

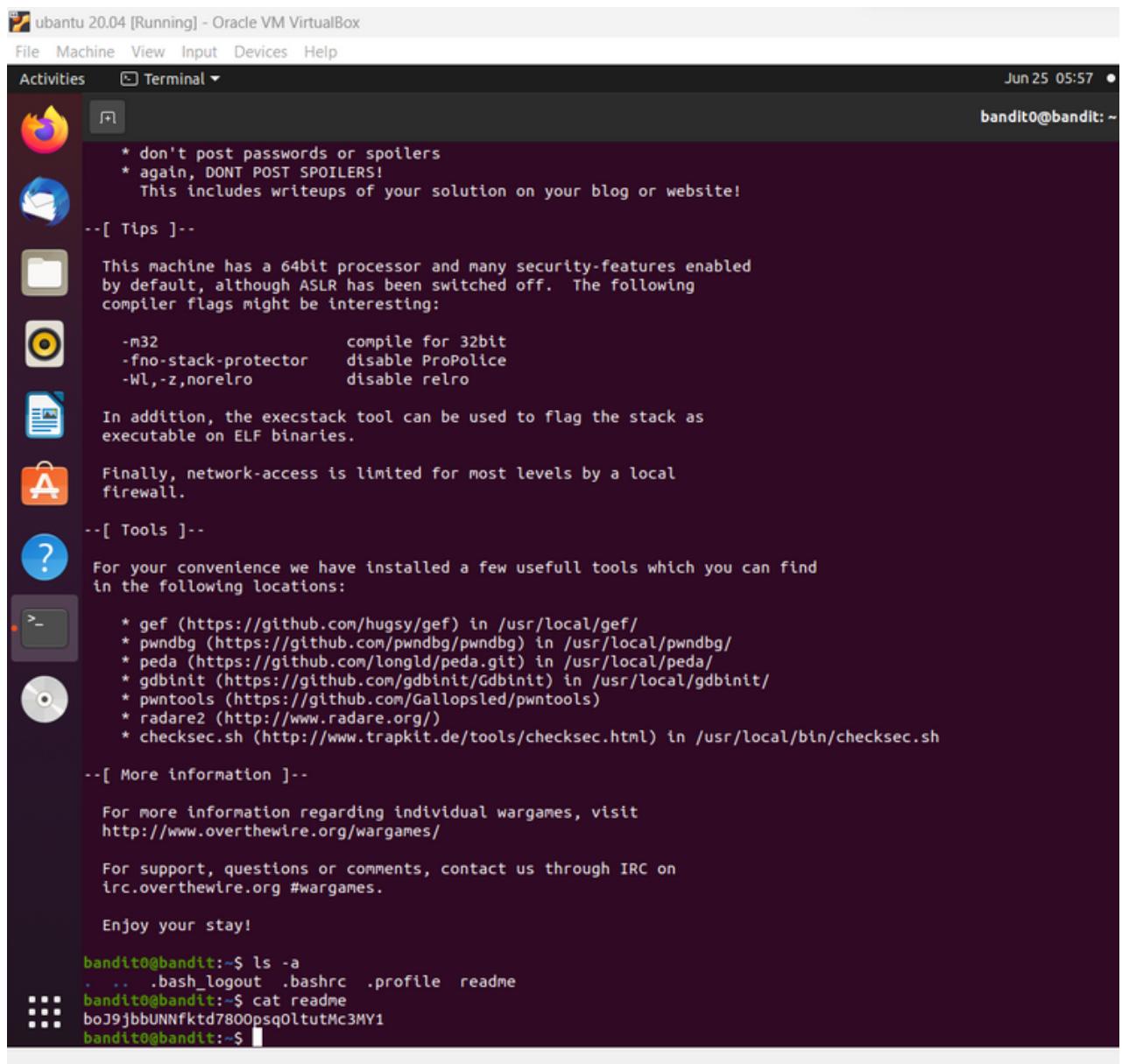
# **TASK 5 [LINUX GAMES]**

## Screenshots of the passwords:

## **Level 0:**

## Level 0 -> level 1:

**Password:** boJ9jbbUNNfktd7800psq0ltutMc3MY1



ubuntu 20.04 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 25 05:57 bandit0@bandit: ~

```
* 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,norelo      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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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!
```

bandit0@bandit:~\$ ls -a  
.. .bash\_logout .bashrc .profile readme  
bandit0@bandit:~\$ cat readme  
boJ9jbbUNNfktd7800psq0ltutMc3MY1  
bandit0@bandit:~\$

## Level 1 -> level 2:

**Password:** CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

```
* 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

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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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!

bandit1@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile
bandit1@bandit:~$ cat ./
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ ^C
bandit1@bandit:~$
```

## Level 2 -> level 3:

**Password:** UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

The screenshot shows a terminal window titled "Terminal" on an Ubuntu 20.04 desktop environment. The window contains a welcome message for a new user, bandit2. The message includes instructions for stack protection, network access, and tool installation, followed by links to documentation and support resources. At the bottom, the user's password is displayed in red.

```
-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/
* gdbinit (https://github.com/Gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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!

bandit2@bandit:~$ ls -a
. .. .bash_logout .bashrc .profile spaces in this filename
bandit2@bandit:~$ cat spaces in the filename
cat: spaces: No such file or directory
cat: in: No such file or directory
cat: the: No such file or directory
cat: filename: No such file or directory
bandit2@bandit:~$ cat spacesinthefilename
cat: spacesinthefilename: No such file or directory
bandit2@bandit:~$ cat spaces\ in\ the\ filename
cat: 'spaces in the filename': No such file or directory
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ [REDACTED]
```

## Level 2 -> level 3:

**Password:** UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

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 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/
- \* gdbinit (<https://github.com/gdbinit/Gdbinit>) in /usr/local/gdbinit/
- \* pwntools (<https://github.com/Gallopsled/pwntools>)
- \* 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/>

