23 July, 23

BYTEWISE FELLOWSHIP CYBERSECURITY

Bandit Level 11-20

BY: SEERAT E MARRYUM

Bandit Level 10 → Level 11

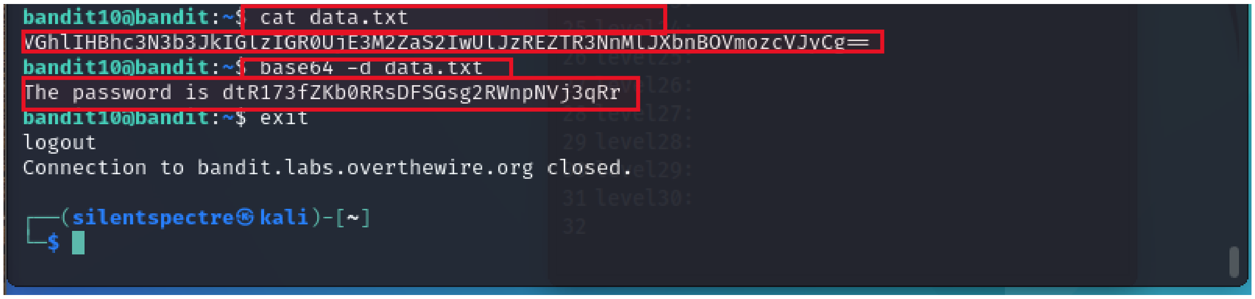
Level Goal

The password for the next level is stored in the file **data.txt**, which contains base64 encoded data

Commands you may need to solve this level

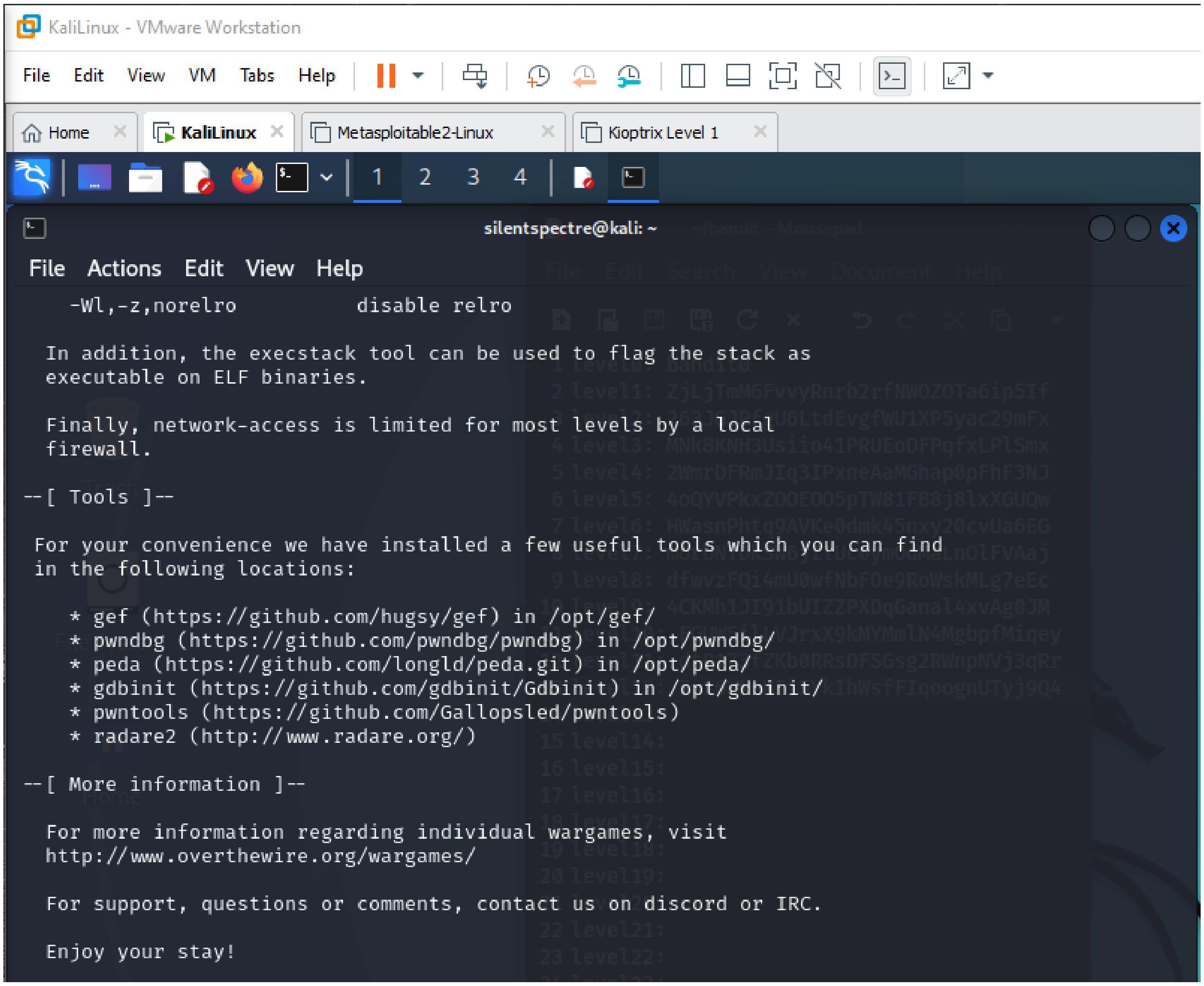
grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

read data.txt, we found the base64 encoded data, so we decode it using this command to get password of next level: **base64 -d data.txt:**



```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
bandit10@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

┌──(silentspectre㉿kali)-[~]
└─$ 
```

