

23 July, 23

## BYTEWISE FELLOWSHIP CYBERSECURITY

### Bandit Level 0-10

BY: SEERAT E MARRYUM

#### **Bandit Level 0**

##### **Level Goal**

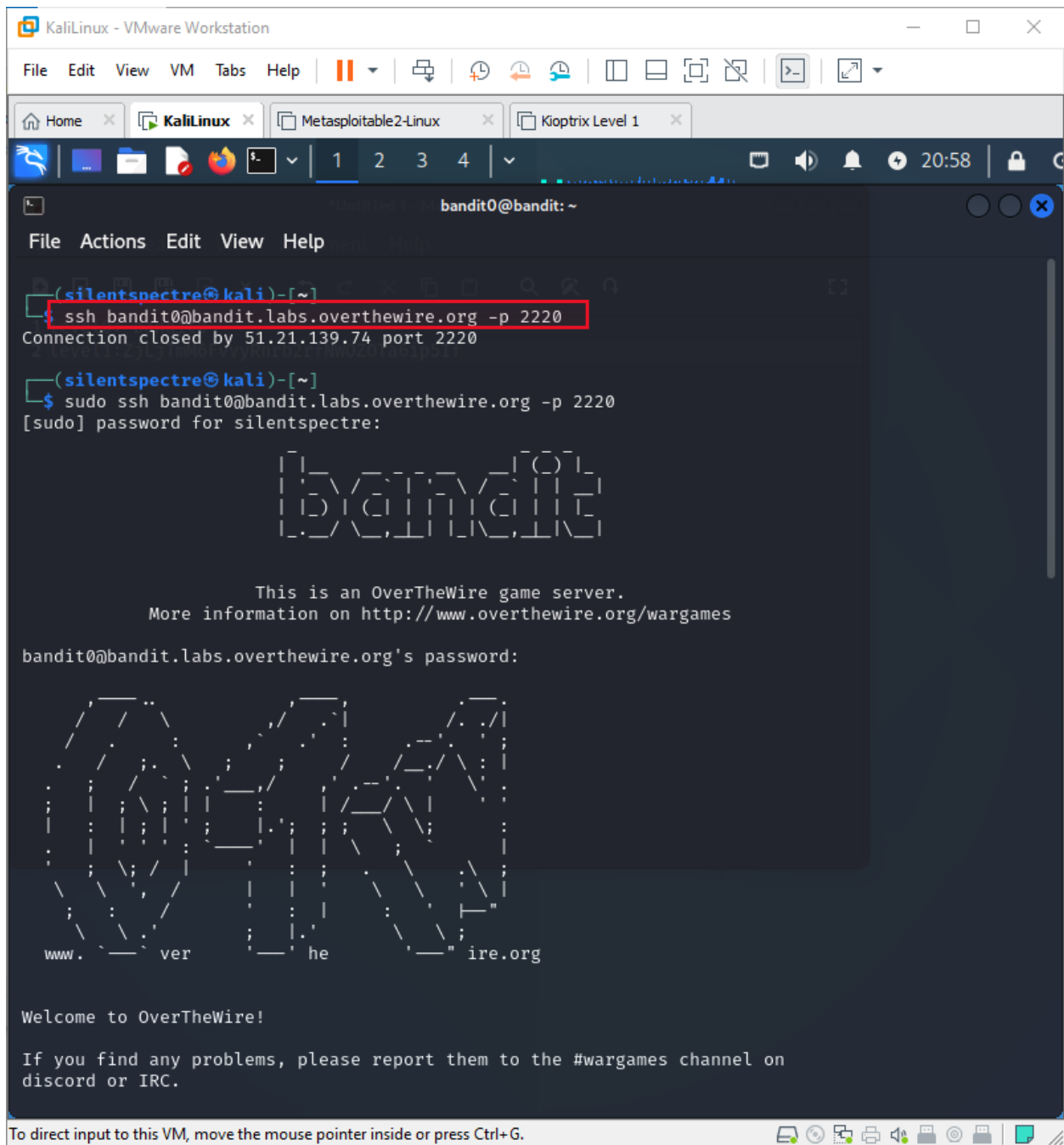
The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org**, on port 2220. The username is **bandit0** and the password is **bandit0**. Once logged in, go to the [Level 1](#) page to find out how to beat Level 1.

##### **Commands you may need to solve this level**

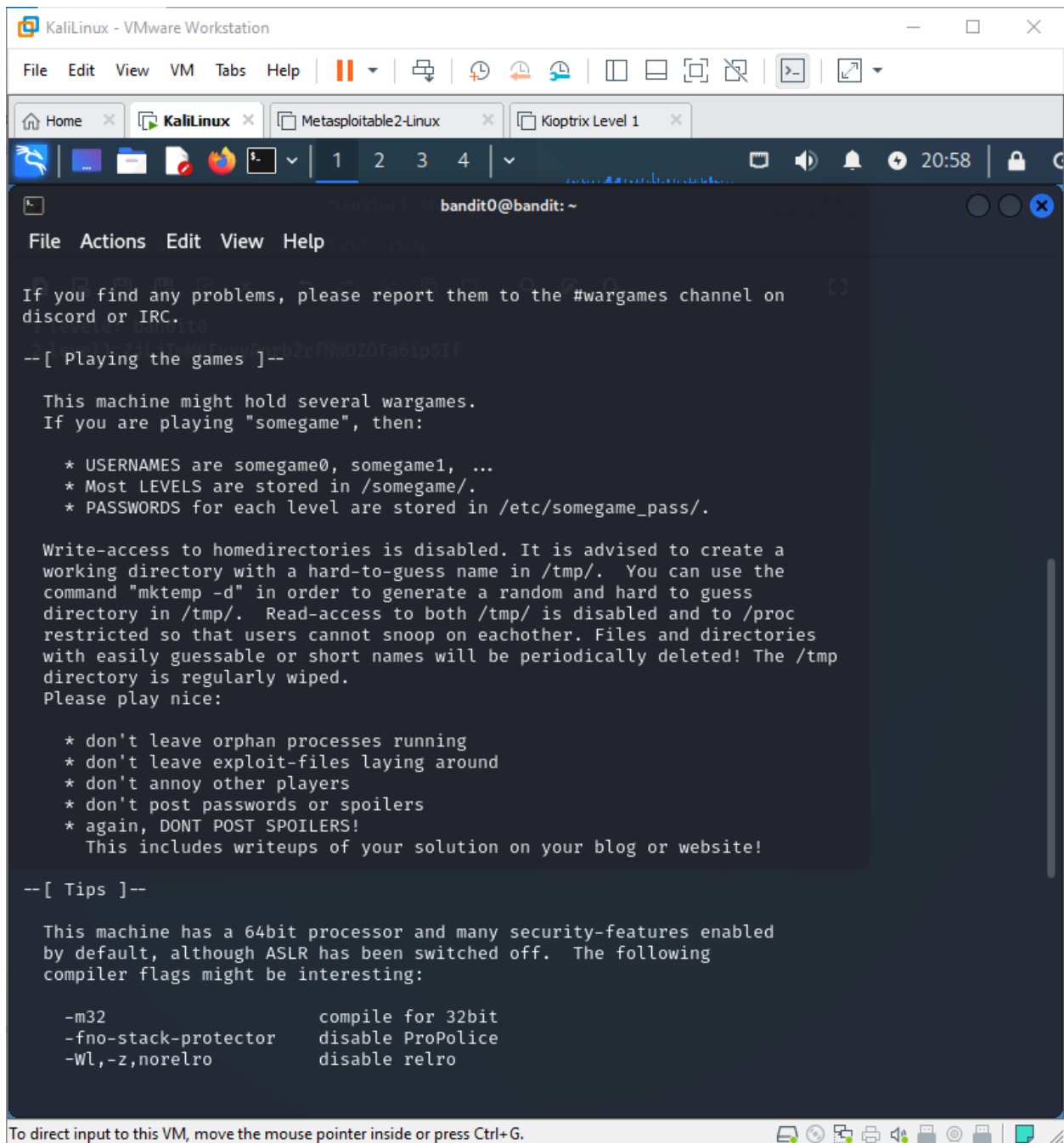
[ssh](#)

Simply login to bandit0 by this command: **ssh [bandit0@bandit.labs.overthewire.org](#) -p 2220**  
and password as **bandit0**:

23 July, 23



23 July, 23



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window is titled 'bandit0@bandit: ~' and displays the following text:

```
File Actions Edit View Help

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/.
* PASSWORDS for each level are stored in /etc/somegame_pass/.

Write-access to homedirectories is disabled. It is advised to create a
working directory with a hard-to-guess name in /tmp/. You can use the
command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc
restricted so that users cannot snoop on eachother. Files and directories
with easily guessable or short names will be periodically deleted! The /tmp
directory is regularly wiped.
Please play nice:

* don't leave orphan processes running
* don't leave exploit-files laying around
* don't annoy other players
* don't post passwords or spoilers
* again, DONT POST SPOILERS!
  This includes writeups of your solution on your blog or website!

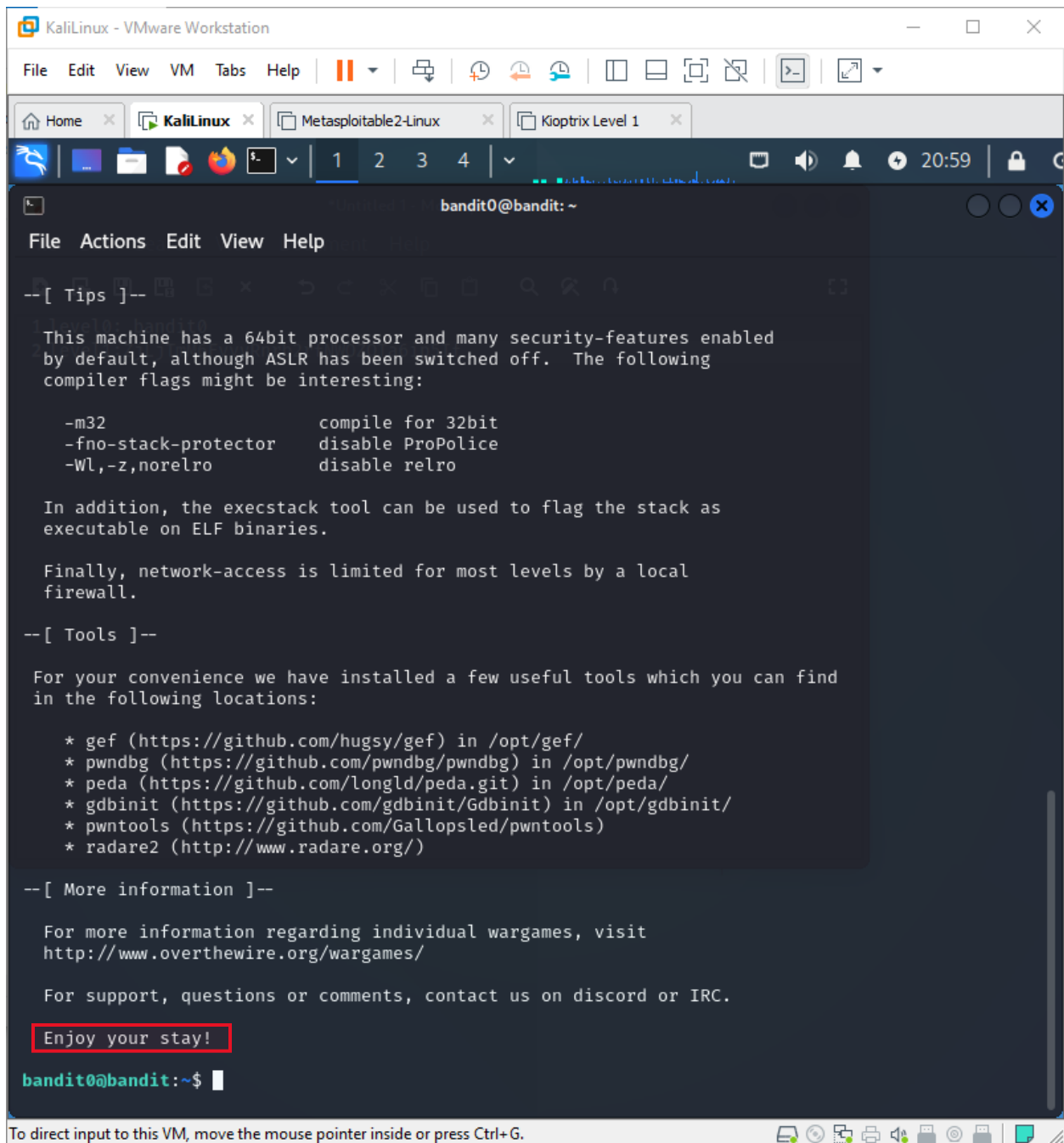
--[ Tips ]--

This machine has a 64bit processor and many security-features enabled
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
```

At the bottom of the window, a status bar reads: 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

23 July, 23



The screenshot shows a Kali Linux VM window titled "KaliLinux - VMware Workstation". The window has a menu bar (File, Edit, View, VM, Tabs, Help) and a toolbar. Below the toolbar is a tab bar with four tabs: "Home", "KaliLinux", "Metasploitable2-Linux", and "Kioptrix Level 1". The "KaliLinux" tab is active. The terminal window shows the prompt "bandit0@bandit: ~". The terminal content includes a "Tips" section with information about the 64-bit processor, security features, and compiler flags (-m32, -fno-stack-protector, -Wl,-z,norelro). It also mentions the execstack tool and network access limitations. A "Tools" section lists several tools and their locations. A "More information" section provides links to wargames and support. The terminal ends with the message "Enjoy your stay!" and the prompt "bandit0@bandit:~\$".

```
bandit0@bandit: ~  
File Actions Edit View Help  
--[ Tips ]--  
This machine has a 64bit processor and many security-features enabled  
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 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/  
* 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!  
bandit0@bandit:~$
```

See the files there by **ls** command and we found readme file, we simple **cat** that file and found the password for next level there:

23 July, 23

```
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
```

## Bandit Level 0 → Level 1

### Level Goal

The password for the next level is stored in a file called **readme** located in the home directory.

Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use

SSH (on port 2220) to log into that level and continue the game.

### Commands you may need to solve this level

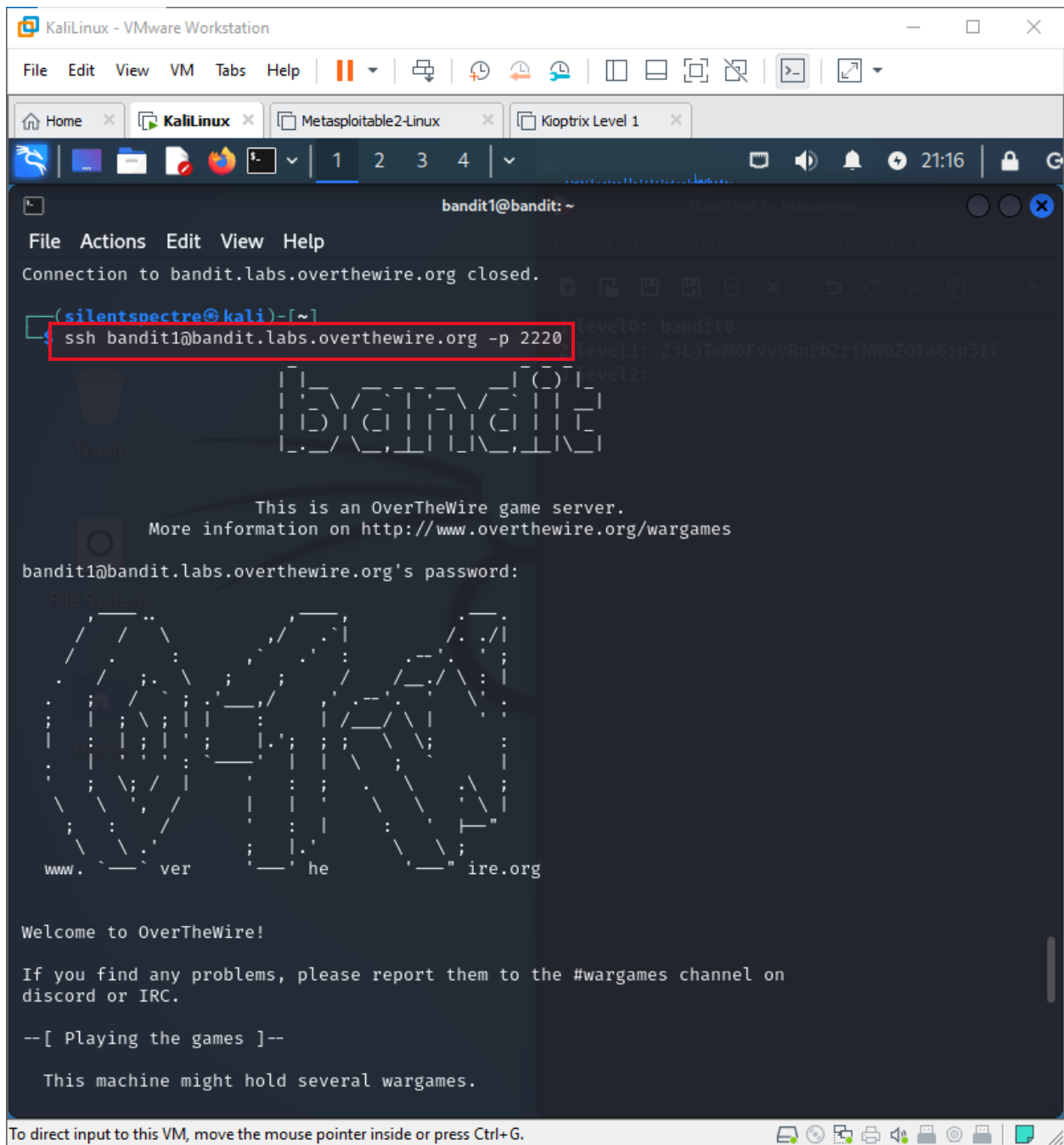
[ls](#) , [cd](#) , [cat](#) , [file](#) , [du](#) , [find](#)

**TIP:** Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start over from bandit0.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, detailed notes are useful to return to where you left off, reference for later problems, or help others after you've completed the challenge.

23 July, 23

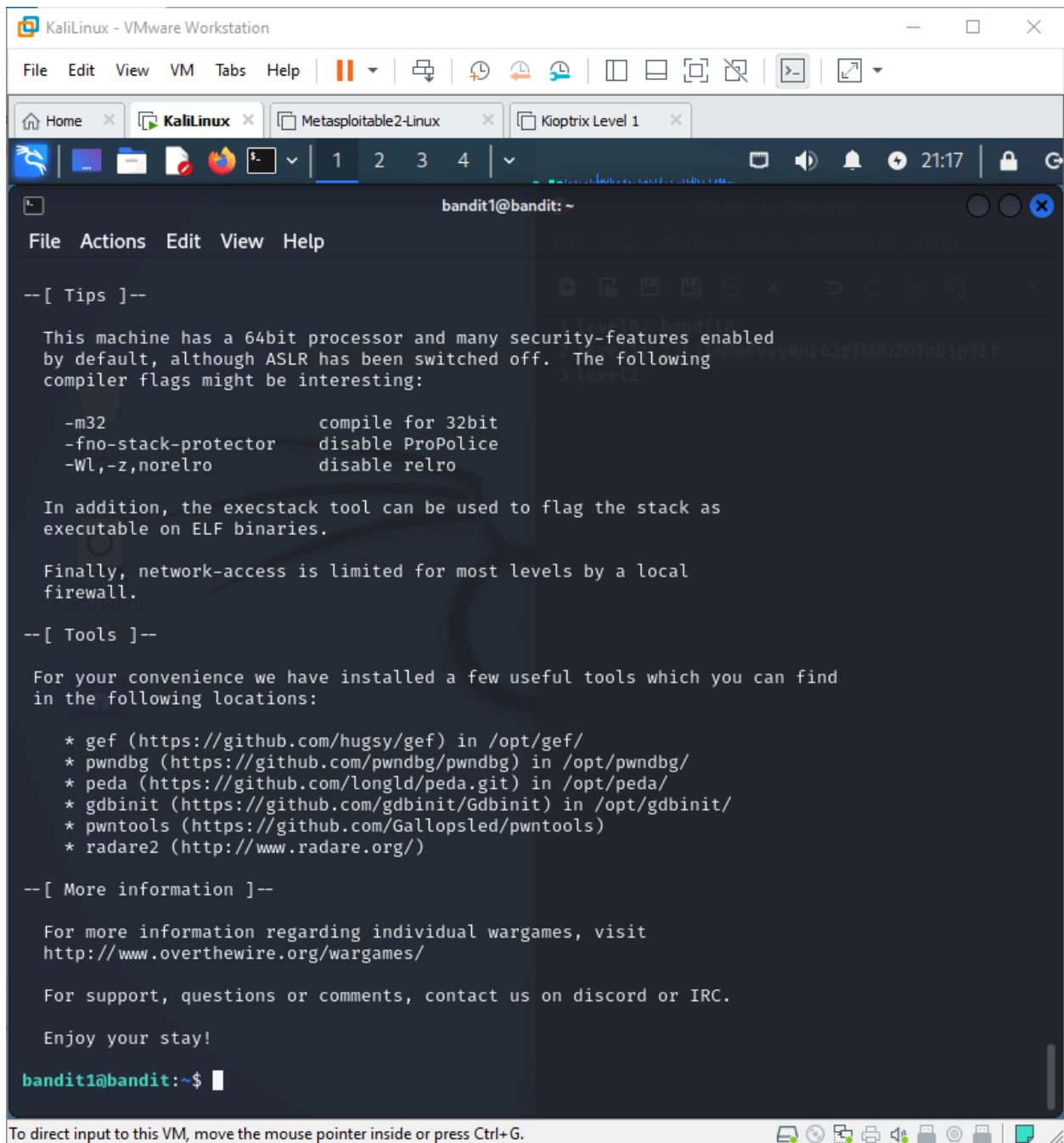


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window displays the following content:

```
bandit1@bandit: ~  
File Actions Edit View Help  
Connection to bandit.labs.overthewire.org closed.  
(silentspectre@kali)-[~]  
$ ssh bandit1@bandit.labs.overthewire.org -p 2220  
level0: bandit0  
level1: 2jLjTnM6FvvyRnrB2rFNW0Z0Ta6ipS1f  
level2:  
bandit1@bandit.labs.overthewire.org's password:  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
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.
```

The terminal output includes ASCII art for 'bandit' and 'OverTheWire'. The bottom of the window shows the VMware status bar with the text: 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

23 July, 23



The screenshot shows a Kali Linux terminal window titled "bandit1@bandit: ~". The terminal displays a welcome message for Bandit Level 1. It includes tips on compiler flags like -m32, -fno-stack-protector, and -Wl,-z,norelro, as well as a list of installed tools like gef, pwndbg, peda, gdbinit, pwntools, and radare2. The prompt "bandit1@bandit:~\$" is visible at the bottom.

```
bandit1@bandit: ~
File Actions Edit View Help

--[ Tips ]--

This machine has a 64bit processor and many security-features enabled
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 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/
* 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:~$
```

## Bandit Level 1 → Level 2

### Level Goal

The password for the next level is stored in a file called - located in the home directory

### Commands you may need to solve this level

ls , cd , cat , file , du , find

23 July, 23

When you run **ls -alps**, you'll get a detailed list of all files and directories in the current directory, including **hidden** ones, with their sizes in blocks and directories marked with a /