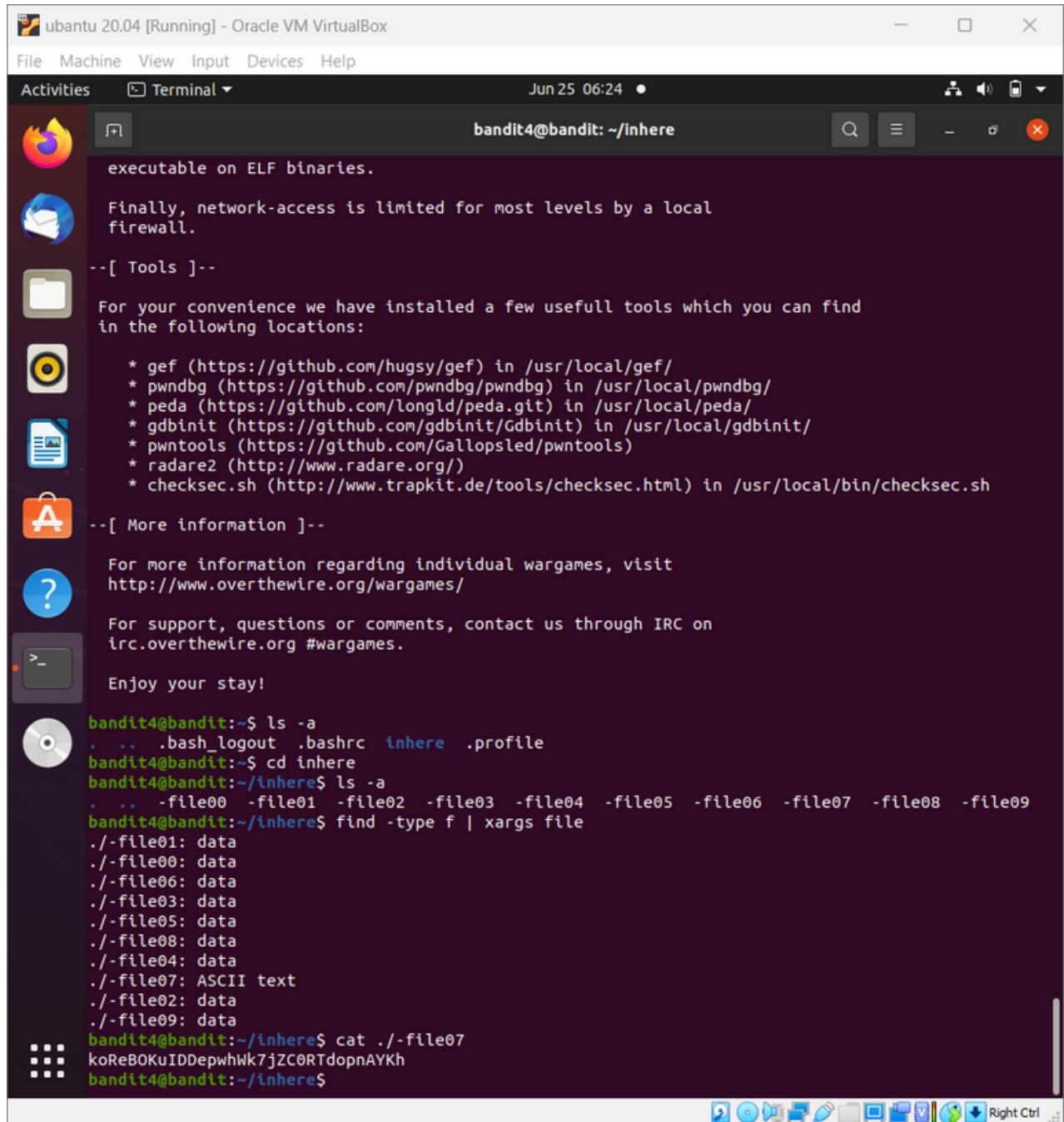
For support, questions or comments, contact us through IRC on irc.overthewire.org #wargames.

Enjoy your stay!

```
bandit3@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  inhere  .profile
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat .hidden
cat: .hidden: No such file or directory
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$
```

## Level 4 -> level 5:

**Password:** koReBOKuIDDepwhWk7jZC0RTdopnAYKh



The screenshot shows a desktop environment for Ubuntu 20.04 running in Oracle VM VirtualBox. The terminal window is titled "bandit4@bandit: ~/inhere". The terminal content is as follows:

```
ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 25 06:24
bandit4@bandit: ~/inhere
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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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/

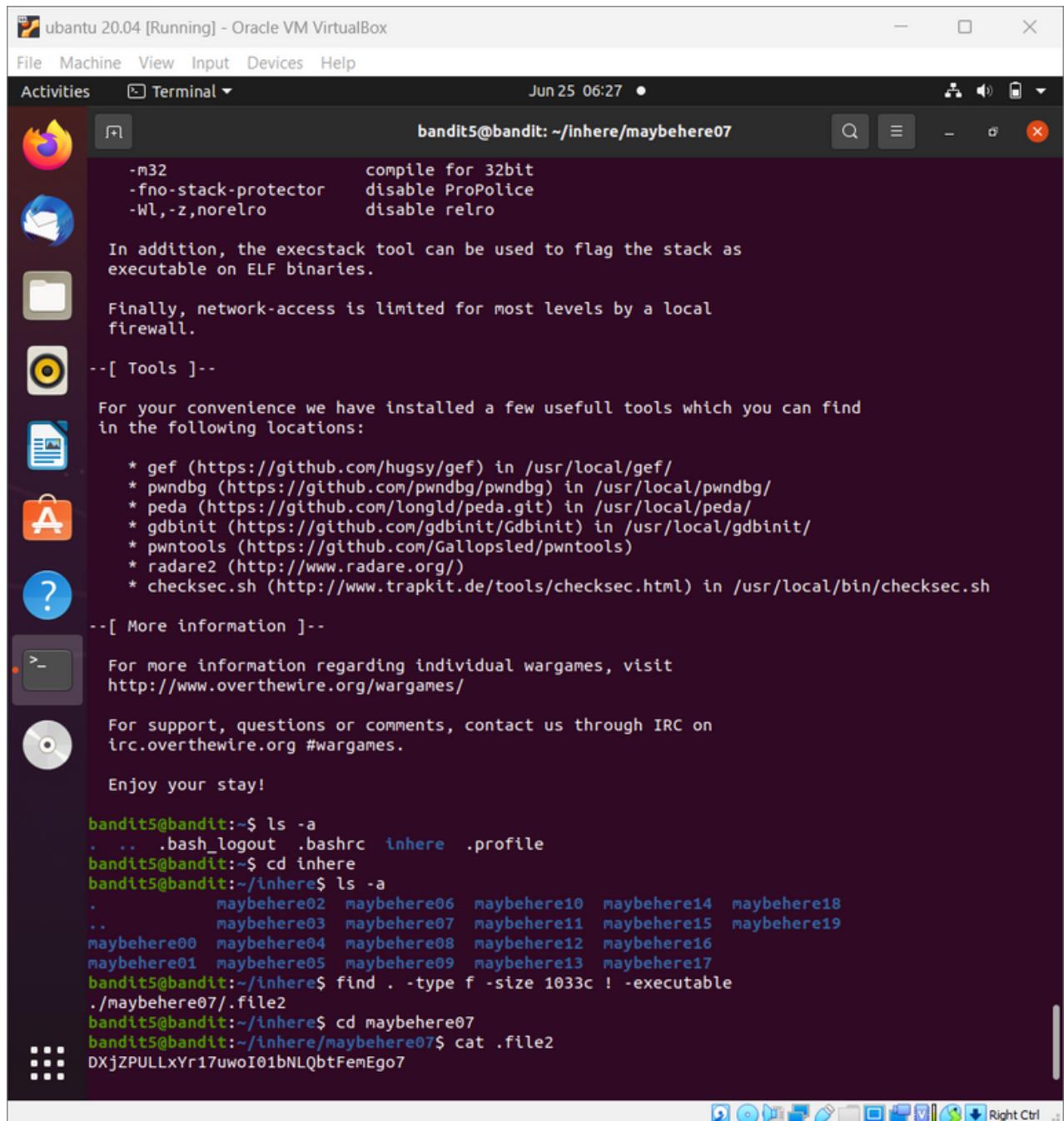
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit4@bandit:~$ ls -a
. . .. .bash_logout .bashrc inhere .profile
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -a
. . .. -file00 -file01 -file02 -file03 -file04 -file05 -file06 -file07 -file08 -file09
bandit4@bandit:~/inhere$ 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:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

## Level 5 -> level 6:

**Password:** DXjZPULLxYr17uwoI01bNLQbtFemEgo7



The image shows a screenshot of an Ubuntu 20.04 desktop environment running in Oracle VM VirtualBox. The terminal window is open and displays the following text:

```
bandit5@bandit: ~/inhere/maybehere07
-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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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/

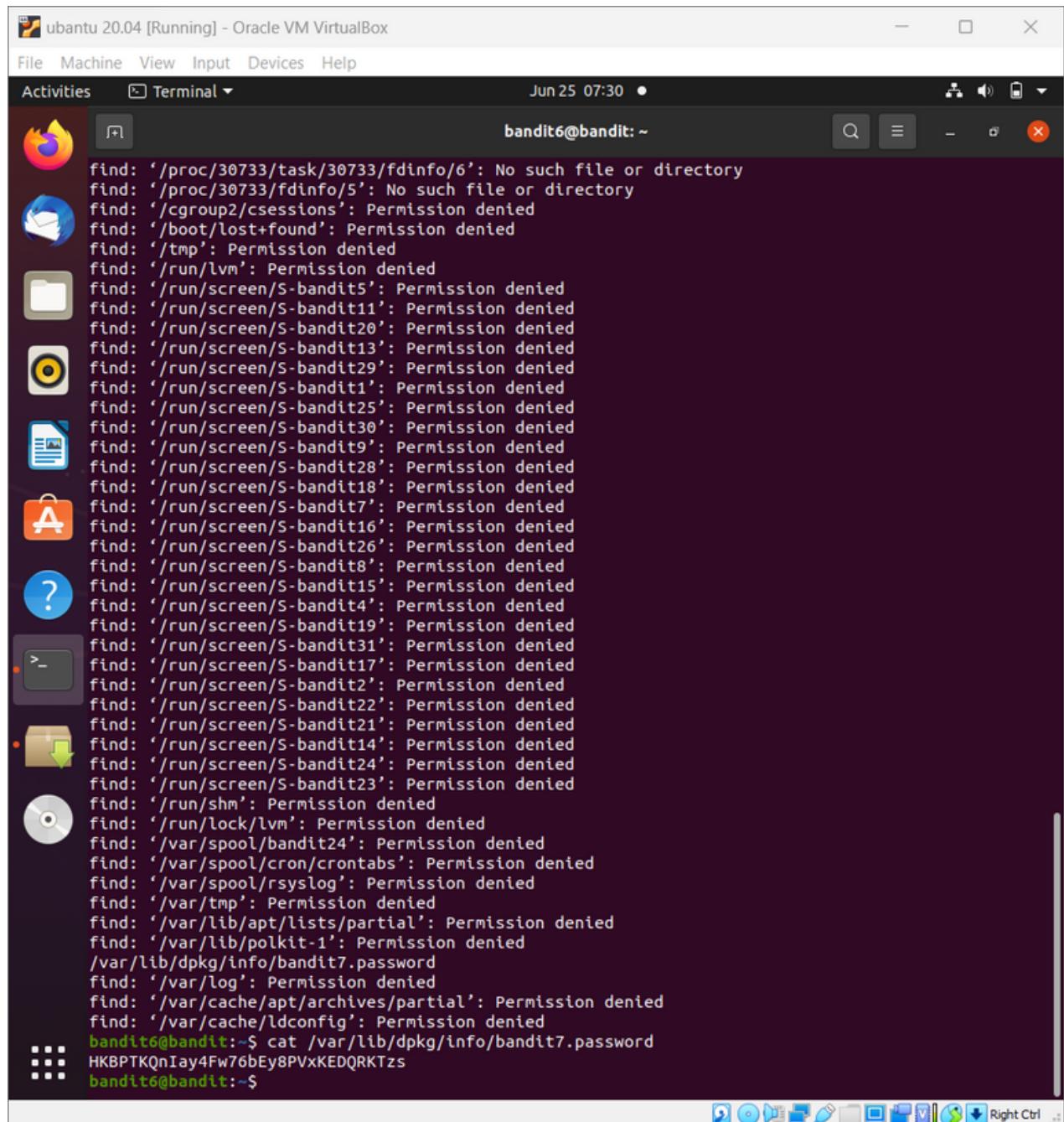
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit5@bandit:~$ ls -a
. .. .bash_logout .bashrc inhere .profile
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls -a
. maybehere02 maybehere06 maybehere10 maybehere14 maybehere18
.. maybehere03 maybehere07 maybehere11 maybehere15 maybehere19
maybehere00 maybehere04 maybehere08 maybehere12 maybehere16
maybehere01 maybehere05 maybehere09 maybehere13 maybehere17
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cd maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat .file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

## Level 6 -> level 7:

**Password:** HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs



The screenshot shows a terminal window titled "ubuntu 20.04 [Running] - Oracle VM VirtualBox". The terminal session is for user "bandit6" at host "bandit:~". The user runs a "find" command to search for files or directories, which results in numerous "Permission denied" errors across various system paths such as "/proc", "/run", and "/var". Finally, the user runs "cat /var/lib/dpkg/info/bandit7.password", which outputs the password "HKBPTKQnlay4Fw76bEy8PVxKEDQRKTzs".

```
find: '/proc/30733/task/30733/fdinfo/6': No such file or directory
find: '/proc/30733/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-bandit5': Permission denied
find: '/run/screen/S-bandit11': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit1': 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-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit17': 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-bandit24': 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/tmp': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
/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 -> level 8:

**Password:** cvX2JJa4CFALtqS87jk27qwqGhBM9plV

The screenshot shows a terminal window titled "ubantu 20.04 [Running] - Oracle VM VirtualBox". The window contains a welcome message for a security challenge, likely a Wargame. The message includes tips for bypassing security features like ASLR, information about available tools (gef, pwndbg, peda, gdbinit, pwntools, radare2, checksec.sh), and links for more information and support.