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

```
    -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!
```

Bandit Level 11 → Level 12

Level Goal

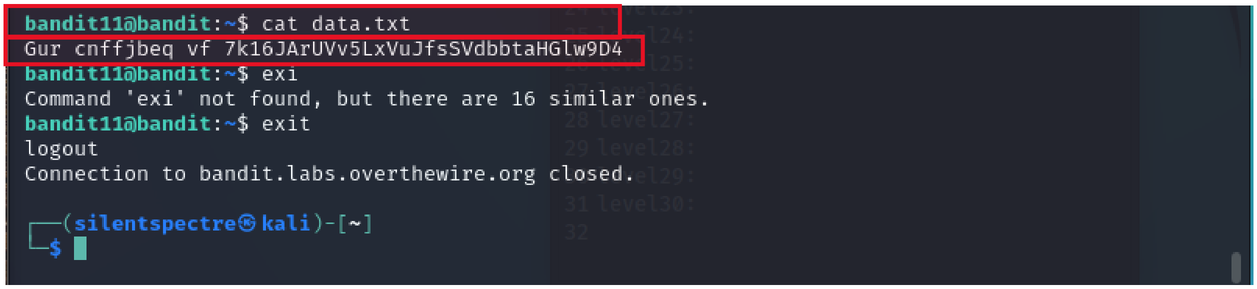
The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

Commands you may need to solve this level

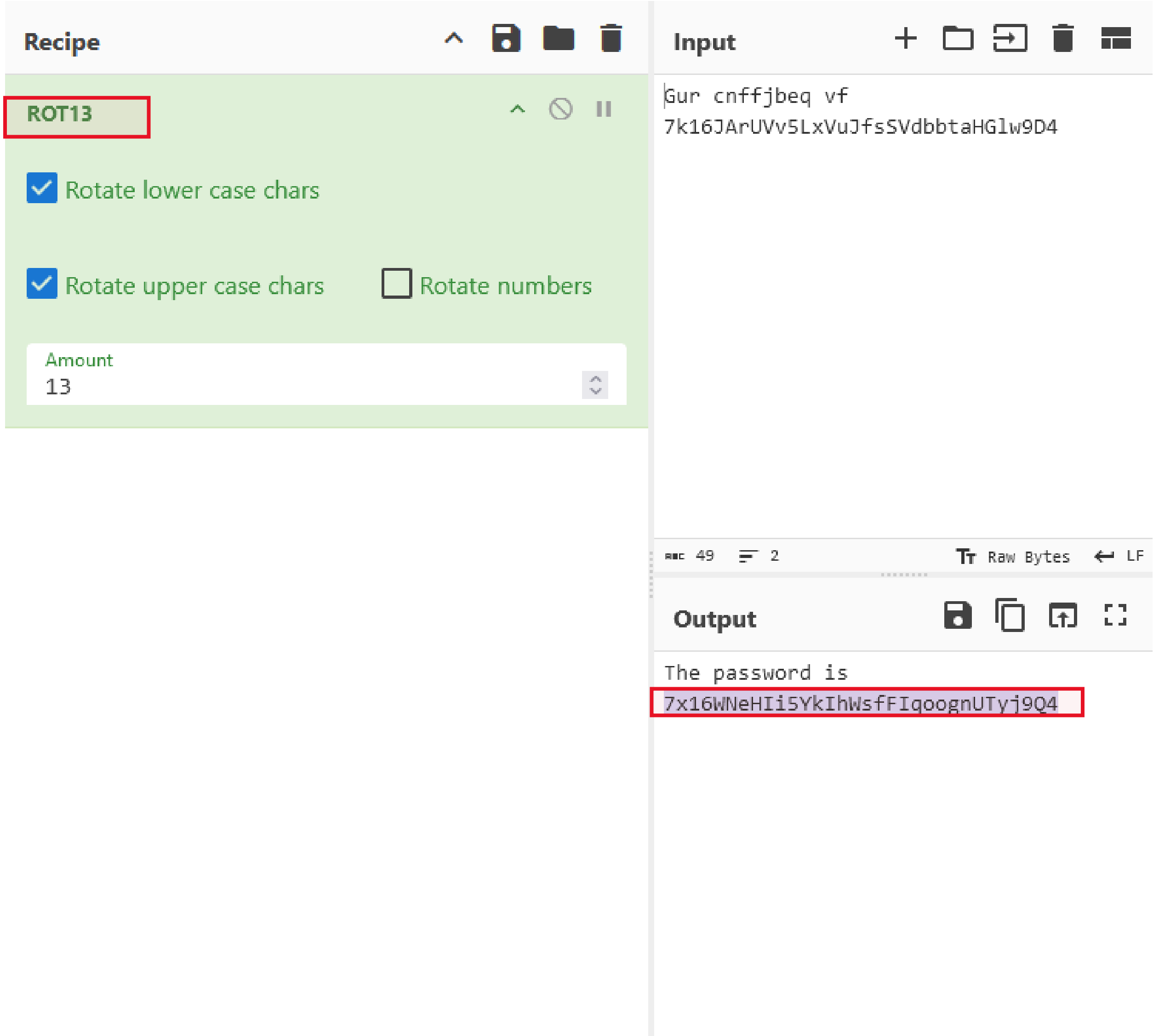
grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd

Read data.txt and we have our password for next level but we have to rot13 this found data to get original password:

23 July, 23



```
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
bandit11@bandit:~$ exi
Command 'exi' not found, but there are 16 similar ones.
bandit11@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.

┌──(silentspectre㉿kali)-[~]
└─$ 
```



ROT13

☑ Rotate lower case chars

☑ Rotate upper case chars □ Rotate numbers

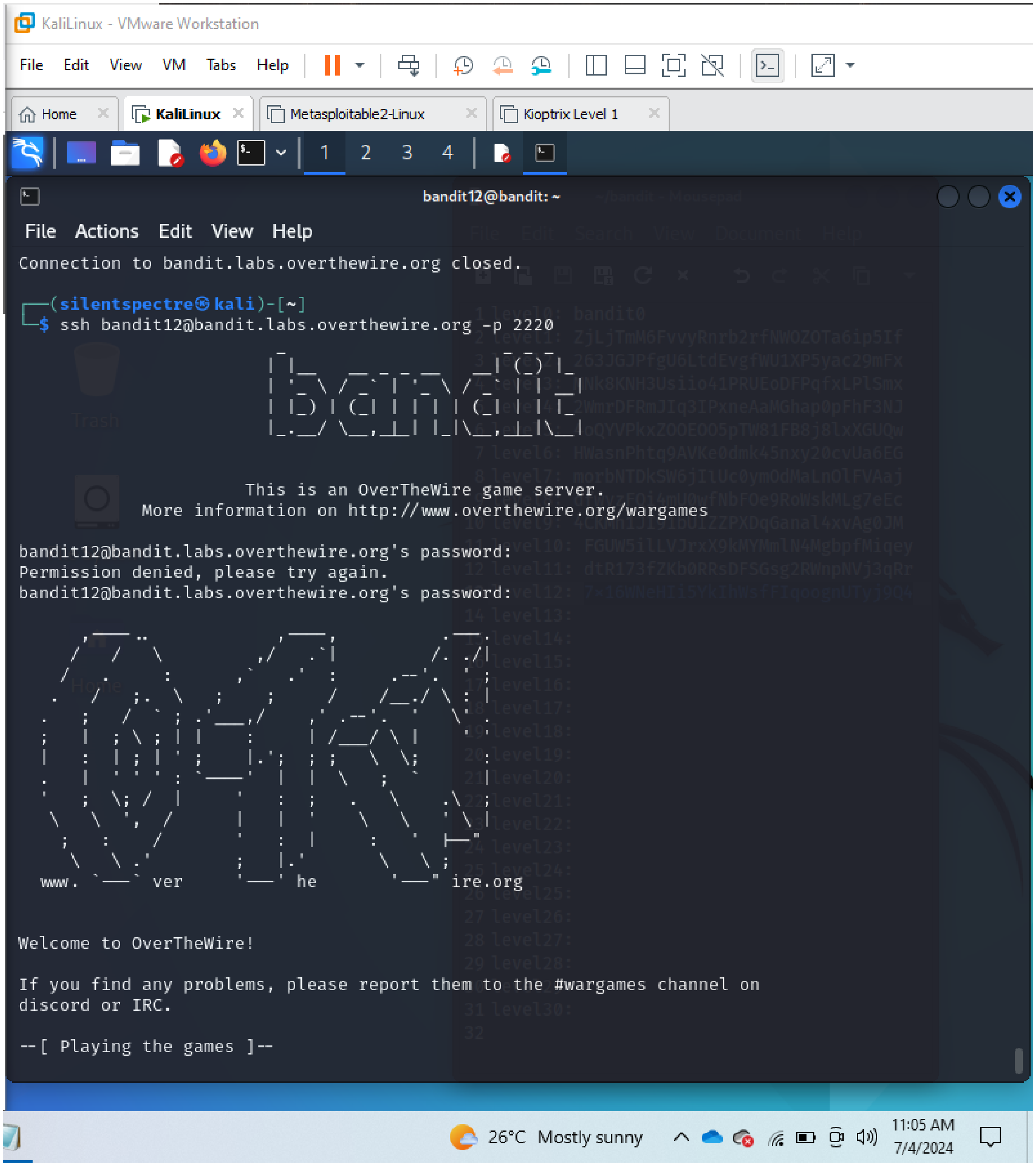
Amount
13

```
Gur cnffjbeq vf
7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
```

49 2

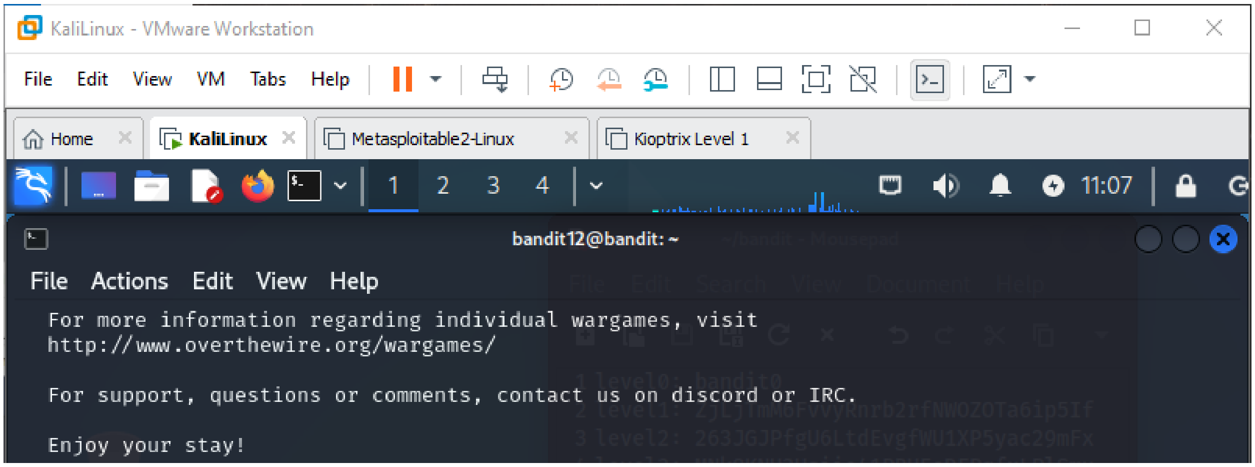
```
The password is
7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
```