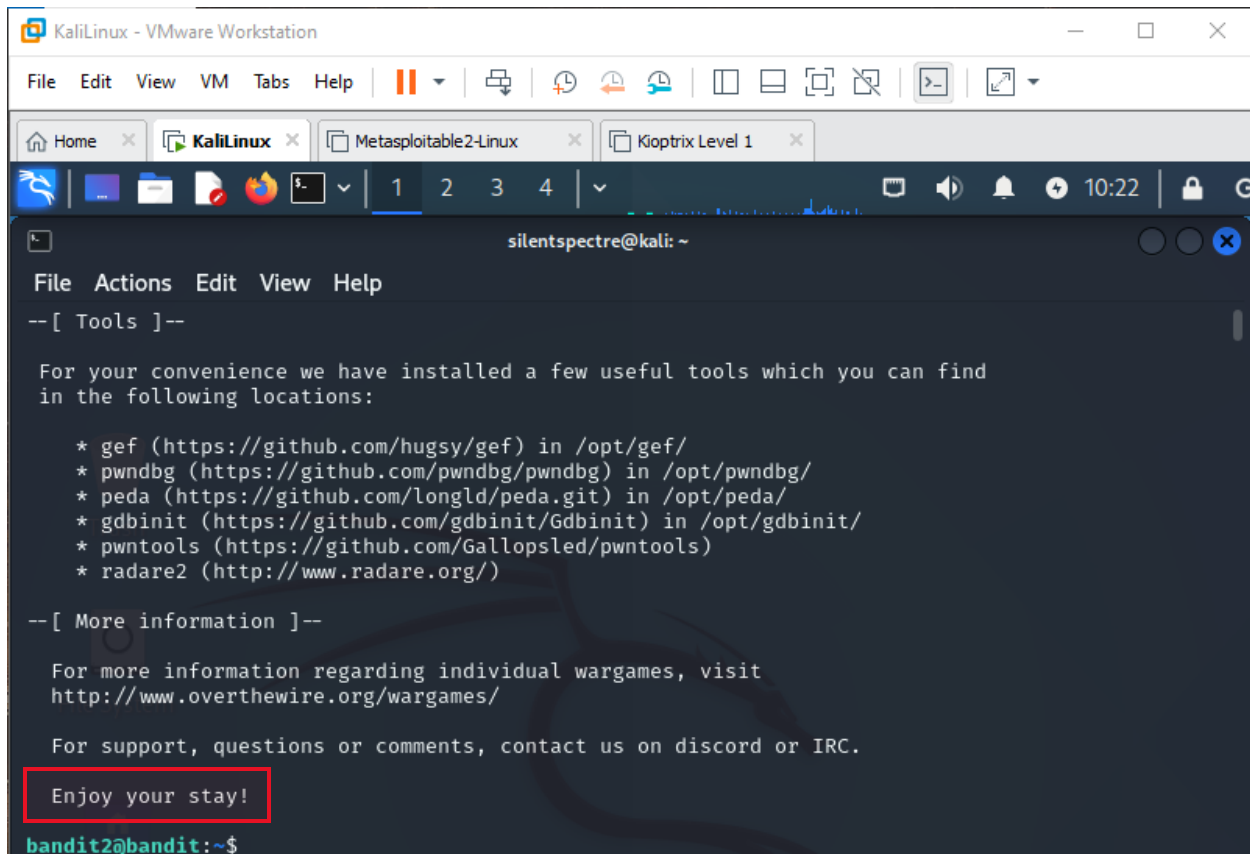
Here I found the file -, cat it and we get the password for next level:

```
bandit1@bandit:~$ ls -alps
total 24
4 -rw-r----- 1 bandit2 bandit1 33 Jun 20 04:07 -
4 drwxr-xr-x 2 root root 4096 Jun 20 04:07 ./
4 drwxr-xr-x 70 root root 4096 Jun 20 04:08 ../
4 -rw-r--r-- 1 root root 220 Mar 31 08:41 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 08:41 .bashrc
4 -rw-r--r-- 1 root root 807 Mar 31 08:41 .profile
bandit1@bandit:~$ cat ./-
263JGJPfG6U6LtdEvgfWU1XP5yac29mFv
```

[illegible]



23 July, 23



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
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/
* 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!
bandit2@bandit:~$
```

## Bandit Level 2 → Level 3

### Level Goal

The password for the next level is stored in a file called **spaces in this filename** located in the home directory

### Commands you may need to solve this level

[ls](#) , [cd](#) , [cat](#) , [file](#) , [du](#) , [find](#)

Run **ls -alps**, to get a detailed list of all files and directories in the current directory, including hidden ones, with their sizes in blocks and directories marked with a /. Here I found the file named: **spaces in this filename**, cat it by this command: **cat spaces\ in\ this\ filename**, if we have a file named spaces in this filename, we would use the **backslash before each space** to

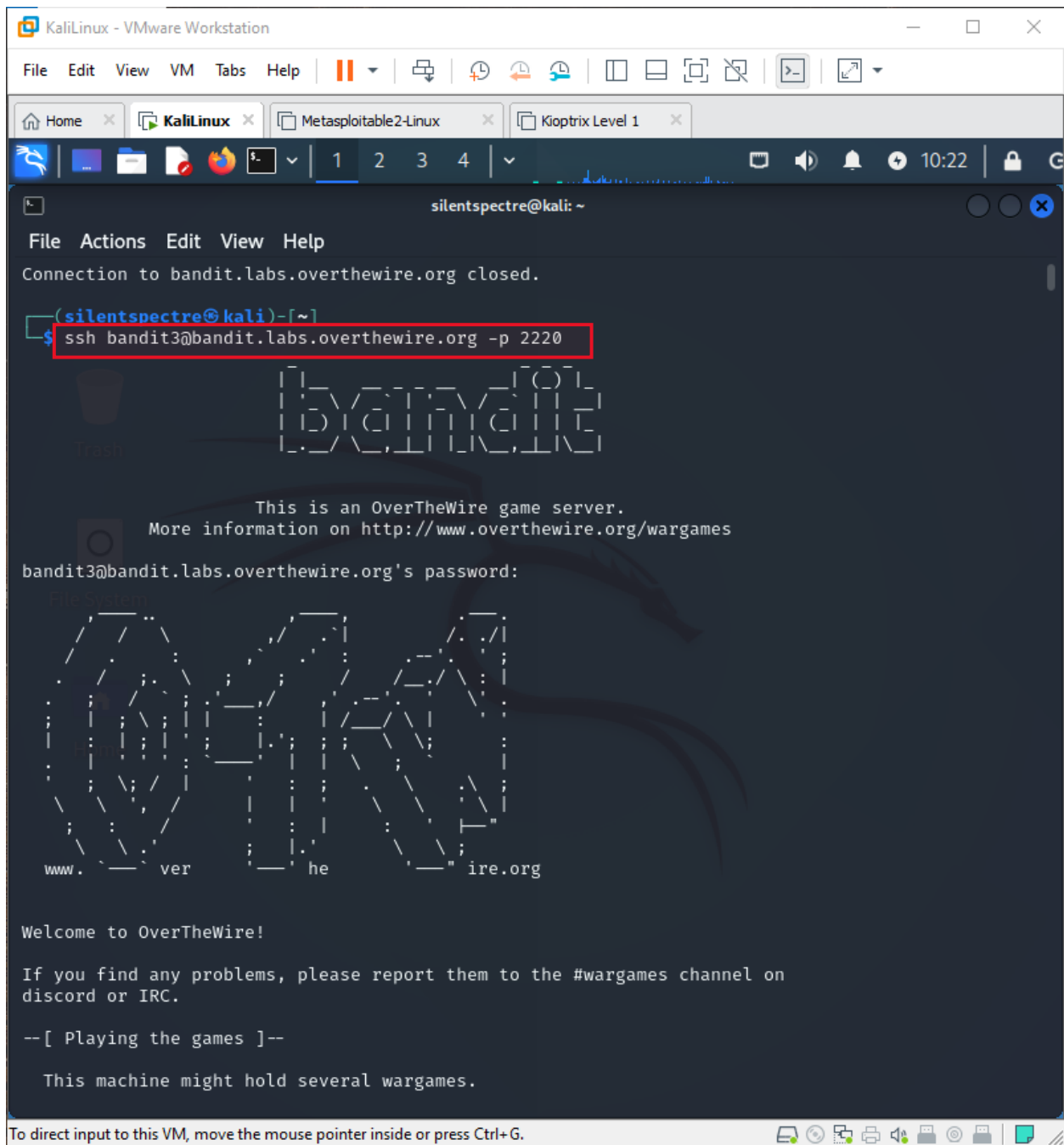
23 July, 23

escape them. This tells the shell to treat the spaces as part of the filename rather than as separators between different arguments and now we get the password in this file:

```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root    4096 Jun 20 04:07 ./
4 drwxr-xr-x 70 root    root    4096 Jun 20 04:08 ../
4 -rw-r--r--  1 root    root     220 Mar 31 08:41 .bash_logout
4 -rw-r--r--  1 root    root   3771 Mar 31 08:41 .bashrc
4 -rw-r--r--  1 root    root     807 Mar 31 08:41 .profile
4 -rw-r----- 1 bandit3 bandit2 33 Jun 20 04:07 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
bandit2@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

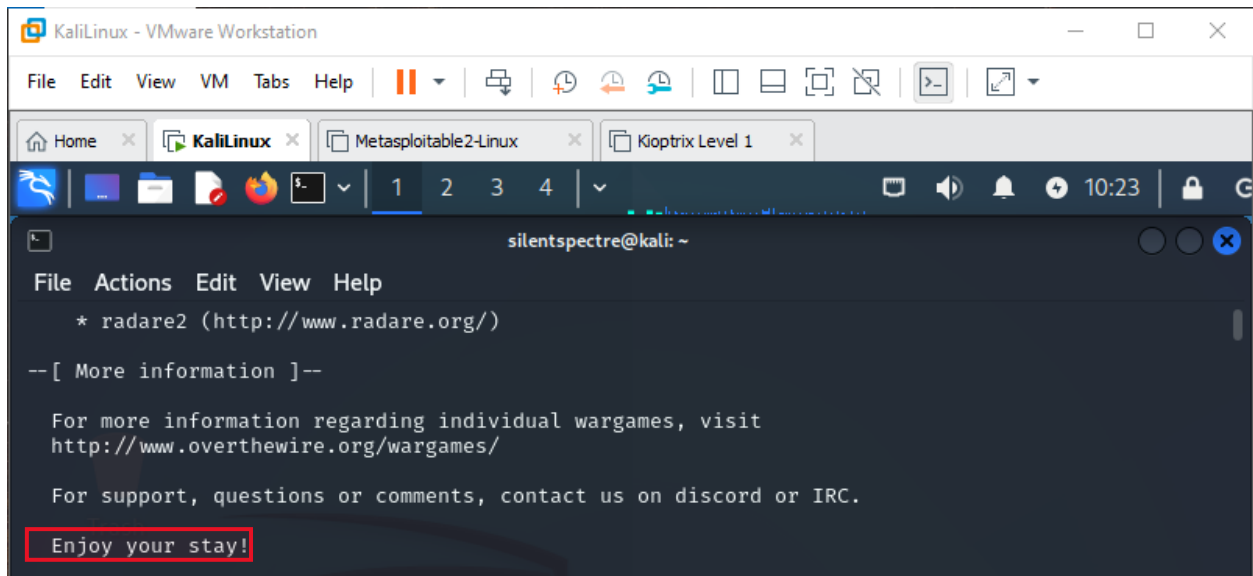
└─(silentspectre@kali)-[~]
```

23 July, 23



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Connection to bandit.labs.overthewire.org closed.
(silentspectre@kali)-[~]
$ ssh bandit3@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit3@bandit.labs.overthewire.org's password:
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.
```

23 July, 23



## Bandit Level 3 → Level 4

### Level Goal

The password for the next level is stored in a hidden file in the **inhere** directory.

### Commands you may need to solve this level

[ls](#) , [cd](#) , [cat](#) , [file](#) , [du](#) , [find](#)

When we see detailed list of files and directories in home we found **inhere** directory, go there and list the files there, we found a file named: **...Hiding-From-You** and reading this file give us password to next level:

23 July, 23

```
bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 Jun 20 04:07 ./
4 drwxr-xr-x 70 root root 4096 Jun 20 04:08 ../
4 -rw-r--r-- 1 root root 220 Mar 31 08:41 .bash_logout
4 -rw-r--r-- 1 root root 3771 Mar 31 08:41 .bashrc
4 drwxr-xr-x 2 root root 4096 Jun 20 04:07 inhere/
4 -rw-r--r-- 1 root root 807 Mar 31 08:41 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Jun 20 04:07 .
drwxr-xr-x 3 root root 4096 Jun 20 04:07 ..
-rw-r----- 1 bandit4 bandit3 33 Jun 20 04:07 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat .hidden
cat: .hidden: No such file or directory
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Jun 20 04:07 .
drwxr-xr-x 3 root root 4096 Jun 20 04:07 ..
-rw-r----- 1 bandit4 bandit3 33 Jun 20 04:07 ... Hiding-From-You
bandit3@bandit:~/inhere$ cat ... Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ ^C
bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

23 July, 23

The screenshot shows a Kali Linux terminal window with the following content:

```

silentspectre@kali: ~
File Actions Edit View Help
(silentspectre@kali)~$ ssh bandit4@bandit.labs.overthewire.org -p 2220
OverTheWire

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

bandit4@bandit.labs.overthewire.org's password:
www.OverTheWire.org

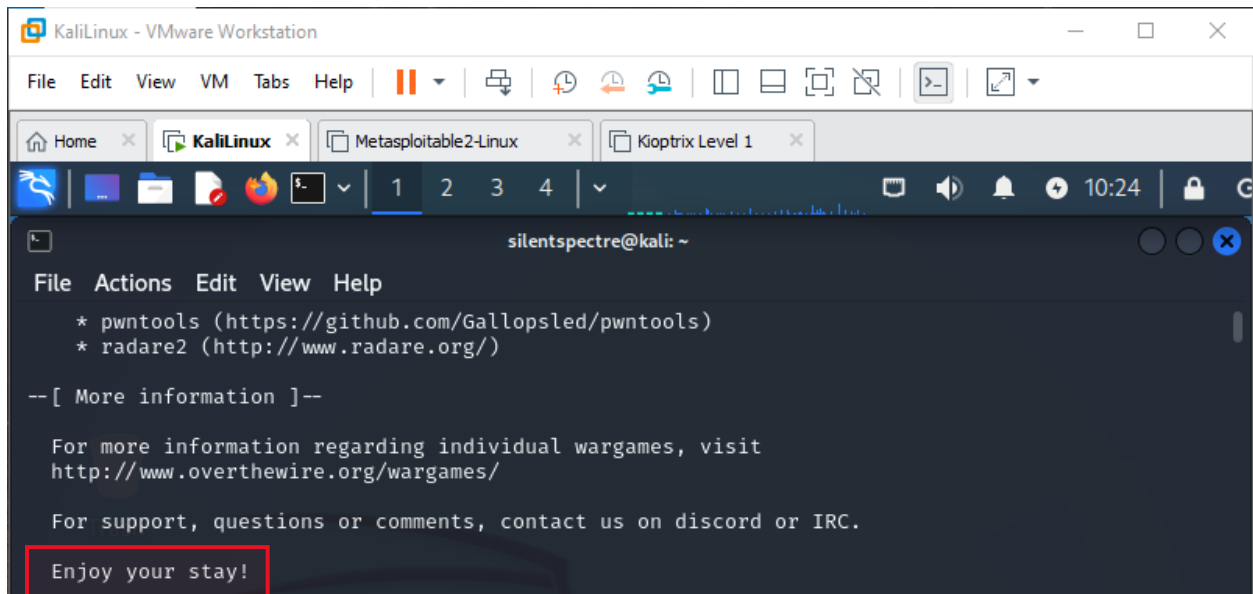
Welcome to OverTheWire!