```
* 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

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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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!

bandit7@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit7@bandit:~$ cat data.txt | grep "millionth"
millionth  cvX2JJa4CFALtqS87jk27qwqGhBM9plV
```

## Level 8 -> level 9:

**Password:** UsVvYFSfZZWbi6wgC7dAFyFuR6jQQUhR

The screenshot shows a terminal window titled "Ubuntu 20.04 [Running] - Oracle VM VirtualBox". The terminal session is for user "bandit8@bandit:~". The window includes a docked icon bar at the bottom with various application icons.

```
bandit8@bandit:~$ ls -a
.  ..  .bash_logout  .bashrc  data.txt  .profile
bandit8@bandit:~$ sort data.txt | uniq -u
UsVvYFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$
```

The terminal displays the following text:

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
```

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/
- \* gdbinit (<https://github.com/Gdbinit/Gdbinit>) in /usr/local/gdbinit/
- \* pwnools (<https://github.com/Gallopsled/pwnools>)
- \* radare2 (<http://www.radare.org/>)
- \* checksec.sh (<http://www.trapkit.de/tools/checksec.html>) in /usr/local/bin/checksec.sh

--[ More information ]--

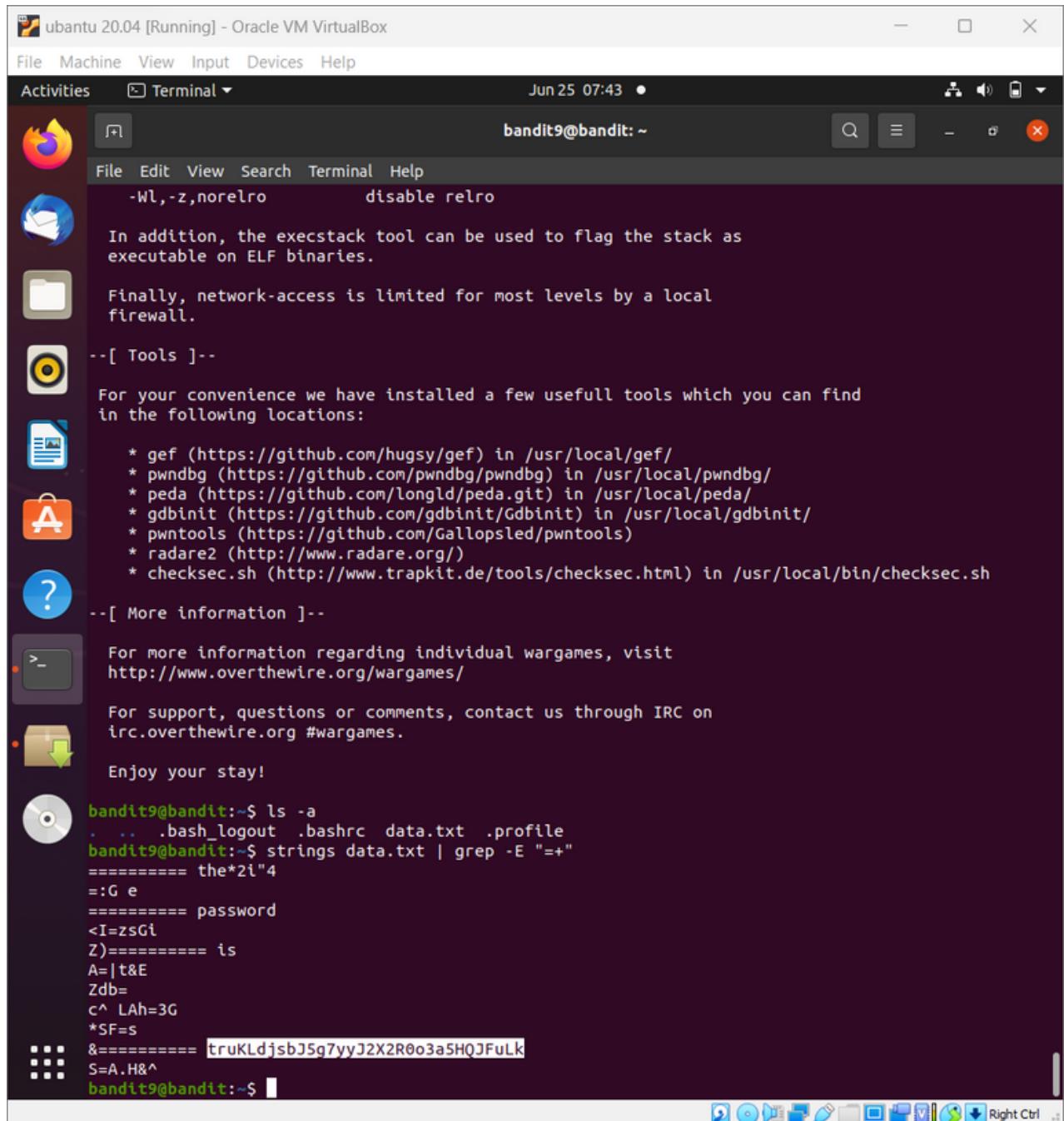
For more information regarding individual wargames, visit <http://www.overthewire.org/wargames/>

For support, questions or comments, contact us through IRC on [#wargames](irc://irc.overthewire.org).

Enjoy your stay!

