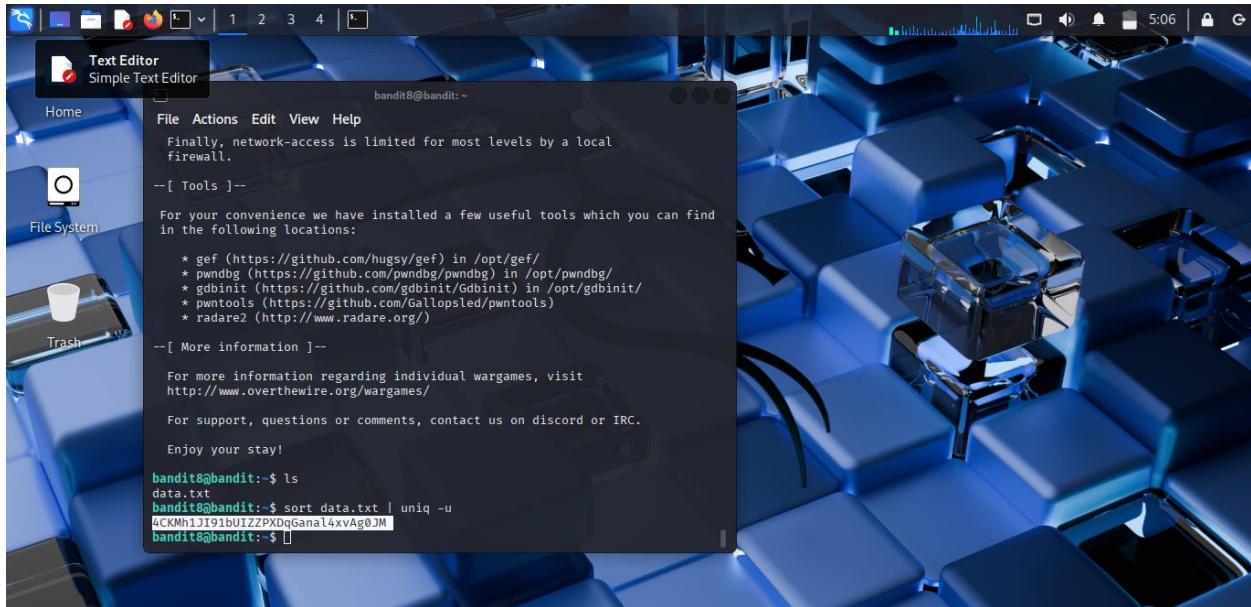
A terminal window titled "Text Editor" showing a shell session for user "bandit7". The terminal is running on a blue-themed desktop environment. The session shows a user attempting to search for the keyword "millionth" in a file named "data.txt" using the "grep" command. The user runs a "find" command to locate "data.txt" and then executes "grep 'millionth'" on it. The output shows the line "dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc" which contains the keyword.

```
bandit7@bandit: ~
find: '/etc/crestore.encrypted': Permission denied
find: '/etc/sudchers.d': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/stunnel': Permission denied
find: '/etc/multipath': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
grep: '/home/bandit9/data.txt': Permission denied
find: '/home/leviathan4/.trash': Permission denied
find: '/home/bandit30-git': Permission denied
grep: '/home/bandit11/data.txt': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/leviathan0/.backup': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/ubuntu': Permission denied
/home/bandit7/data.txt:millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
find: '/home/bandit28-git': Permission denied
grep: '/home/bandit12/data.txt': Permission denied
find: '/home/bandit29-git': Permission denied
grep: '/home/bandit8/data.txt': Permission denied
find: '/home/drifter8/chroot': Permission denied
grep: '/home/bandit10/data.txt': Permission denied
bandit7@bandit:~$ find / -name "data.txt" -exec grep -H 'millionth' {} \; 2>/dev/null
/home/bandit7/data.txt:millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
bandit7@bandit:~$
```