23 July, 23



```
Connection to bandit.labs.overthewire.org closed.

┌──(silentspectre㉿kali)-[~]
└─$ ssh bandit12@bandit.labs.overthewire.org -p 2220
                        _                     _ _ _
                       | |__   __ _ _ __   __| (_) |_
                       | '_ \ / _` | '_ \ / _` | | __|
                       | |_) | (_| | | | | (_| | | |_
                       |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit12@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit12@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---`  ver     '---' he       '---" ire.org


Welcome to OverTheWire!

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

--[ Playing the games ]--
```

23 July, 23



```
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!
```

```
level0: bandit0
level1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
level2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

Bandit Level 12 → Level 13

Level Goal

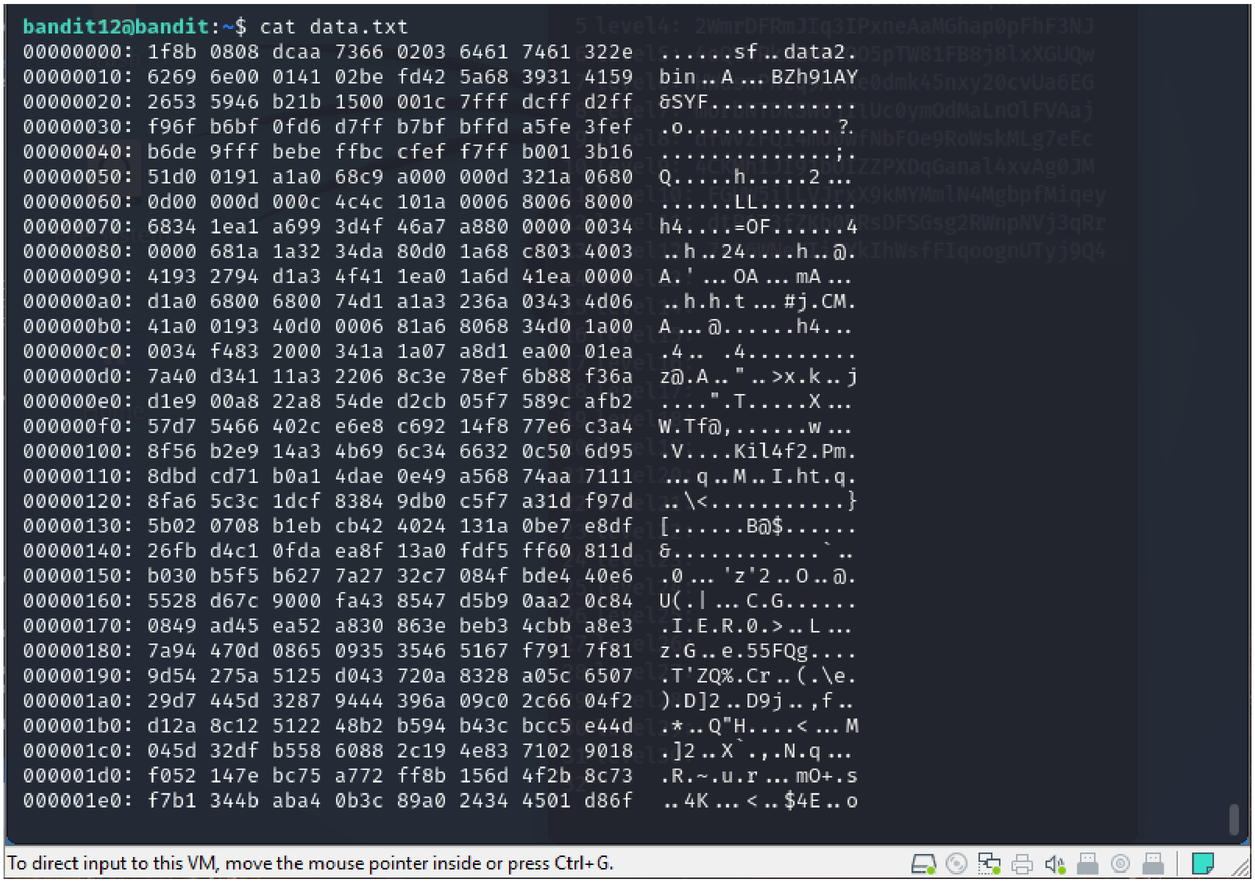
The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work. Use mkdir with a hard to guess directory name. Or better, use the command “mktemp -d”. Then copy the datafile using cp, and rename it using mv (read the manpages!)

Commands you may need to solve this level

grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd, mkdir, cp, mv, file