## Level 9 -> level 10:

**Password:** truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk

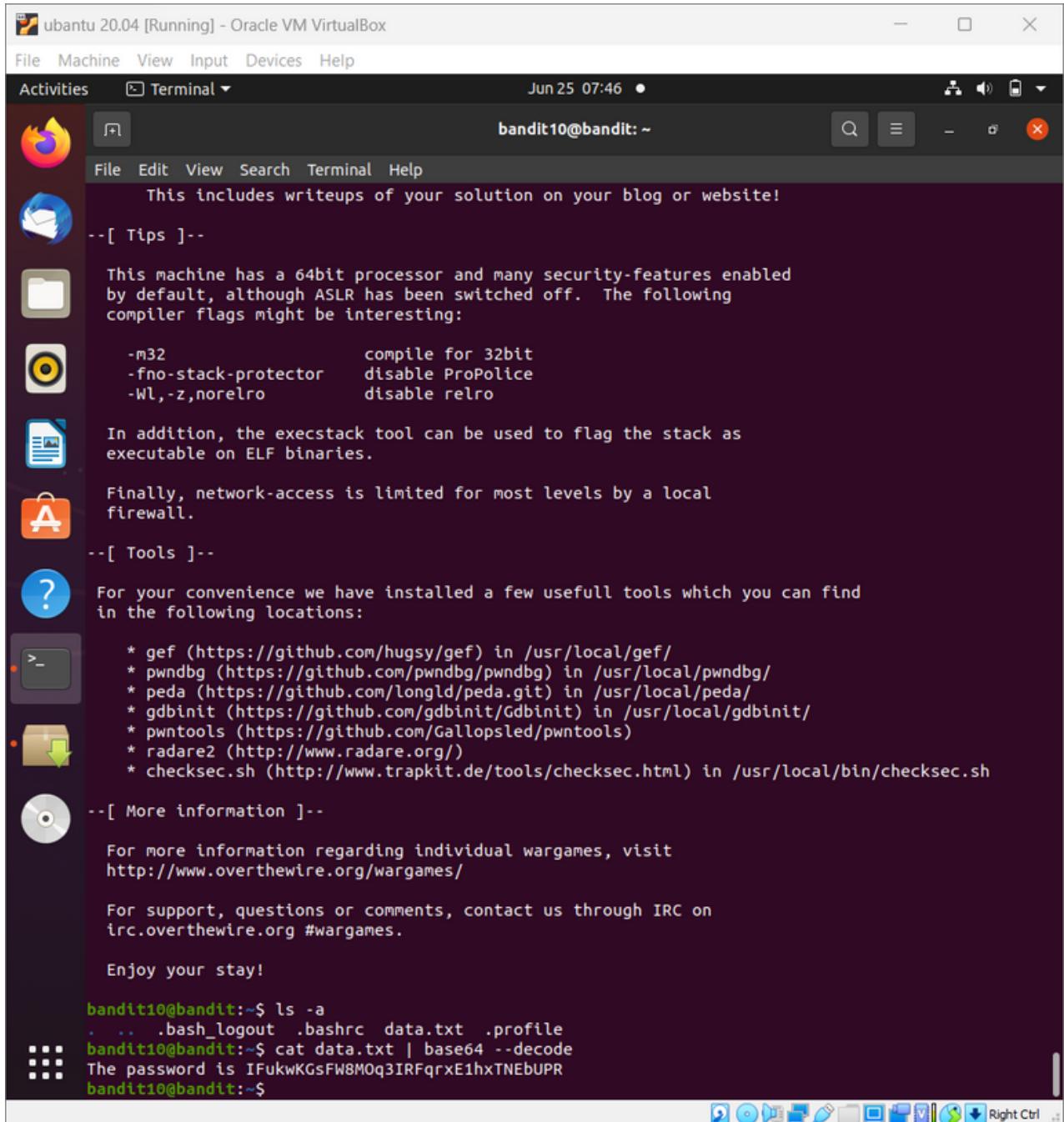


The image shows a screenshot of an Ubuntu 20.04 desktop environment running in Oracle VM VirtualBox. A terminal window is open, displaying a welcome message for the Bandit challenge system. The message includes instructions for stack protection, network access, and a list of installed tools like gef, pwndbg, peda, gdbinit, pwntools, radare2, and checksec.sh. It also provides links for more information and support. At the bottom of the terminal, the user runs 'ls -a' and 'strings data.txt | grep -E "="' to find the password 'truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk'.

```
ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 25 07:43 •
bandit9@bandit: ~
File Edit View Search Terminal 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 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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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!
bandit9@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit9@bandit:~$ strings data.txt | grep -E "="
===== the*2i"4
=:G e
===== password
<I=zsGi
Z)=====
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
===== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
S=A.H&
bandit9@bandit:~$
```

## Level 10 -> level 11:

**Password:** IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

A screenshot of an Ubuntu 20.04 desktop environment running in Oracle VM VirtualBox. The desktop has a dark theme with icons for various applications like a browser, file manager, and terminal. A terminal window is open, showing a message from the system administrator and some tips for the user. The terminal prompt shows the user is currently on the bandit10 account.

```
ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 25 07:46 •
bandit10@bandit: ~
File Edit View Search Terminal Help
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,norelo  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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!
bandit10@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$
```

## Level 11 -> level 12:

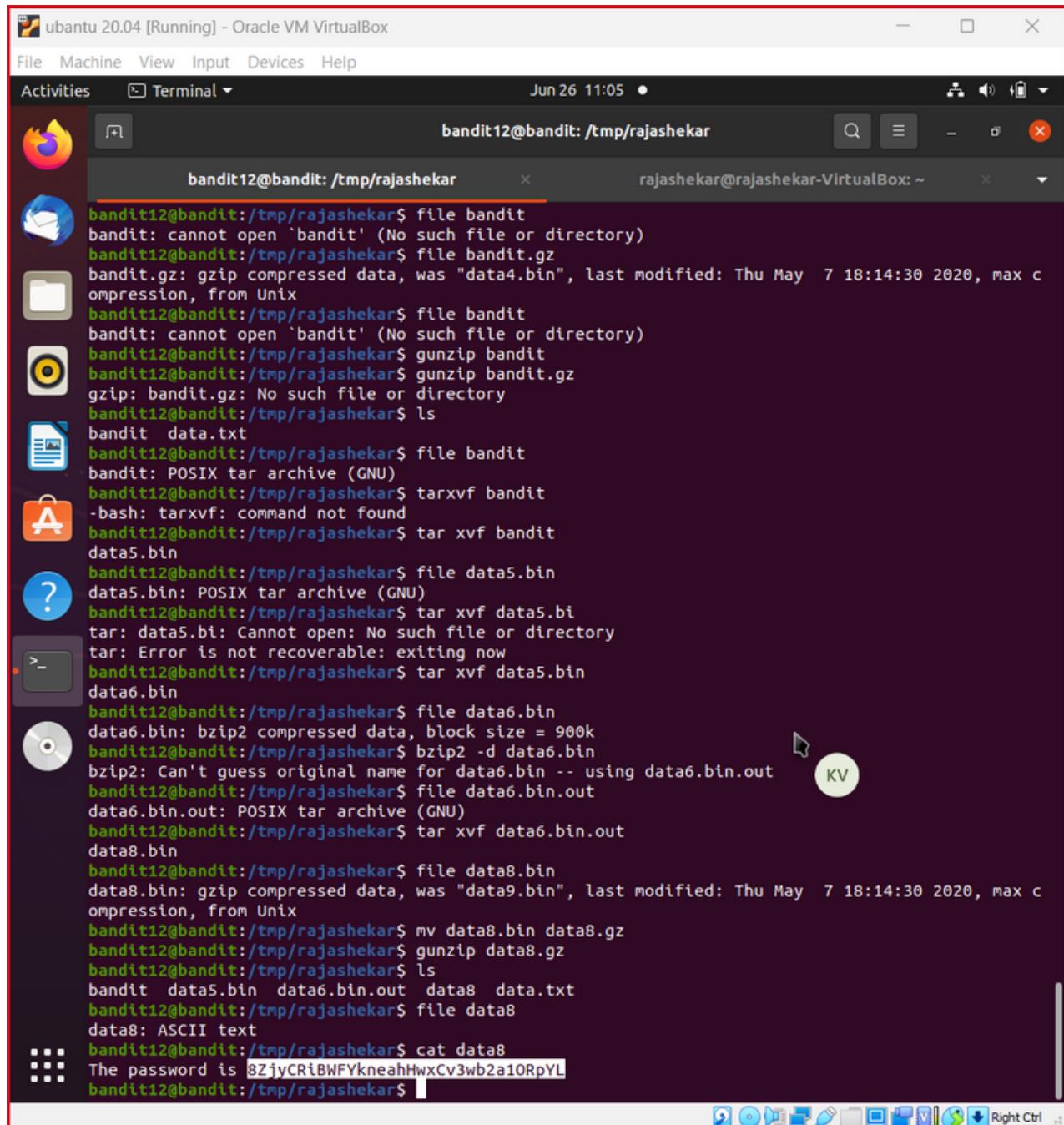
**Password:** 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