Bandit-9

Identify the only unique line in a large text file.

```
sort data.txt | uniq -u
```



```
bandit8@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/

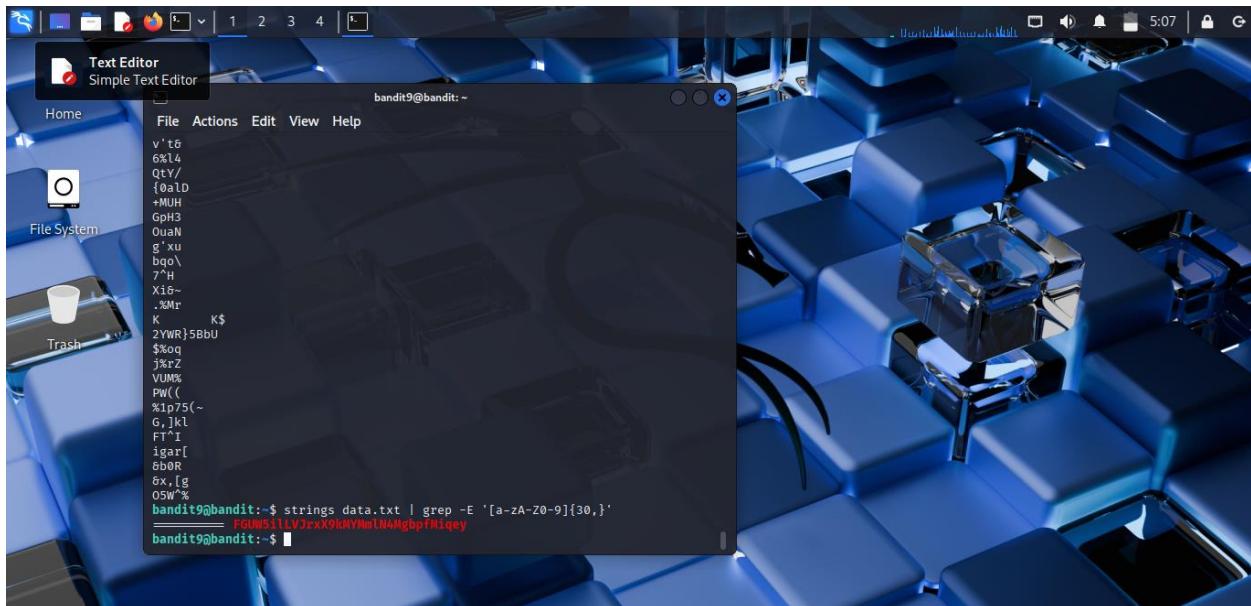
For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
bandit8@bandit: ~ls
data.txt
bandit8@bandit: ~sort data.txt | uniq -u
4CKMh1JJ91buIZZPXQgGana14xvAg0JM
bandit8@bandit: ~
```

Bandit-10

Extract human-readable strings from a binary file.

```
strings data.txt | grep -E '[A-Za-z0-9]{30,}'
```

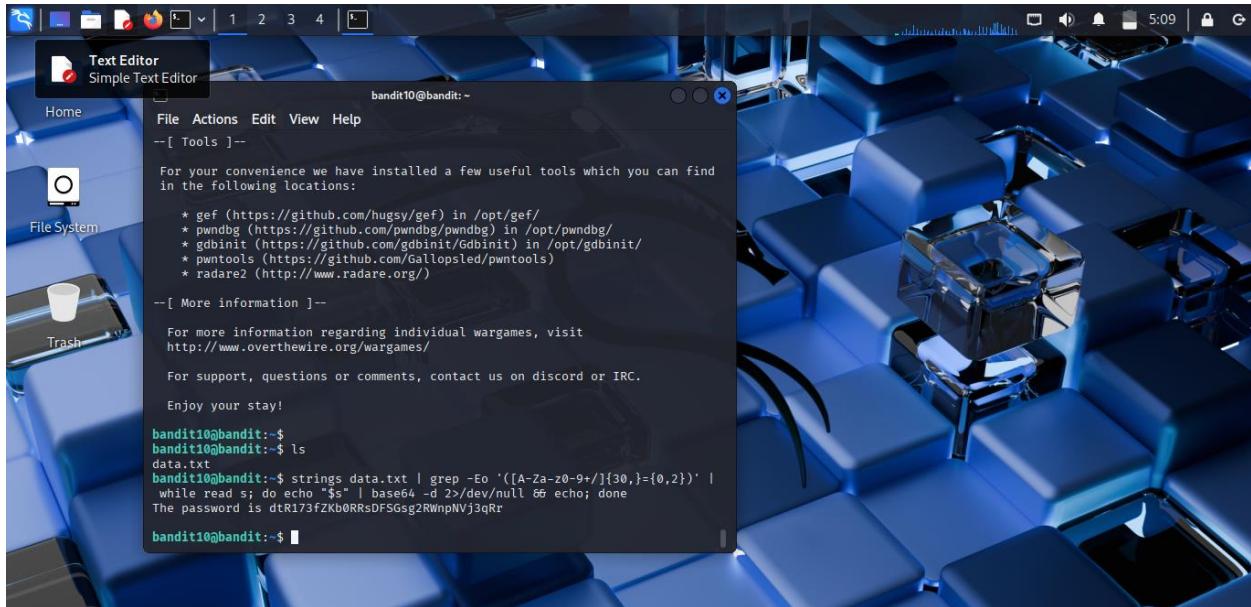


```
bandit9@bandit: ~
v't6
6x14
QtY/
{oaID
+MUH
GpH3
OuaN
g'xu
bqo\
7'H
X16-
%Mr
K      K$
2WWR}5BbU
$2og
jkzZ
VUM%
PW(
%ip75(~
G,]kl
FT'I
igar[
6b0R
0x,lg
OSW%
bandit9@bandit: ~strings data.txt | grep -E '[a-zA-Z0-9]{30,}'
===== FGWWS1LLVJrxX9kNYNm1N4NgbpfMikey
bandit9@bandit: ~
```