Read data.txt file:

23 July, 23



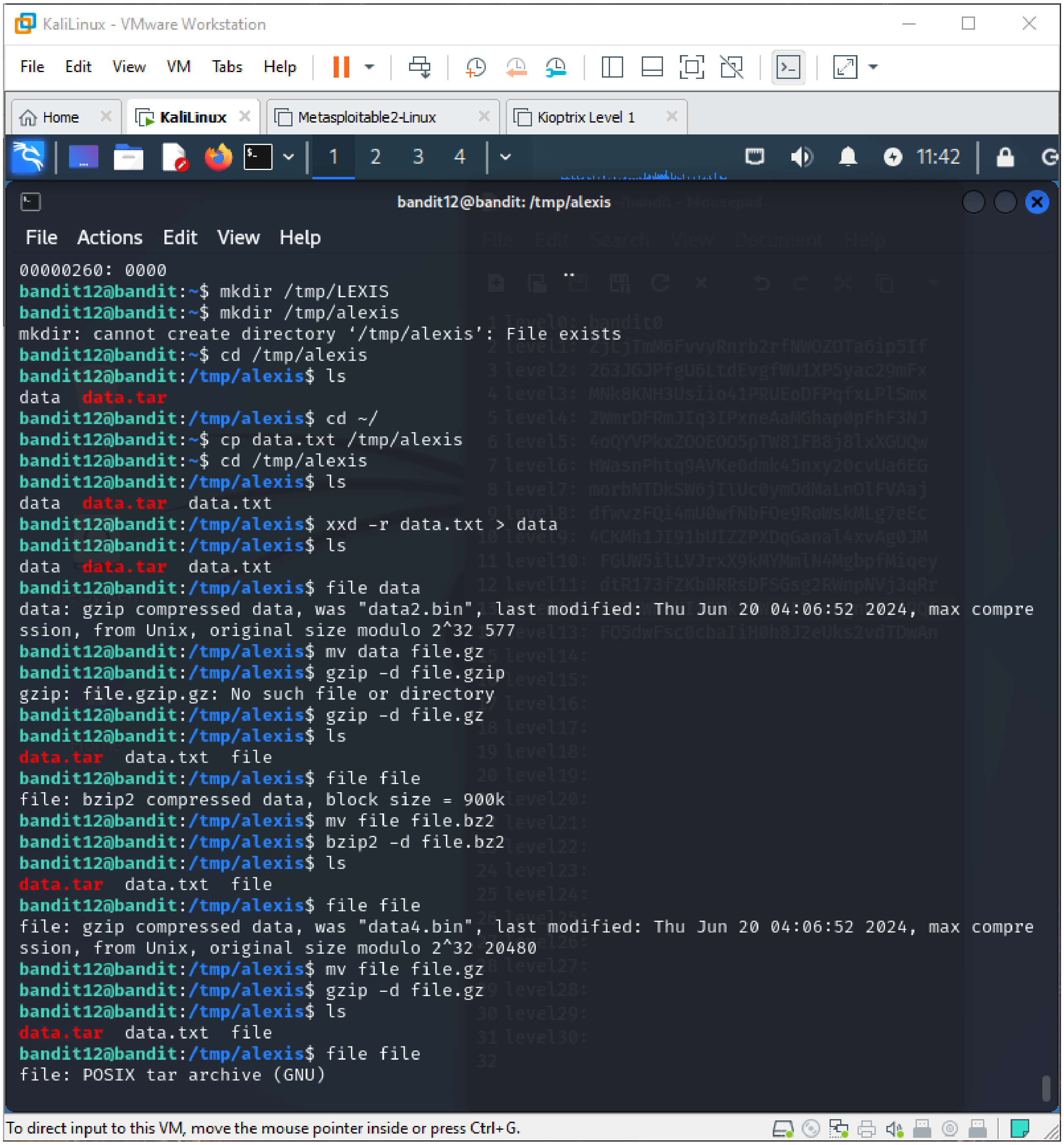
```
bandit12@bandit:~$ cat data.txt
00000000: 1f8b 0808 dcaa 7366 0203 6461 7461 322e  ......sf..data2.
00000010: 6269 6e00 0141 02be fd42 5a68 3931 4159  bin..A...BZh91AY
00000020: 2653 5946 b21b 1500 001c 7fff dcff d2ff  &SYF............
00000030: f96f b6bf 0fd6 d7ff b7bf bffd a5fe 3fef  .o.............?.
00000040: b6de 9fff bebe ffbc cfef f7ff b001 3b16  ..............;.
00000050: 51d0 0191 a1a0 68c9 a000 000d 321a 0680  Q.....h......2...
00000060: 0d00 000d 000c 4c4c 101a 0006 8006 8000  ......LL........
00000070: 6834 1ea1 a699 3d4f 46a7 a880 0000 0034  h4....=OF......4
00000080: 0000 681a 1a32 34da 80d0 1a68 c803 4003  ..h..24....h..@.
00000090: 4193 2794 d1a3 4f41 1ea0 1a6d 41ea 0000  A.'...OA...mA...
000000a0: d1a0 6800 6800 74d1 a1a3 236a 0343 4d06  ..h.h.t...#j.CM.
000000b0: 41a0 0193 40d0 0006 81a6 8068 34d0 1a00  A...@......h4...
000000c0: 0034 f483 2000 341a 1a07 a8d1 ea00 01ea  .4.. .4.........
000000d0: 7a40 d341 11a3 2206 8c3e 78ef 6b88 f36a  z@.A.."..>x.k..j
000000e0: d1e9 00a8 22a8 54de d2cb 05f7 589c afb2  ....".T.....X...
000000f0: 57d7 5466 402c e6e8 c692 14f8 77e6 c3a4  W.Tf@,......w...
00000100: 8f56 b2e9 14a3 4b69 6c34 6632 0c50 6d95  .V....Kil4f2.Pm.
00000110: 8dbd cd71 b0a1 4dae 0e49 a568 74aa 7111  ...q..M..I.ht.q.