The screenshot shows a terminal window titled "ubuntu 20.04 [Running] - Oracle VM VirtualBox". The terminal is running as user "bandit11@bandit:~". The window contains a welcome message for the user, providing tips and information about the machine's security features and available tools. The message includes compiler flags like -m32, -fno-stack-protector, and -Wl,-z,norelo, and mentions the execstack tool for flagging the stack as executable. It also notes a local firewall限制. The terminal ends with a command to list files in the current directory, showing ". .bash\_logout .bashrc data.txt .profile" and the password "The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu".

```
ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 25 07:49
bandit11@bandit:~ [Search] [List] [-] [X]
File Edit View Search Terminal Help
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,norelo      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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!
bandit11@bandit:~$ ls -a
. .. .bash_logout .bashrc data.txt .profile
bandit11@bandit:~$ cat data.txt | tr 'n-zA-MN-ZA-M' 'a-zA-Z'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$
```

## Level 12 -> level 13:

**Password:** 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

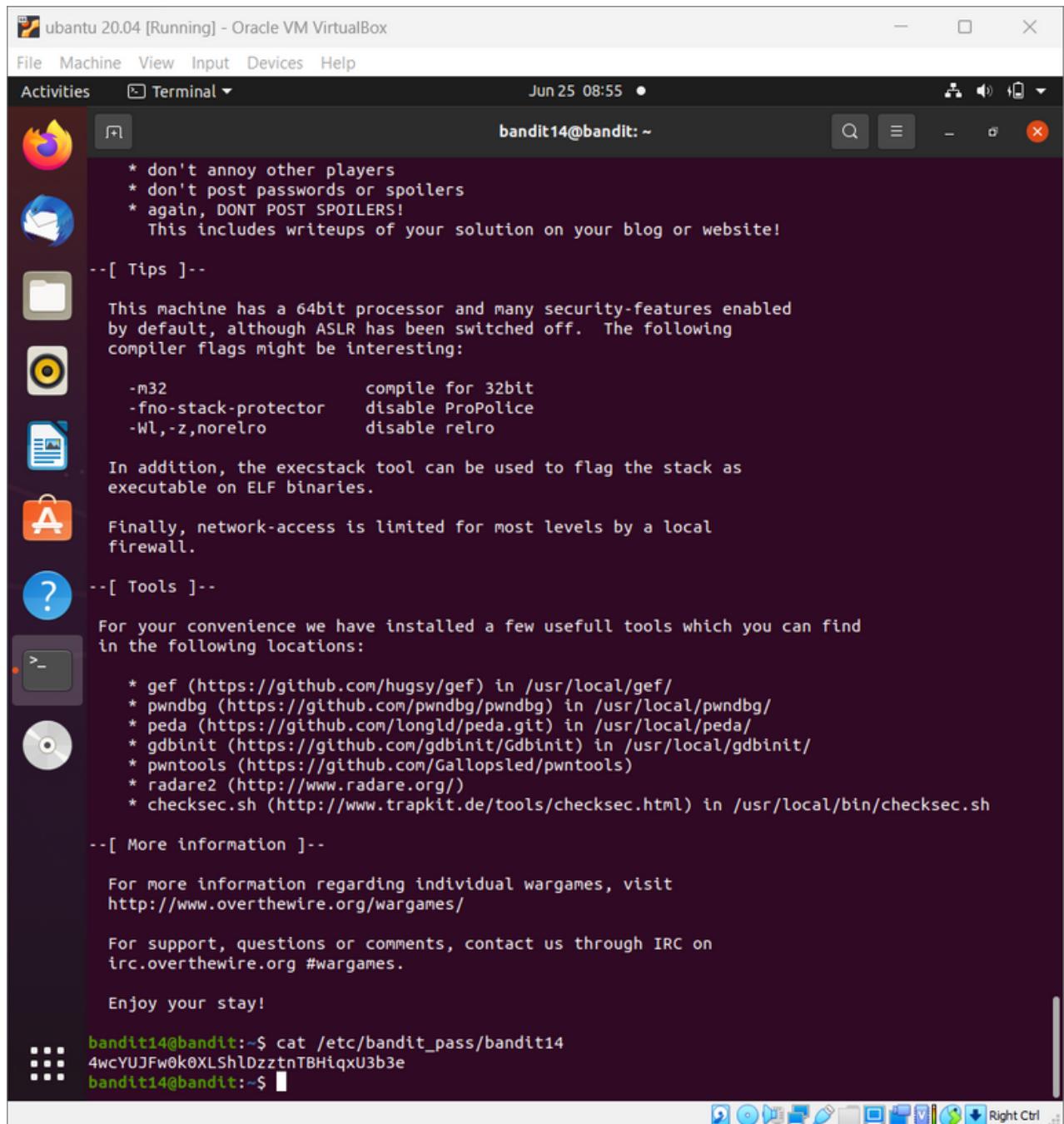


The screenshot shows a desktop environment with a terminal window open. The terminal window title is "bandit12@bandit: /tmp/rajashekhar". The terminal content shows the user attempting to identify files and extracting compressed data. The user runs "file" command on "bandit" and "bandit.gz", which are both found to be gzip compressed data. They then run "ls" to see contents. The user tries to extract "bandit" and "bandit.gz" using "tar xvf" but gets errors because they are not tar archives. They then try "tar xvf bandit" on "data5.bin" and "data6.bin", which are also found to be tar archives. Finally, the user extracts "data8.bin" using "tar xvf data8.bin.out" and finds it is an ASCII text file containing the password "8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL".

```
bandit12@bandit:~/tmp/rajashekhar$ file bandit
bandit: cannot open 'bandit' (No such file or directory)
bandit12@bandit:~/tmp/rajashekhar$ file bandit.gz
bandit.gz: gzip compressed data, was "data4.bin", last modified: Thu May  7 18:14:30 2020, max compression, from Unix
bandit12@bandit:~/tmp/rajashekhar$ file bandit
bandit: cannot open 'bandit' (No such file or directory)