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:
  
```

23 July, 23



## Bandit Level 4 → Level 5

### Level Goal

The password for the next level is stored in the only human-readable file in the **inhere** directory.

Tip: if your terminal is messed up, try the “reset” command.

### Commands you may need to solve this level

[ls](#) , [cd](#) , [cat](#) , [file](#) , [du](#) , [find](#)

go to inhere directory and search for files that are human readable, find all regular files in the

current directory and its subdirectories, and then determine their file types using the file

command: **find .type f | xargs file**. The only human readable file here is file07 so we read it and

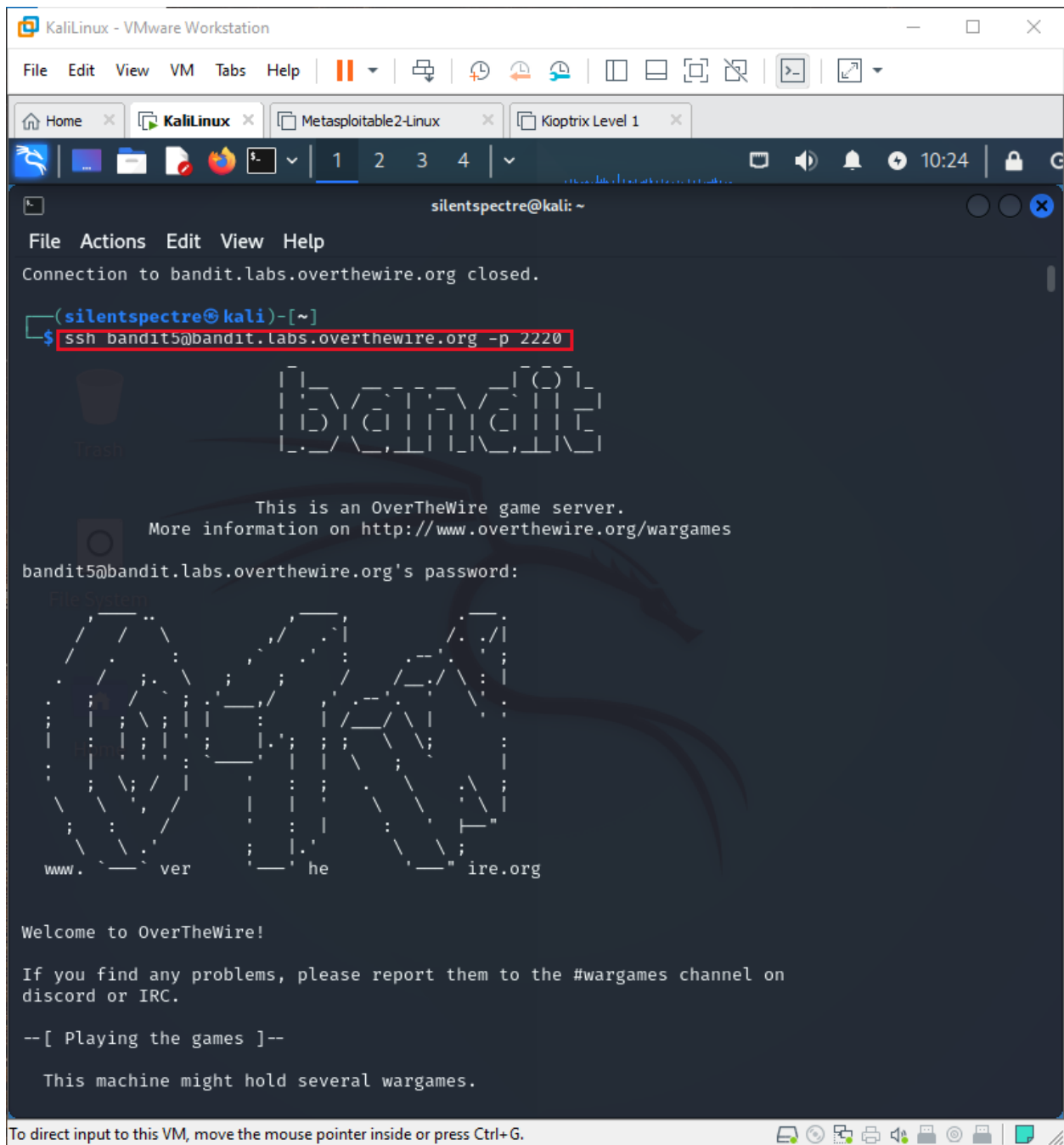
it shows the password for next level:

23 July, 23

```
bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 Jun 20 04:07 ./
4 drwxr-xr-x 70 root root 4096 Jun 20 04:08 ../
4 -rw-r--r--  1 root root  220 Mar 31 08:41 .bash_logout
4 -rw-r--r--  1 root root 3771 Mar 31 08:41 .bashrc
4 drwxr-xr-x  2 root root 4096 Jun 20 04:07 inhere/
4 -rw-r--r--  1 root root  807 Mar 31 08:41 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file08: data
./-file06: data
./-file09: data
./-file01: data
./-file03: data
./-file04: data
./-file00: data
./-file07: ASCII text
./-file05: data
./-file02: data
bandit4@bandit:~/inhere$ man xargs
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZ00E005pTW81FB8j8LxXGUQw
bandit4@bandit:~/inhere$ exit
logout
```



23 July, 23

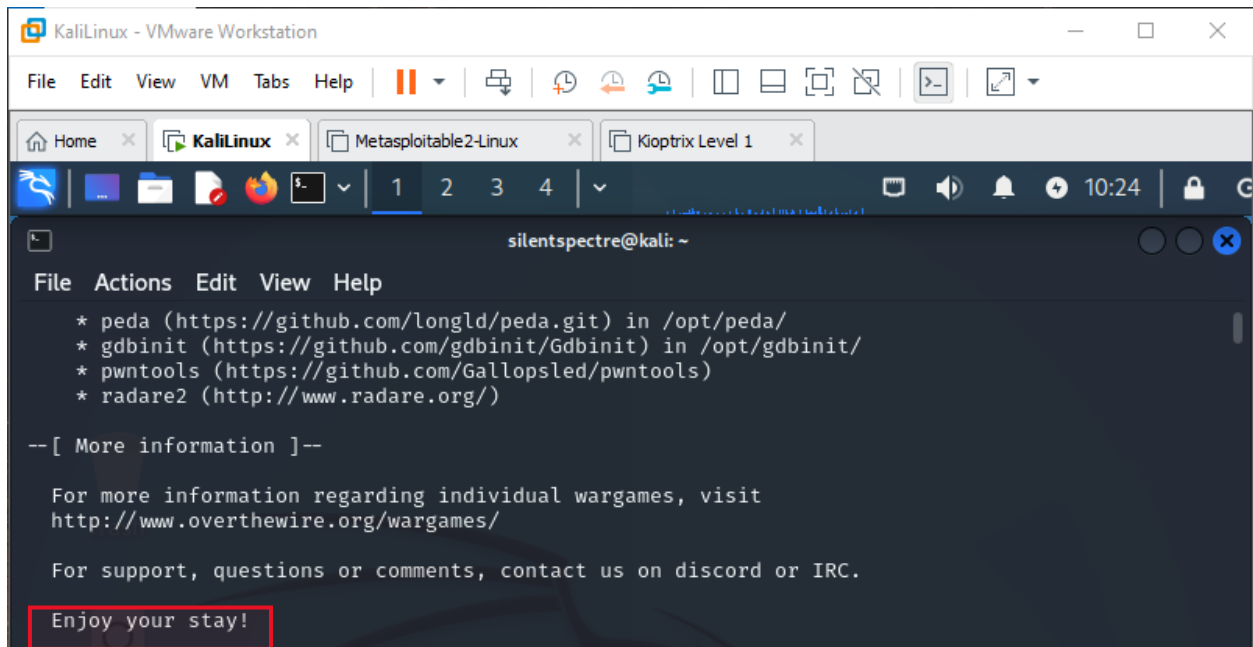


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window is titled 'silentspectre@kali: ~'. It displays the output of an SSH command: `ssh bandit5@bandit.labs.overthewire.org -p 2220`. The terminal output includes a message about the connection to `bandit.labs.overthewire.org` being closed, followed by the prompt `(silentspectre@kali)-[~]`. The user then runs the SSH command, which results in a connection to `bandit5@bandit.labs.overthewire.org`. The terminal displays a large ASCII art logo for 'OverTheWire' and a message: 'This is an OverTheWire game server. More information on <http://www.overthewire.org/wargames>'. Below this, it asks for the password of `bandit5@bandit.labs.overthewire.org`. The terminal then displays another large ASCII art logo for 'OverTheWire' and a welcome message: 'Welcome to OverTheWire!'. It also provides instructions on how to report problems and mentions that the machine might hold several wargames.

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Connection to bandit.labs.overthewire.org closed.
(silentspectre@kali)-[~]
$ ssh bandit5@bandit.labs.overthewire.org -p 2220
bandit5@bandit.labs.overthewire.org's password:
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit5@bandit.labs.overthewire.org's password:
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.
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

23 July, 23



## Bandit Level 5 → Level 6

### Level Goal

The password for the next level is stored in a file somewhere under the **inhere** directory and has all of the following properties:

- human-readable
- 1033 bytes in size
- not executable

### Commands you may need to solve this level

ls , cd , cat , file , du , find

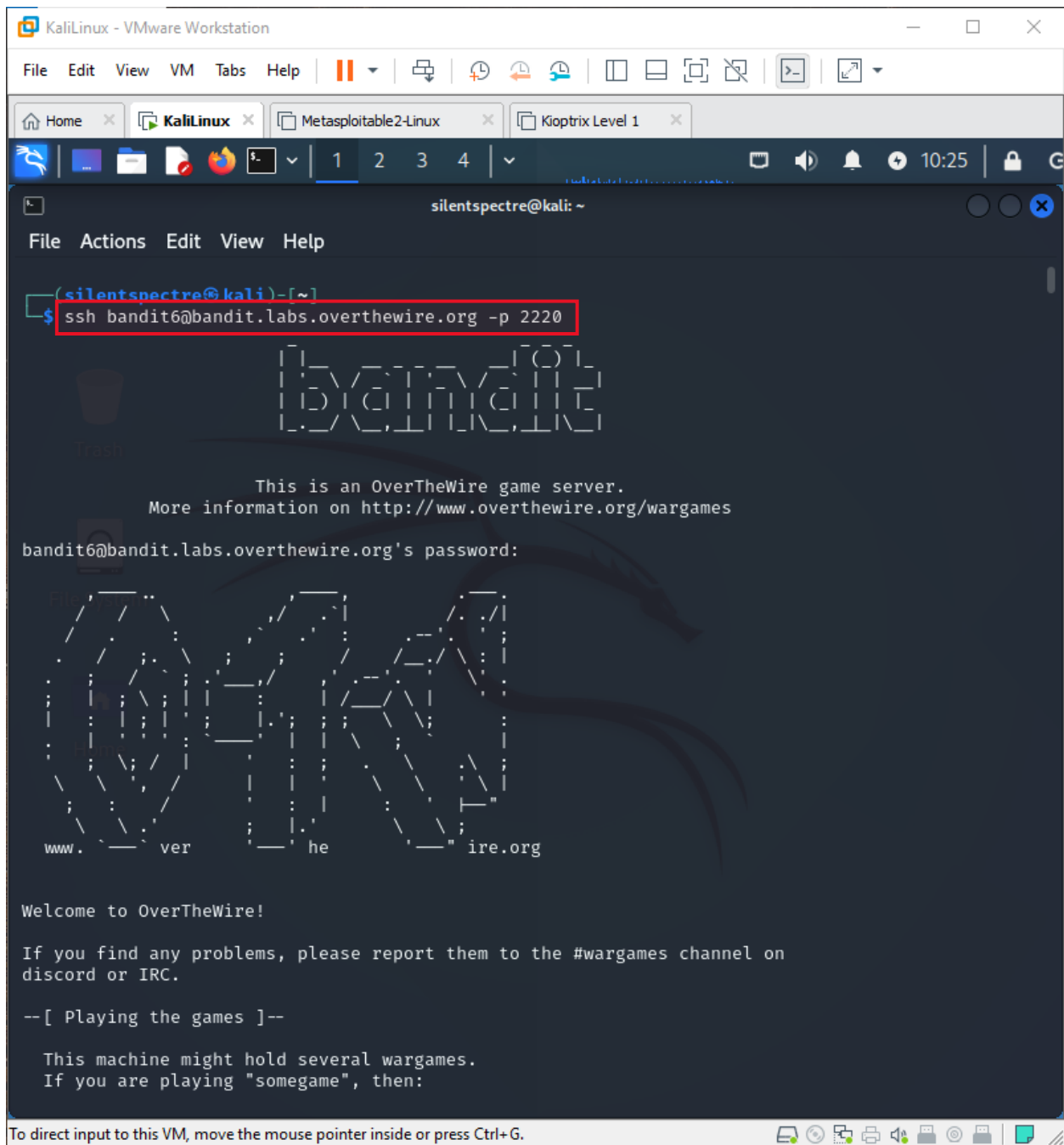
Go to inhere directory and find the file having the properties: human-readable, 1033 bytes in size, not executable using the command: **find .type f -size 1033c ! -executable**. Read this file to get password of next level:

23 July, 23