00000120: 8fa6 5c3c 1dcf 8384 9db0 c5f7 a31d f97d  ..\<...........}
00000130: 5b02 0708 b1eb cb42 4024 131a 0be7 e8df  [......B@$......
00000140: 26fb d4c1 0fda ea8f 13a0 fdf5 ff60 811d  &............`..
00000150: b030 b5f5 b627 7a27 32c7 084f bde4 40e6  .0...'z'2..O..@.
00000160: 5528 d67c 9000 fa43 8547 d5b9 0aa2 0c84  U(.|...C.G......
00000170: 0849 ad45 ea52 a830 863e beb3 4cbb a8e3  .I.E.R.0.>..L...
00000180: 7a94 470d 0865 0935 3546 5167 f791 7f81  z.G..e.55FQg....
00000190: 9d54 275a 5125 d043 720a 8328 a05c 6507  .T'ZQ%.Cr..(.\e.
000001a0: 29d7 445d 3287 9444 396a 09c0 2c66 04f2  ).D]2..D9j..,f..
000001b0: d12a 8c12 5122 48b2 b594 b43c bcc5 e44d  .*..Q"H....<...M
000001c0: 045d 32df b558 6088 2c19 4e83 7102 9018  .]2..X`.,.N.q...
000001d0: f052 147e bc75 a772 ff8b 156d 4f2b 8c73  .R.~.u.r...mO+.s
000001e0: f7b1 344b aba4 0b3c 89a0 2434 4501 d86f  ..4K...<..$4E..o
```

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

Make directory /tmp/alexeis, copy data.txt into directory /tmp/alexis, go to /tmp/alexis and list the files there, data.txt contains a hex dump (or hexadecimal representation of binary data). The **xxd -r data.txt > data** command will convert this hex dump back into its original binary form. and save it as data. Now we see file type of data. its gzip file. Renames or moves the file data to file.gz, decompress a file that has been compressed using gzip**,** then list out the files and we have new file named as file, see its type, its in bzip2 format , so we repeat the above steps till we got