Bandit-11

Decode a base64-encoded file to reveal the password.

```
strings data.txt | grep -Eo '([A-Za-z0-9+/]{30,}{0,2})' | while read s; do echo "$s" | base64 -d
2>/dev/null && echo; done
```



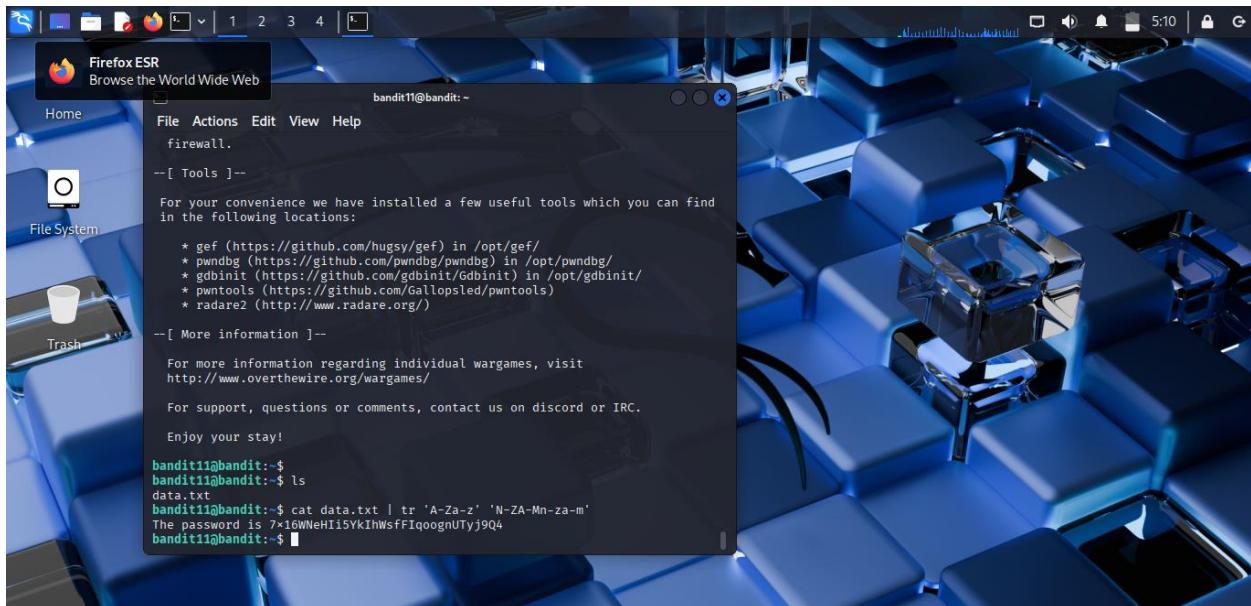
```
Text Editor
Simple Text Editor
bandit10@bandit:~
```

Home File Actions Edit View Help
--[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/
* gobininit (<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:~\$
bandit10@bandit:~\$ ls
data.txt
bandit10@bandit:~\$ strings data.txt | grep -Eo '([A-Za-z0-9+/]{30,}={0,2})' |
while read s; do echo "\$s" | base64 -d >/dev/null && echo; done
The password is dtr173fZKb0RRsDFSGsg2RWnpNVj3qRt
bandit10@bandit:~\$

Bandit-12

Decrypt a ROT13-encoded file using tr

```
cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
```



```
Firefox ESR
Browse the World Wide Web
bandit11@bandit:~
```

Home File Actions Edit View Help
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/
* gobininit (<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:~\$
bandit11@bandit:~\$ ls
data.txt
bandit11@bandit:~\$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHii5YklhWsfFlqoognUTyj9Q4
bandit11@bandit:~\$

7x16WNeHii5YklhWsfFlqoognUTyj9Q4