```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./^C
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
-bash: cat: ./maybehere07/.file2: No such file or directory
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

bandit5@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

23 July, 23

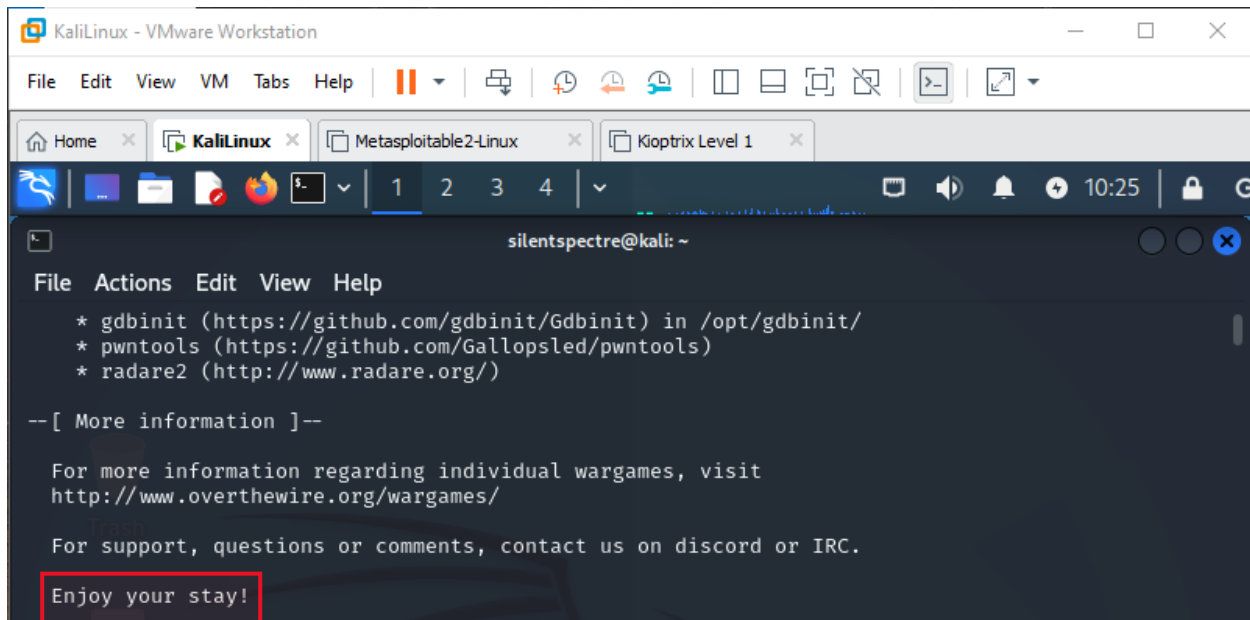


The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window is titled 'silentspectre@kali: ~' and displays the command `ssh bandit6@bandit.labs.overthewire.org -p 2220` being executed. The output of the command shows a connection to an OverTheWire game server. The server's banner includes ASCII art for 'OverTheWire', a welcome message, and instructions for playing wargames. The terminal output is as follows:

```
silentspectre@kali)-[~]  
$ ssh bandit6@bandit.labs.overthewire.org -p 2220  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit6@bandit.labs.overthewire.org's password:  
  
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:
```

The terminal window is part of a larger interface showing the VMware Workstation window with tabs for 'KaliLinux', 'Metasploitable2-Linux', and 'Kioptrix Level 1'. The system clock in the top right corner indicates 10:25.

23 July, 23



## Bandit Level 6 → Level 7

### Level Goal

The password for the next level is stored **somewhere on the server** and has all of the following properties:

- owned by user bandit7
- owned by group bandit6
- 33 bytes in size

### Commands you may need to solve this level

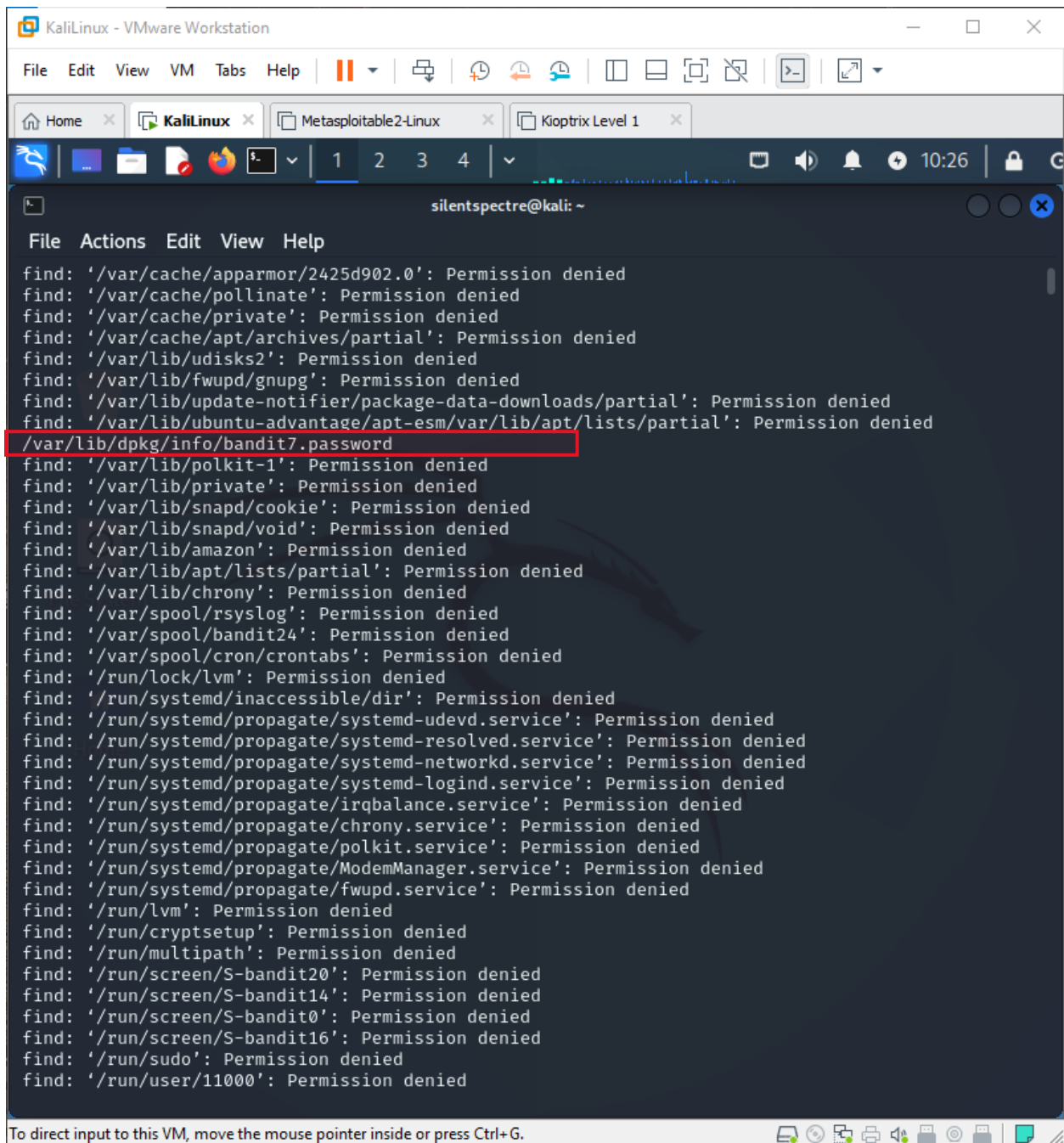
[ls](#) , [cd](#) , [cat](#) , [file](#) , [du](#) , [find](#) , [grep](#)

Find the file having the properties: owned by user bandit7, owned by group bandit6, 33 bytes in size using command: **find / -type f -user bandit7 -group bandit6 -size 33c**. Here we find path to password file of next level:

23 July, 23

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/snap': Permission denied
find: '/lost+found': Permission denied
find: '/root': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/2986507/task/2986507/fdinfo/6': No such file or directory
find: '/proc/2986507/fdinfo/5': No such file or directory
find: '/tmp': Permission denied
find: '/dev/shm': Permission denied
find: '/dev/mqueue': Permission denied
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/var/tmp': 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/cache/ldconfig': Permission denied
find: '/var/cache/apparmor/baad73a1.0': Permission denied
find: '/var/cache/apparmor/2425d902.0': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/lib/udisks2': Permission denied
find: '/var/lib/fwupd/gnupg': Permission denied
```

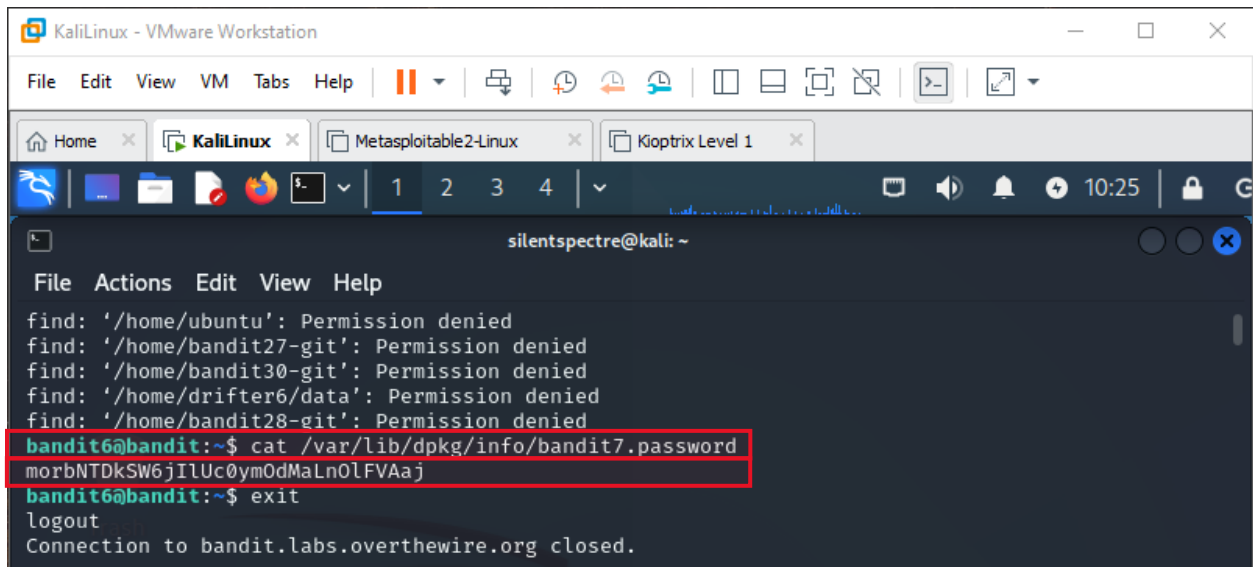
23 July, 23