23 July, 23

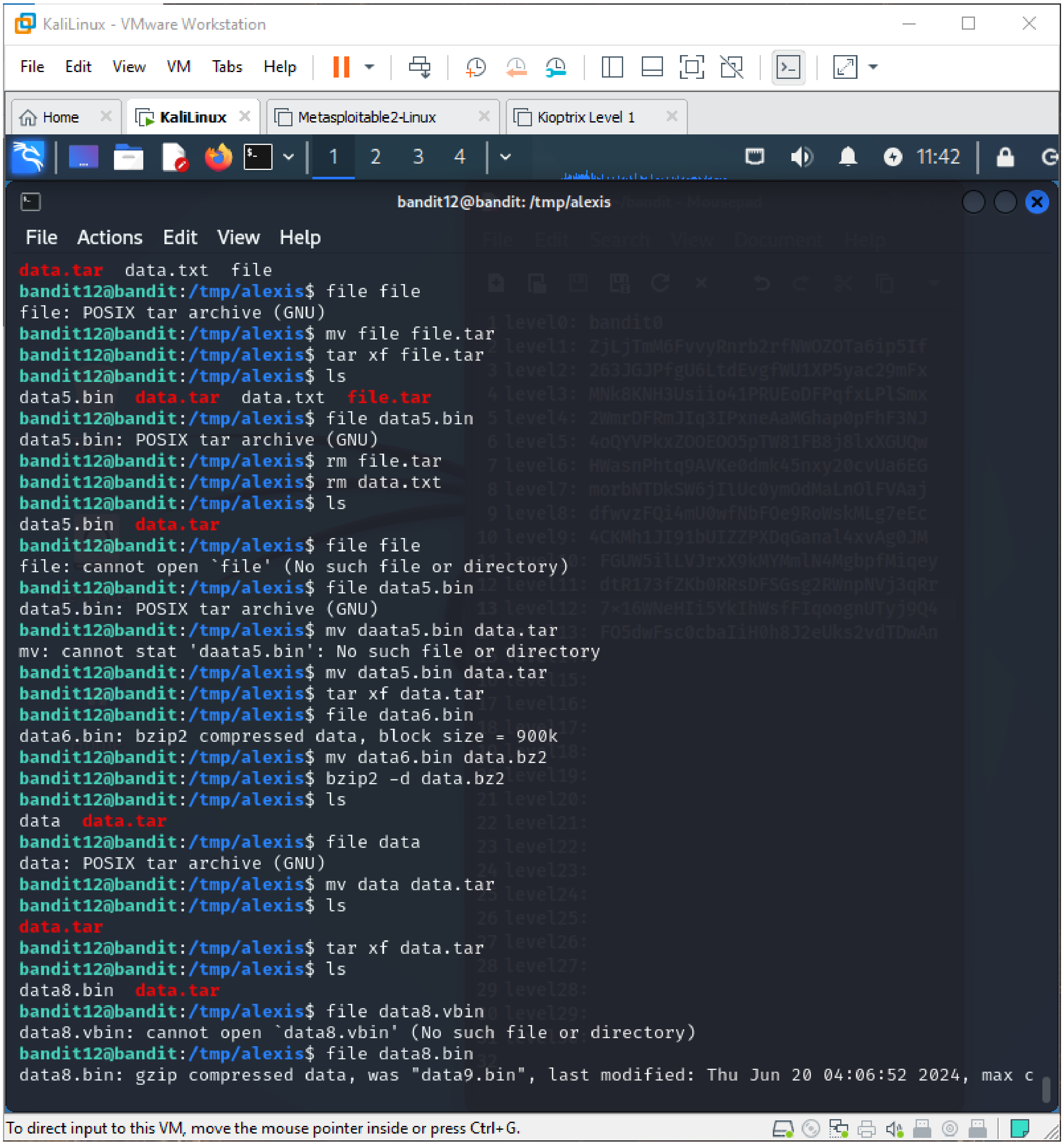
our file data containing password to next level:



KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
11:42
bandit12@bandit: /tmp/alexis
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

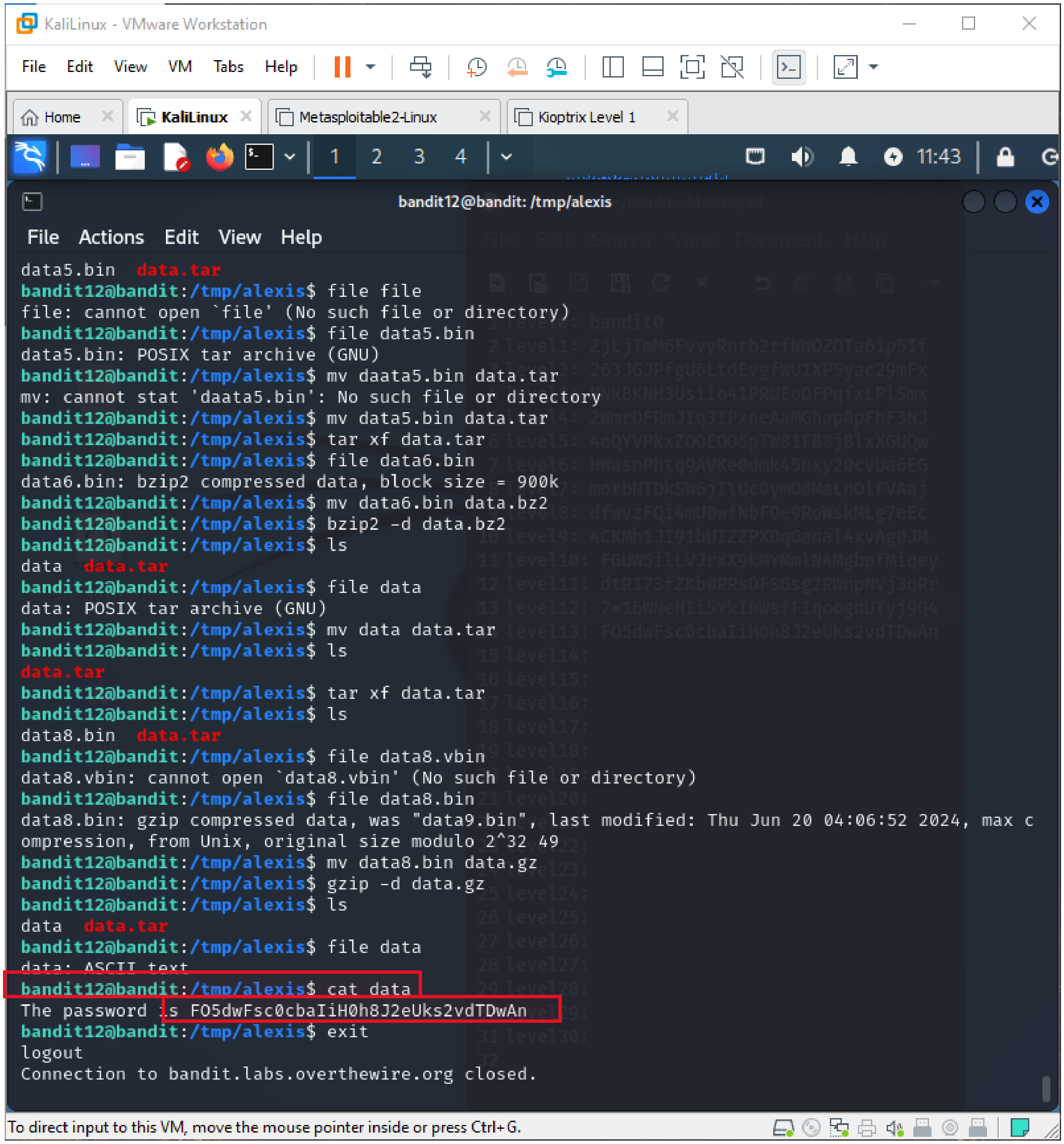
```
00000260: 0000
bandit12@bandit:~$ mkdir /tmp/LEXIS
bandit12@bandit:~$ mkdir /tmp/alexis
mkdir: cannot create directory ‘/tmp/alexis’: File exists
bandit12@bandit:~$ cd /tmp/alexis
bandit12@bandit:/tmp/alexis$ ls
data  data.tar
bandit12@bandit:/tmp/alexis$ cd ~/
bandit12@bandit:~$ cp data.txt /tmp/alexis
bandit12@bandit:~$ cd /tmp/alexis
bandit12@bandit:/tmp/alexis$ ls
data  data.tar  data.txt
bandit12@bandit:/tmp/alexis$ xxd -r data.txt > data
bandit12@bandit:/tmp/alexis$ ls
data  data.tar  data.txt
bandit12@bandit:/tmp/alexis$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Jun 20 04:06:52 2024, max compre
ssion, from Unix, original size modulo 2^32 577
bandit12@bandit:/tmp/alexis$ mv data file.gz
bandit12@bandit:/tmp/alexis$ gzip -d file.gzip
gzip: file.gzip.gz: No such file or directory
bandit12@bandit:/tmp/alexis$ gzip -d file.gz