bandit12@bandit:~/tmp/rajashekhar$ gunzip bandit
bandit12@bandit:~/tmp/rajashekhar$ gunzip bandit.gz
gzip: bandit.gz: No such file or directory
bandit12@bandit:~/tmp/rajashekhar$ ls
bandit data.txt
bandit12@bandit:~/tmp/rajashekhar$ file bandit
bandit: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/rajashekhar$ tar xvf bandit
-bash: tarxvf: command not found
bandit12@bandit:~/tmp/rajashekhar$ tar xvf bandit
data5.bin
bandit12@bandit:~/tmp/rajashekhar$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/rajashekhar$ tar xvf data5.bi
tar: data5.bi: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
bandit12@bandit:~/tmp/rajashekhar$ tar xvf data5.bin
data6.bin
bandit12@bandit:~/tmp/rajashekhar$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:~/tmp/rajashekhar$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:~/tmp/rajashekhar$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/rajashekhar$ tar xvf data6.bin.out
data8.bin
bandit12@bandit:~/tmp/rajashekhar$ 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/rajashekhar$ mv data8.bin data8.gz
bandit12@bandit:~/tmp/rajashekhar$ gunzip data8.gz
bandit12@bandit:~/tmp/rajashekhar$ ls
bandit data5.bin data6.bin.out data8 data.txt
bandit12@bandit:~/tmp/rajashekhar$ file data8
data8: ASCII text
bandit12@bandit:~/tmp/rajashekhar$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:~/tmp/rajashekhar$
```

## Level 13 -> level 14:

**Password:** 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e



The screenshot shows a terminal window titled "bandit14@bandit:~" running on an Ubuntu 20.04 desktop. The terminal displays a welcome message for a new user, providing tips and information about the machine's security features and available tools. The message includes instructions for ASLR, compiler flags, execstack, and network access. It also lists several useful tools like gef, pwndbg, peda, gdbinit, pwntools, radare2, and checksec.sh. At the bottom, it provides links for more information and support, and ends with a friendly message. The terminal window is part of the Unity interface, with a dock at the bottom containing icons for various applications.

```
* 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

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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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/

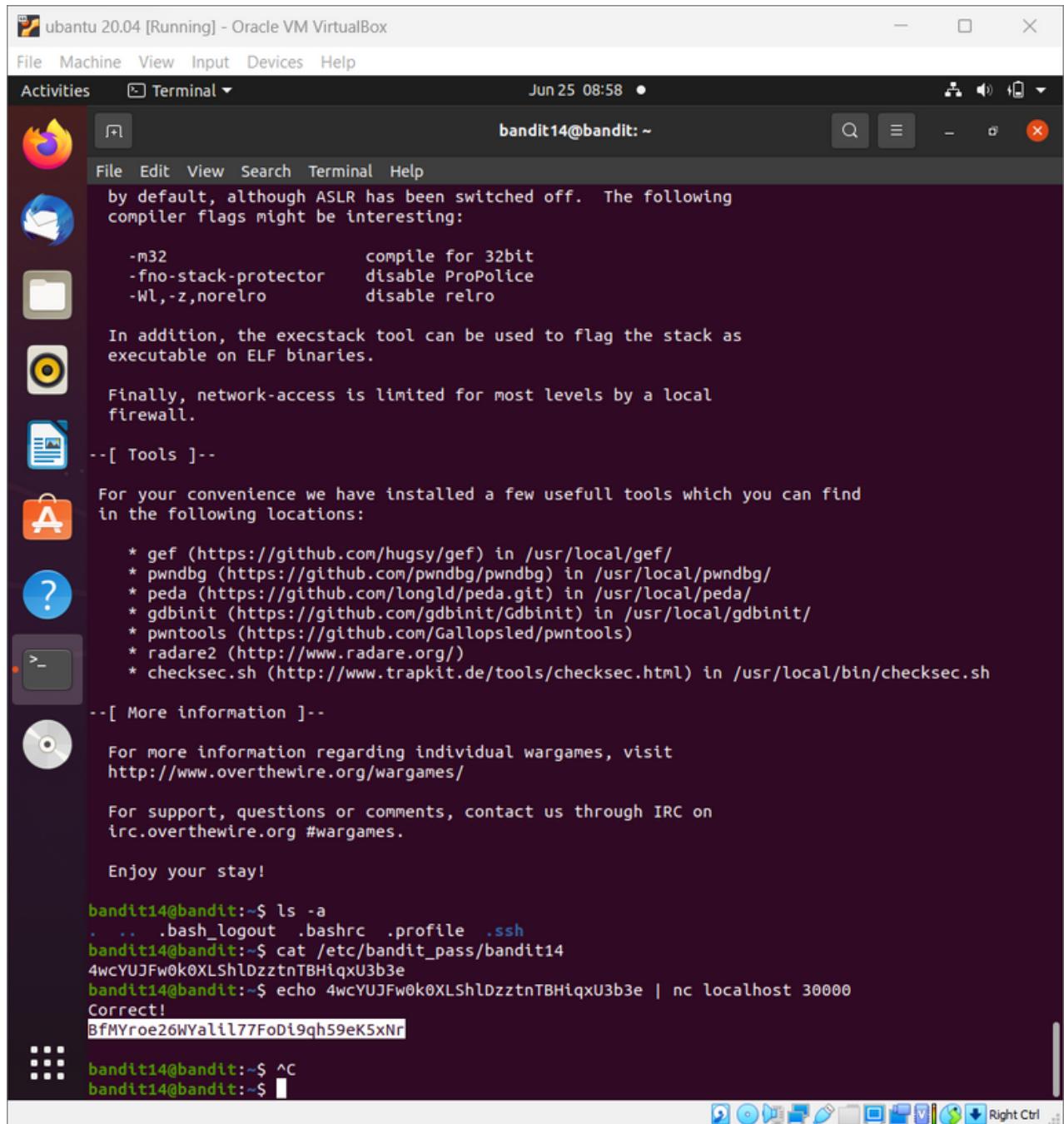
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$
```