```
File Actions Edit View Help
find: '/var/cache/apparmor/2425d902.0': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/lib/udisks2': Permission denied
find: '/var/lib/fwupd/gnupg': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/private': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/lib/snapd/void': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': 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-bandit20': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit0': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/sudo': Permission denied
find: '/run/user/11000': Permission denied
```

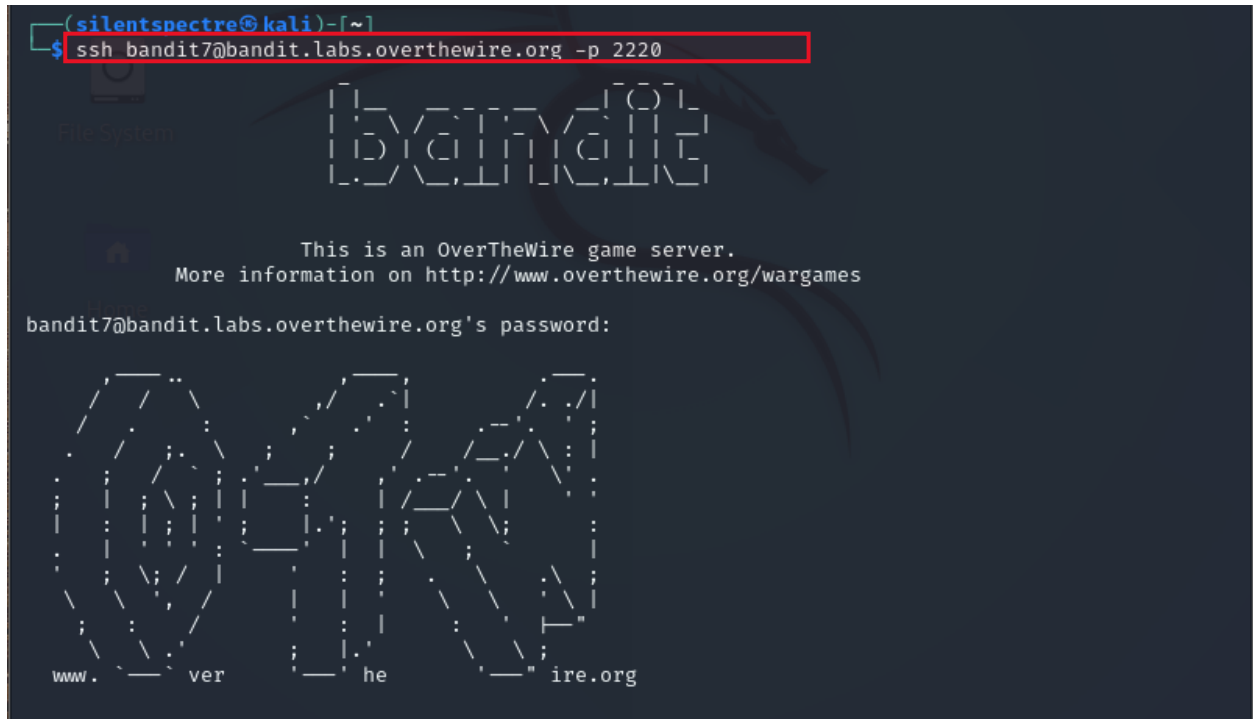
Cat this file to get the password:

23 July, 23



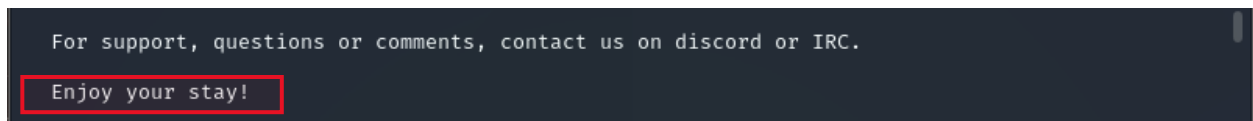
The screenshot shows a Kali Linux terminal window with the title bar "KaliLinux - VMware Workstation". The terminal output shows several "Permission denied" messages for various directories. The final command executed is `cat /var/lib/dpkg/info/bandit7.password`, which outputs the password `morbNTDkSW6jIlUc0ymOdMaLn0LFVAaj`. The terminal also shows the user logging out and the connection to `bandit.labs.overthewire.org` closing.

```
silentspectre@kali: ~  
File Actions Edit View Help  
find: '/home/ubuntu': Permission denied  
find: '/home/bandit27-git': Permission denied  
find: '/home/bandit30-git': Permission denied  
find: '/home/drifter6/data': Permission denied  
find: '/home/bandit28-git': Permission denied  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIlUc0ymOdMaLn0LFVAaj  
bandit6@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.
```



The screenshot shows an SSH session to `bandit7@bandit.labs.overthewire.org`. The terminal displays a large ASCII art logo for "OverTheWire" and a message stating "This is an OverTheWire game server. More information on <http://www.overthewire.org/wargames>". It then prompts for the password.

```
(silentspectre@kali)-[~]  
$ ssh bandit7@bandit.labs.overthewire.org -p 2220  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit7@bandit.labs.overthewire.org's password:  
  
www. ver he ire.org
```



The screenshot shows the footer of the SSH session, which includes contact information for support and a welcome message.

```
For support, questions or comments, contact us on discord or IRC.  
Enjoy your stay!
```

## Bandit Level 7 → Level 8

### Level Goal

The password for the next level is stored in the file **data.txt** next to the word **millionth**



23 July, 23

## Commands you may need to solve this level

[man](#), grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

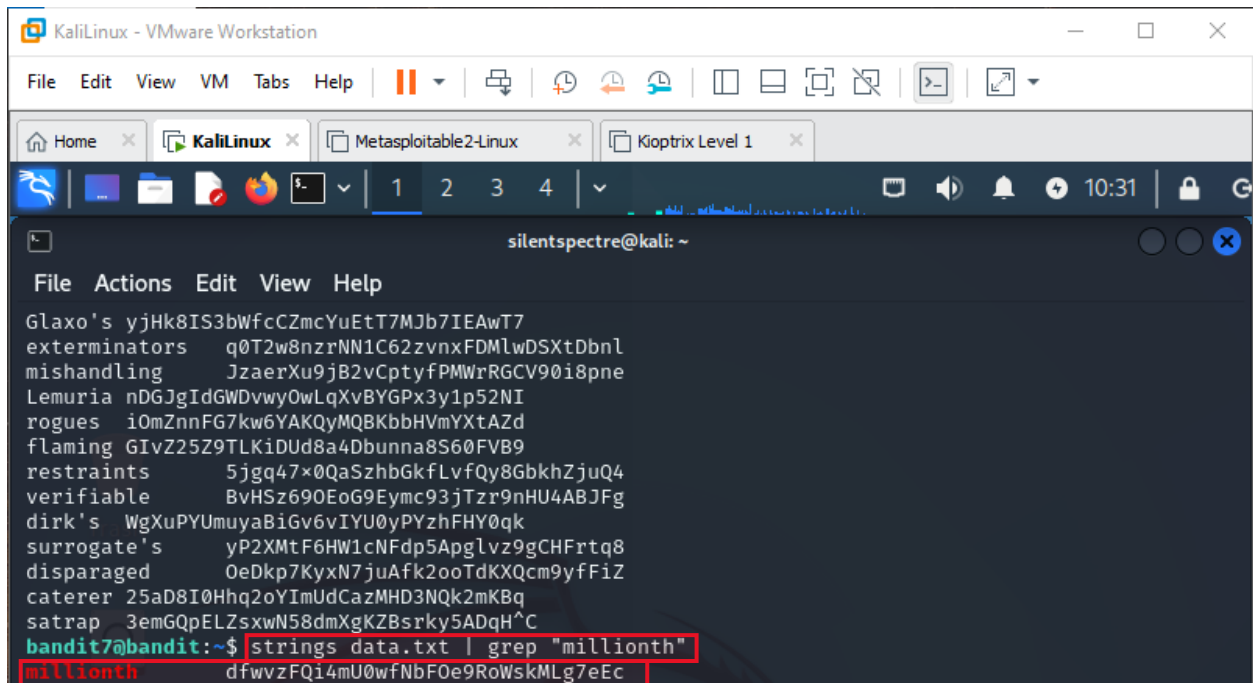
list all files and directories in home directory. Here I found data.txt file, so I read it.

```
bandit7@bandit:~$ ls -alps
total 4108
 4 drwxr-xr-x  2 root    root      4096 Jun 20 04:07 ./
 4 drwxr-xr-x 70 root    root      4096 Jun 20 04:08 ../
 4 -rw-r--r--  1 root    root       220 Mar 31 08:41 .bash_logout
 4 -rw-r--r--  1 root    root     3771 Mar 31 08:41 .bashrc
4088 -rw-r----- 1 bandit8 bandit7 4184396 Jun 20 04:07 data.txt
 4 -rw-r--r--  1 root    root       807 Mar 31 08:41 .profile
bandit7@bandit:~$ cat bandit7
cat: bandit7: No such file or directory
bandit7@bandit:~$ cat da
cat: da: No such file or directory
bandit7@bandit:~$ cat data
cat: data: No such file or directory
bandit7@bandit:~$ cat data.txt
interrogator    ZZDr4txsCpg779y6ECUhXIU2YGjv5kTi
reminisce       Xt0mfwT7bzxqzyJNewLqD4p8s9lwS0l
deforesting     HcDcIJnzZn5fvwTSGxCa3tTv5P2Bpg1G
architecture's  hckrxY5R0KiJ7VUtdygZSY45XIrDZ52G
footballers     nnviUfbLyMPRLunuyr6paNBbGgKzrrvl
breastbone      0fcGSFP30pQf7uxVdQJ4z478Y1CK6WEG
Livonia bPpdVLMBAvgT16WNeJHx4sGwD5yqb2jV
unsightliness's 8RWzuPYjliioXFjv9RjLmGcvZZEL38Tk
belittles       BE07urS01iTT0yQVWfhRUXq0TUULvUva
retrogression   H84msZtwsRfP9c50j20XNLZh9DuE9Pzn
epithets        K2zKsDeHfZstTROagl5uxkdIb9BN3PnE
imam            llSMJno3lRu98Tpy3QR0W2uDy7z0MzqK
festoons        cWaENLZLL4T4fQexuBKxUbhaRXjdEeFJ
blackguards     rWpggkiQZbH0wXe8PWk0GziHBtzwq0BD
itinerary       bHXJmN8lhTQN1xsP0v6FEdAosqmH9Ju4
genteelest      hjtw3BzMY7CLhk5wM0Rkbo6w1yZ06zX0
lamprey's       GzTG8I3gBohESCVOwiXpHNMZrfk1qGTu
pride's JS7hFyZBhinB4h0ZstUj3r7eYLLQusur
telecasting      uAIw1FGJ2Lyp375kqGTPwqxJ2zVqszMz
```

As the password is in front of millionth word in this file, so search for the string "millionth"

within a file named data.txt using command: **strings data.txt | grep "millionth"** and read it:

23 July, 23



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal displays a list of words and their corresponding hashes, followed by a command to search for the word "millionth" in a file named "data.txt". The command is highlighted with a red box, and the output is also highlighted with a red box.

```
File Actions Edit View Help
Glaxo's yjHk8IS3bWfcCZmcYuEtT7MJb7IEAwT7
exterminators q0T2w8nzrNN1C62zvnxFdMlwDSXtDbnl
mishandling JzaerXu9jB2vCptyfPMWrRGCV90i8pne
Lemuria nDGJgIdGWDvwyOwLqXvBYGPx3y1p52NI
rogues i0mZnnFG7kw6YAKQyMQBKbbHVmYXtAZd
flaming GIvZ25Z9TLKiDUd8a4Dbunna8S60FVB9
restraints 5jgq47x0QaSzhbGkfLvFQy8GbkhZjuQ4
verifiable BvHSz690EoG9Eymc93jTzr9nHU4ABJFg
dirk's WgXuPYUmuyaBiGv6vIYU0yPYzhFHY0qk
surrogate's yP2XMtF6HW1cNFdp5Apglvz9gCHFrtq8
disparaged 0eDkp7KyxN7juAfk2ooTdKXQcm9yFfiZ
caterer 25aD8I0Hhq2oYImUdCazMHD3NQk2mKBq
satrap 3emGQpELZsxnN58dmXgKZBsrky5ADqH^C
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

23 July, 23

The screenshot shows a Kali Linux terminal window with the following content:

```

silentspectre@kali: ~
File Actions Edit View Help
(silentspectre@kali)-[~]
$ ssh bandit8@bandit.labs.overthewire.org -p 2220

```

The terminal output displays the ASCII art logo for OverTheWire, which includes the text "OverTheWire" in a stylized font, followed by "This is an OverTheWire game server." and "More information on <http://www.overthewire.org/wargames>".

Below the logo, the terminal prompts for the password:

```

bandit8@bandit.labs.overthewire.org's password:

```

The terminal then displays the ASCII art logo for OverTheWire again, followed by the text "Welcome to OverTheWire!".

Below the welcome message, the terminal provides instructions:

```

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

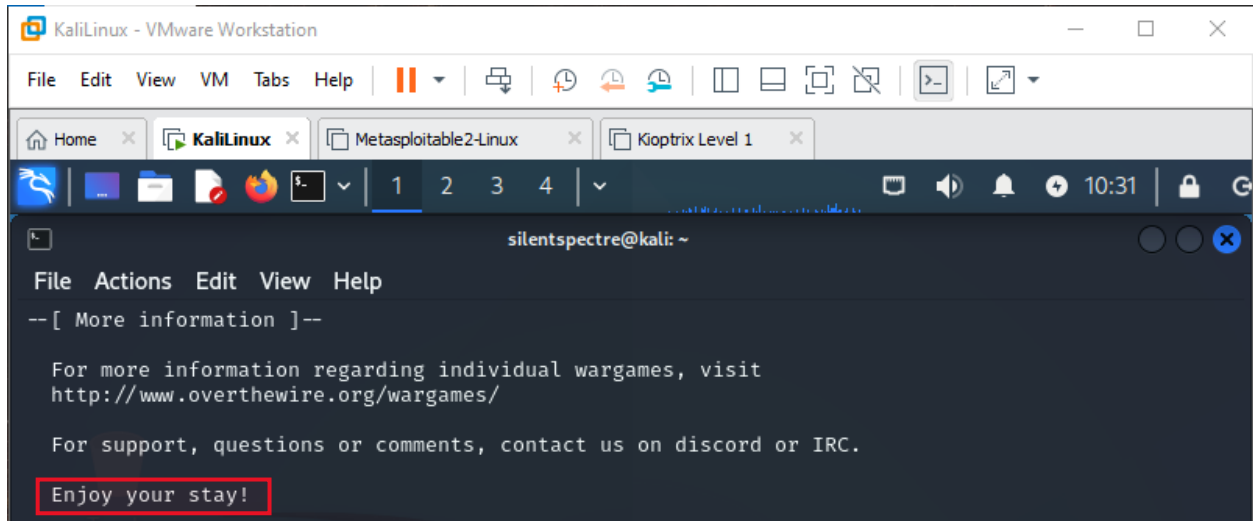
--[ Playing the games ]--

This machine might hold several wargames.
If you are playing "somegame", then:

```

The terminal window also shows the top bar of the Kali Linux desktop environment, including the file manager, terminal, and other applications.

23 July, 23



## Bandit Level 8 → Level 9

### Level Goal

The password for the next level is stored in the file **data.txt** and is the only line of text that occurs only once

### Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

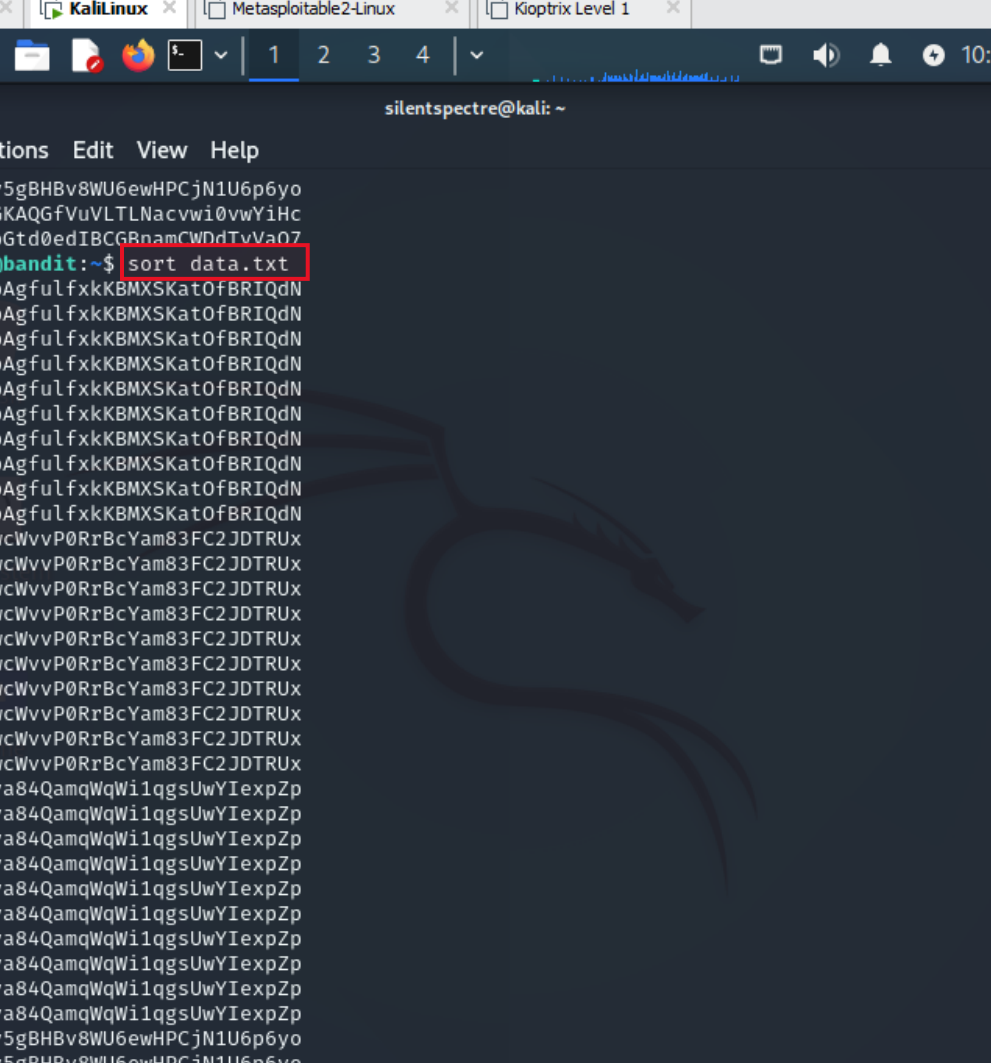
read data.txt,

23 July, 23

```
bandit8@bandit:~$ cat data.txt
VMpFvIE8BvkGHL2ZZCbTjstNxjAhdTCE
qz2NpIwJIT5Tk9PsY90ENphupqrvoOrx
8euCQ4tPvk7BgMGLUs5CG6M9ffaQgCuE
RJSptBMwy6XajgYQT4mb3Vfgo3egzFoh
90NcgN5BWYzeN2qLMKIEcxLqnRLfpzLn
qUXN7Q4fsXVlyfMe5k12HyiJqnLCFijw
4JTXH3PW1jq0HyiqfB9gGv9FmohdWsGy
A05YA8bNKfYzyjvKk4VEJN7anzrp0p3f
neTbLI6EYQ9o7bRCRNeDRfBSIA00cy0S
KY1tLMnNgn3Qha4IwF2wXB2iUdbc8ekr
qUXN7Q4fsXVlyfMe5k12HyiJqnLCFijw
zfuV10XBDnWLFgBaawNRqJJB2iYfPIGE
4ro7Cv8eAvYTPDAdOLK062y0usi1bALM
C4Ezjsh7veP7WYhm6ULiIxyHyRAcspjv
ypM1SoR8fE6imXFXZP9UQsbSeeDZ43gl
nQjxj69xUzCyY902y42KSeci8MyYtpnS
I3aC4r2LaJkt5215RS0VyJnBl9vo4Uuj
Xj4mWqAGKAQGfVuVLTlnacvwi0vwYiHc
9mQnTm1J2l975HYtCthq0SNCKCJTq5N0
86WFzG8qrEkEhG3kDH6peqCjvEGpUDli
y5si0BKagXbPyLjMrfExpghBL05gljfc
y5si0BKagXbPyLjMrfExpghBL05gljfc
4kNFm4ZkvPsPRMeNphCrFv80Sh2Ezn1o
neTbLI6EYQ9o7bRCRNeDRfBSIA00cy0S
VMpFvIE8BvkGHL2ZZCbTjstNxjAhdTCE
4m2FCTzgrR8FGFrmmjF8v2hKEPn4emLV
mz0ztNpSf8qFa8RsRtHJnwqAtDs7UPHb
F1y1UE7dMVtJU9a0y89cM2iTAyXvMfi
4idw5nXgGcTzN2mXicJHccNbVJfWfxfk
```

Sort the lines in data.txt in ascending order: **sort data.txt**

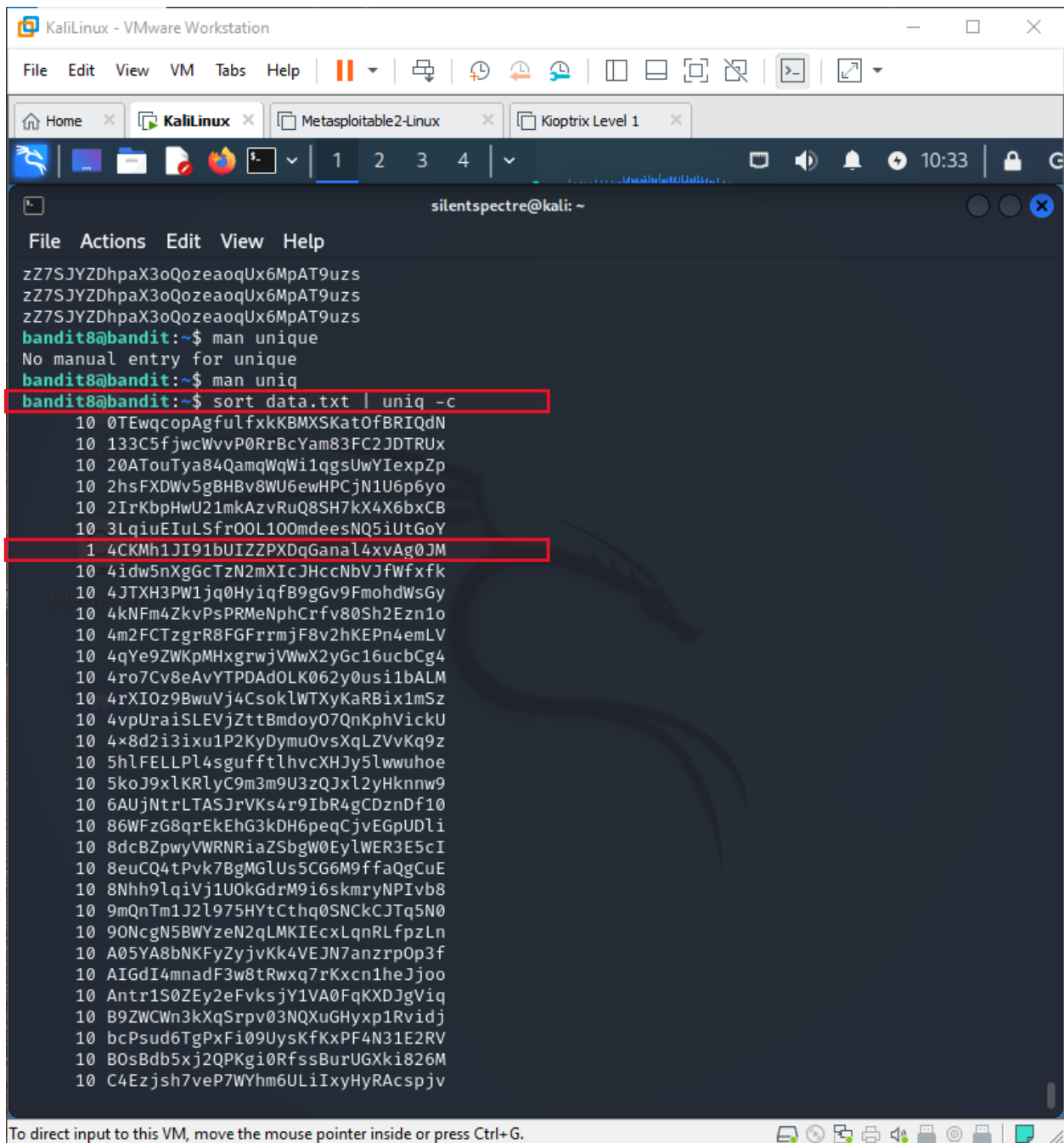
23 July, 23



The screenshot shows a Kali Linux terminal window. The terminal title is "silentspectre@kali: ~". The prompt is "bandit8@bandit:~\$". The command "sort data.txt" has been entered and is highlighted with a red box. The output of the command is a list of files and directories, including "0TEwqcopAgfulfxxkKBMXSKatOfBRIQdN", "133C5fjwcWvvP0RrBcYam83FC2JDTRUx", "20ATouTya84QamqWqWi1qgsUwYIexpZp", and "2hsFXDWv5gBHBv8WU6ewHPCjN1U6p6yo". The terminal window is part of a VMware Workstation interface, with the top bar showing "KaliLinux - VMware Workstation" and the bottom bar showing "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