## Level 14 -> level 15:

**Password:** BfMYroe26WYalil77FoDi9qh59eK5xNr



The screenshot shows a desktop environment for Ubuntu 20.04 running in Oracle VM VirtualBox. The terminal window is open at the root prompt (bandit14@bandit:~) and displays a welcome message for the Bandit challenge system. The message provides information about ASLR, compiler flags, execstack, network access, and available tools like gef, pwndbg, peda, gdbinit, pwntools, radare2, and checksec.sh. It also links to the OverTheWire wargames website and IRC support. The terminal session ends with the password being echoed back.

```
ubuntu 20.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 25 08:58 •
bandit14@bandit:~ File Edit View Search Terminal Help
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/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* 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/

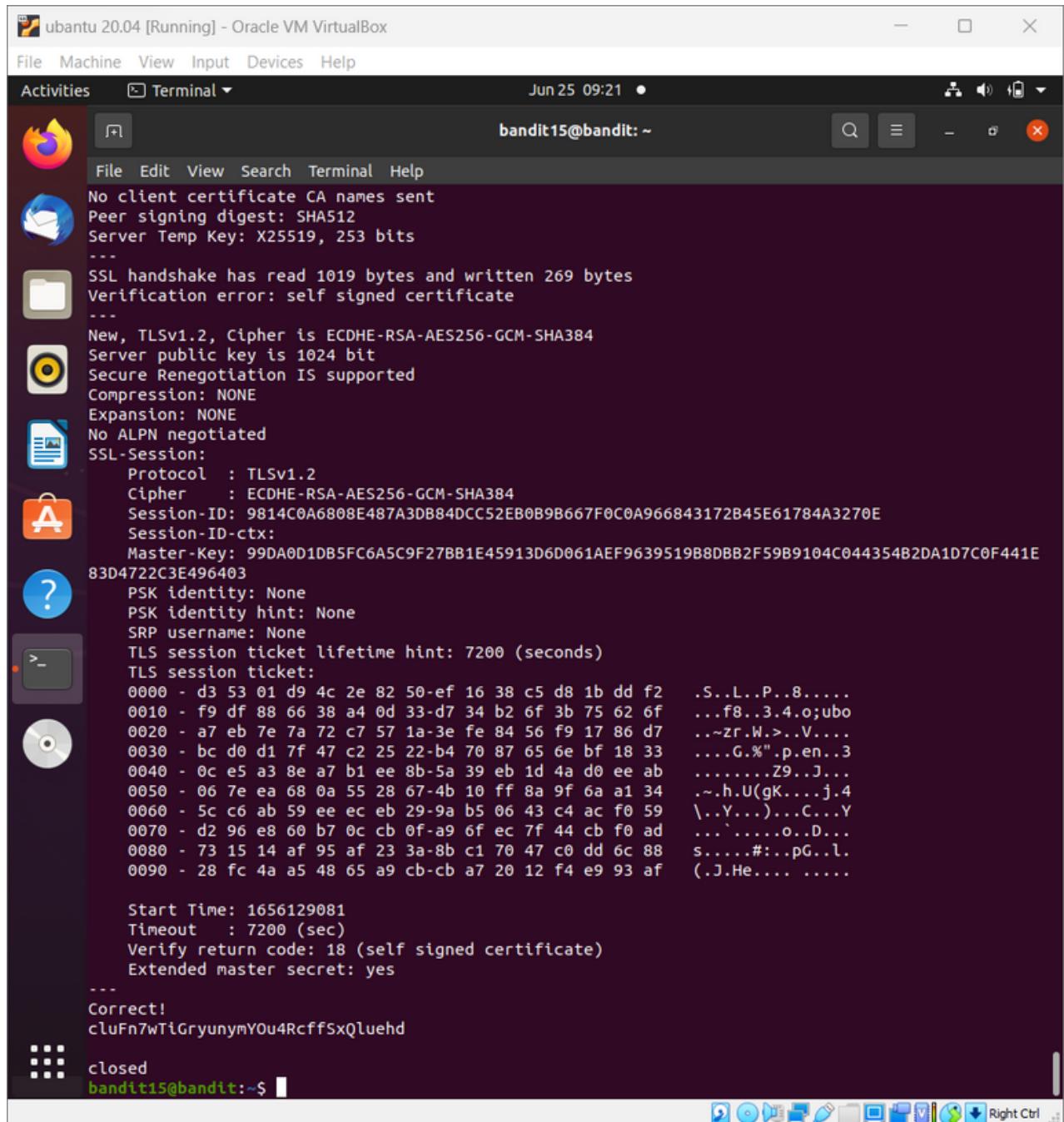
For support, questions or comments, contact us through IRC on
irc.overthewire.org #wargames.

Enjoy your stay!

bandit14@bandit:~$ ls -a
. . . .bash_logout .bashrc .profile .ssh
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ echo 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e | nc localhost 30000
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit14@bandit:~$ ^C
bandit14@bandit:~$
```

## Level 15 -> level 16:

**Password:** cluFn7wTiGryunymY0u4RcffSxQluehd



The screenshot shows a Linux desktop environment running in Oracle VM VirtualBox. The desktop has a dark theme with icons for various applications like a browser, file manager, terminal, and system settings. A terminal window is open, showing the output of a SSL/TLS analysis tool (likely Wireshark or similar) on a session between a client and a server named 'bandit15'. The terminal shows detailed information about the SSL handshake, including the cipher suite (ECDHE-RSA-AES256-GCM-SHA384), session ID, and master key. It also displays the raw hex dump of the TLS session ticket. At the bottom of the terminal, the password 'cluFn7wTiGryunymY0u4RcffSxQluehd' is entered and confirmed as correct.

```
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1019 bytes and written 269 bytes
Verification error: self signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 9814C0A6808E487A3DB84DCC52EB0B9B667F0C0A966843172B45E61784A3270E
    Session-ID-ctx:
        Master-Key: 99DA0D1DB5FC6A5C9F27BB1E45913D6D061AEF9639519B8DBB2F59B9104C044354B2DA1D7C0F441E
83D4722C3E496403
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
        0000 - d3 53 01 d9 4c 2e 82 50-ef 16 38 c5 d8 1b dd f2 .S..L..P..8.....
        0010 - f9 df 88 66 38 a4 0d 33-d7 34 b2 6f 3b 75 62 6f ...f8..3.4.o;ubo
        0020 - a7 eb 7e 7a 72 c7 57 1a-3e fe 84 56 f9 17 86 d7 ...~zr.W.>..V....
        0030 - bc d0 d1 7f 47 c2 25 22-b4 70 87 65 6e bf 18 33 ....G.%".p.en..3
        0040 - 0c e5 a3 8e a7 b1 ee 8b-5a 39 eb 1d 4a d0 ee ab .....Z9..J...
        0050 - 06 7e ea 68 0a 55 28 67-4b 10 ff 8a 9f 6a a1 34 ..~.h.U(gK....j.4
        0060 - 5c c6 ab 59 ee ec eb 29-9a b5 06 43 c4 ac f0 59 \..Y...).C...Y
        0070 - d2 96 e8 60 b7 0c cb 0f-a9 6f ec 7f 44 cb f0 ad ...`.....o.D...
        0080 - 73 15 14 af 95 af 23 3a-8b c1 70 47 c0 dd 6c 88 s....#...pG..l.
        0090 - 28 fc 4a a5 48 65 a9 cb-cb a7 20 12 f4 e9 93 af (.J.He.... .....

    Start Time: 1656129081
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: yes
    ...
    Correct!
    cluFn7wTiGryunymY0u4RcffSxQluehd
closed
bandit15@bandit:~$
```