**sort data.txt | uniq -c** to sort the lines in data.txt and then count the occurrences of each unique line. The only file that appears one time will be unique and is the password of next level:


23 July, 23



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home KaliLinux Metasploitable2-Linux Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
zz7SJYZDhpaX3oQoeaoqUx6MpAT9uzs
zz7SJYZDhpaX3oQoeaoqUx6MpAT9uzs
zz7SJYZDhpaX3oQoeaoqUx6MpAT9uzs
bandit8@bandit:~$ man unique
No manual entry for unique
bandit8@bandit:~$ man uniq
bandit8@bandit:~$ sort data.txt | uniq -c
10 0TEwqcopAgfulfxxkKBMXSKatOfBRIQdN
10 133C5fjwcWvvp0RrBcYam83FC2JDTRUx
10 20ATouTya84QamqWqWi1qgsUwYIexpZp
10 2hsFXDWv5gBHBv8WU6ewHPCjN1U6p6yo
10 2IrKbpHwU21mkAzvRuQ8SH7kX4X6bxCB
10 3LqiuEIuLSfr0OL100mdeesNQ5iUtGoY
1 4CKMh1JI91bUIZPXQdGanal4xvAg0JM
10 4idw5nXgGcTzN2mXIcJHccNbVJfWfxfk
10 4JTXH3PW1jq0HyiqfB9gGv9FmohdWsGy
10 4kNFm4ZkvPsPRMeNphCrFv80Sh2Ezn1o
10 4m2FCTzgrR8FGFrrmjF8v2hKEPn4emLV
10 4qYe9ZWkpMHxgrwjVWwX2yGc16ucbCg4
10 4ro7Cv8eAvYTPDAd0LK062y0usi1bALM
10 4rXIOz9BwuVj4CsokLWTXyKaRBix1mSz
10 4vpUraiSLEVjZttBmdoy07QnKphVickU
10 4x8d2i3ixu1P2KyDymu0vsXqLZVvKq9z
10 5hlFELLPL4sgufftlhvcXHJy5lwwuhoe
10 5koJ9xlKRlyC9m3m9U3zQJxl2yHknnw9
10 6AUjNtrLTASJrVKs4r9IbR4gCDznDf10
10 86WFzG8qrEkEhG3kDH6peqCjvEGpUDli
10 8dcBZpwyVWRNRiaZSbgW0EylWER3E5cI
10 8euCQ4tPvk7BgMGLUs5CG6M9ffaQgCuE
10 8Nhh9lqiVj1UOkGdrM9i6skmryNPIvb8
10 9mQnTm1J2l975HYtCthq0SNCKCJTq5N0
10 9ONcgN5BWYzeN2qLMKIEcxLqnRLfpzLn
10 A05YA8bNKfyZyvvKk4VEJN7anzrp0p3f
10 AIGdI4mnadF3w8tRwxq7rKxcn1heJjoo
10 Antr1S0ZEy2eFvksjY1VA0FqKXDJgViq
10 B9ZWCWn3kXqSrpv03NQXuGHyp1Rvidj
10 bcPsud6TgPxFi09UysKfKxPF4N31E2RV
10 B0sBdb5xj2QPKgi0RfssBurUGXki826M
10 C4Ezjsh7veP7WYhm6ULiIxyHyRAcspjv
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

23 July, 23


```
(silentspectre@kali)~$ ssh bandit9@bandit.labs.overthewire.org -p 2220
```



File System

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

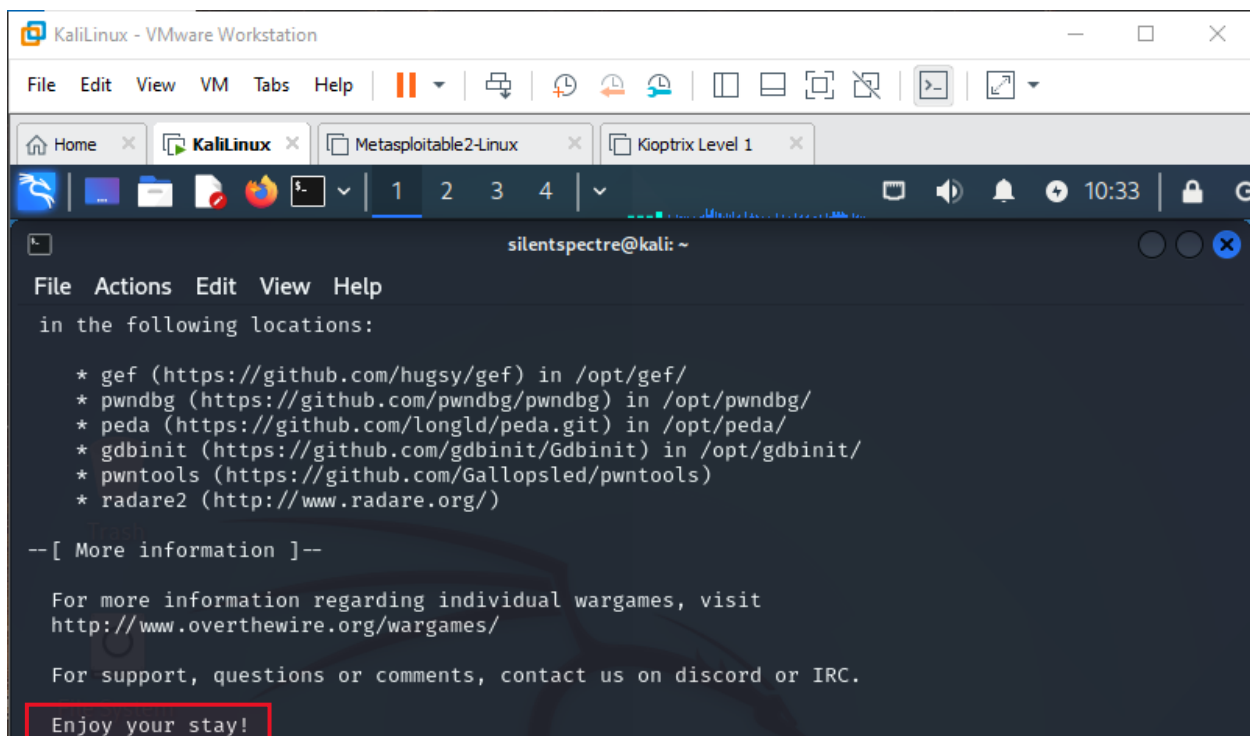
bandit9@bandit.labs.overthewire.org's password:



[www. ver he ire.org](http://www.overthewire.org)

Welcome to OverTheWire!

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



KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x

1 2 3 4

10:33

```
silentspectre@kali: ~
```

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/
- \* 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!

Bandit Level 9 → Level 10



23 July, 23

## Level Goal

The password for the next level is stored in the file **data.txt** in one of the few human-readable strings, preceded by several '=' characters.

## Commands you may need to solve this level

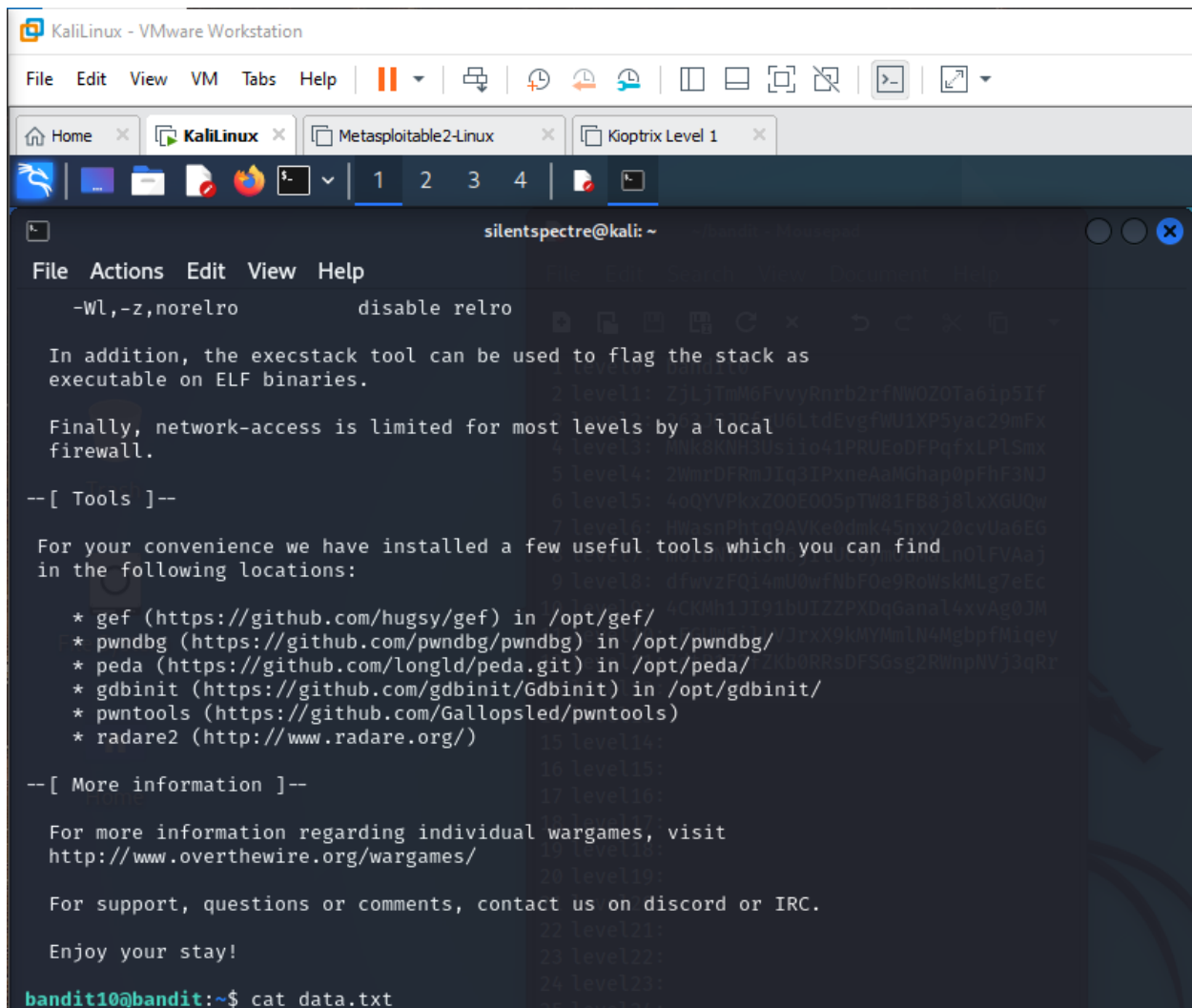
grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

**strings data.txt | grep "="** to search for lines in the output of the strings command that contain the equals sign (=). Here we get the password for next level:

```
bandit9@bandit:~$ strings data.txt | grep "="
[===== the
EJ}@k=
T%===== passwordG
\      =f7
}===== ist"
WL[L=S
)|P-Vz
=Y`W^
=9|
s7.-;$
g=6E
| =?y=
===== FGUW5ilLVJrxX9kMYMmLN4MgbpfMiqey
=n/iZ
: '=F
timed out waiting for input: auto-logout
Connection to bandit.labs.overthewire.org closed.

(silentspectre@kali)-[~]
$
```

23 July, 23



KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x

1 2 3 4

silentspectre@kali: ~

File Actions Edit View Help

-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 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/
- \* 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!

bandit10@bandit:~\$ cat data.txt