bandit12@bandit:/tmp/alexis$ ls
data.tar  data.txt  file
bandit12@bandit:/tmp/alexis$ file file
file: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/alexis$ mv file file.bz2
bandit12@bandit:/tmp/alexis$ bzip2 -d file.bz2
bandit12@bandit:/tmp/alexis$ ls
data.tar  data.txt  file
bandit12@bandit:/tmp/alexis$ file file
file: gzip compressed data, was "data4.bin", last modified: Thu Jun 20 04:06:52 2024, max compre
ssion, from Unix, original size modulo 2^32 20480
bandit12@bandit:/tmp/alexis$ mv file file.gz
bandit12@bandit:/tmp/alexis$ gzip -d file.gz
bandit12@bandit:/tmp/alexis$ ls
data.tar  data.txt  file
bandit12@bandit:/tmp/alexis$ file file
file: POSIX tar archive (GNU)
```

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
11:42
bandit12@bandit: /tmp/alexis
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

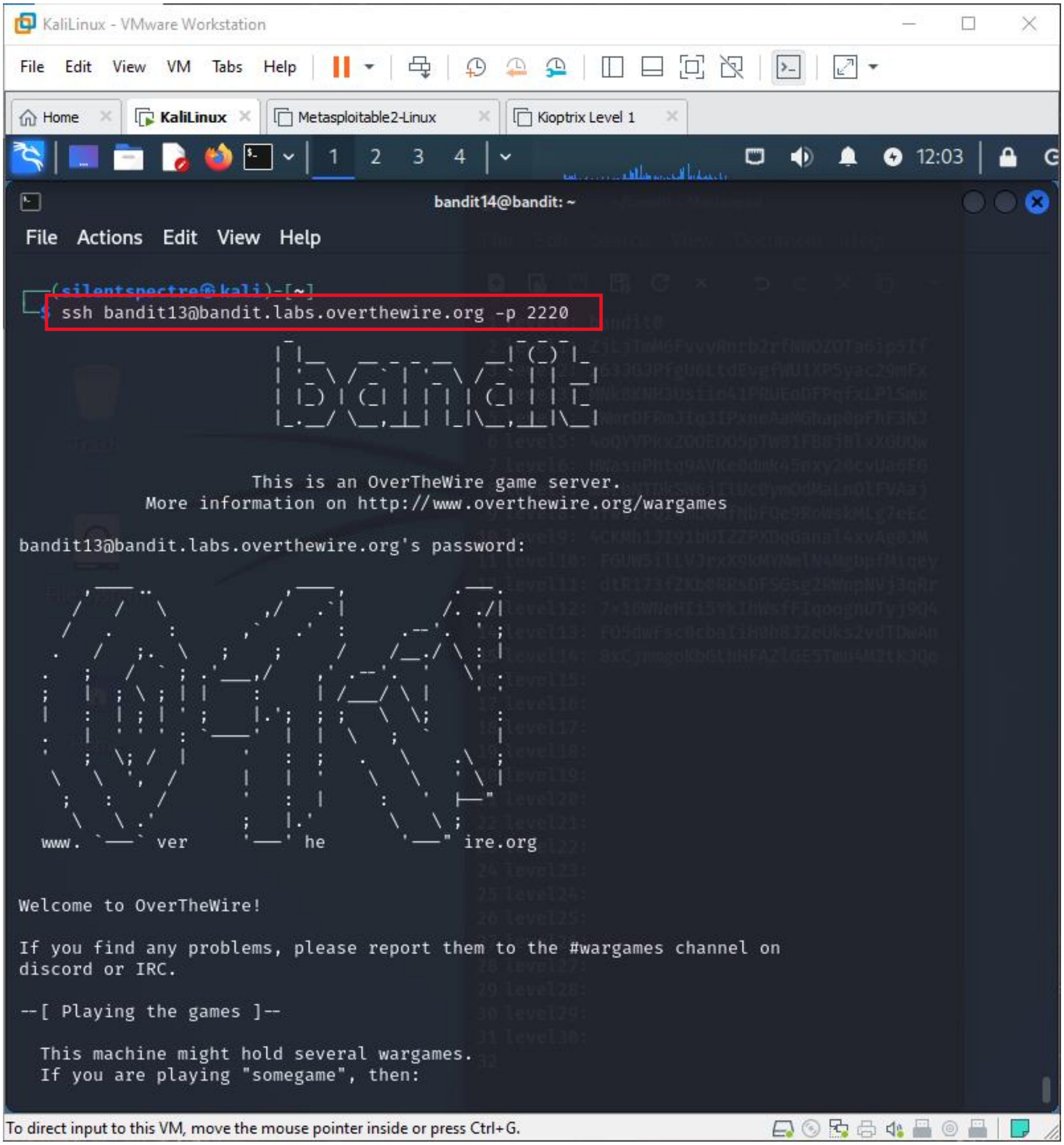
```
data.tar  data.txt  file
bandit12@bandit:/tmp/alexis$ file file
file: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alexis$ mv file file.tar
bandit12@bandit:/tmp/alexis$ tar xf file.tar
bandit12@bandit:/tmp/alexis$ ls
data5.bin  data.tar  data.txt  file.tar
bandit12@bandit:/tmp/alexis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alexis$ rm file.tar
bandit12@bandit:/tmp/alexis$ rm data.txt
bandit12@bandit:/tmp/alexis$ ls
data5.bin  data.tar
bandit12@bandit:/tmp/alexis$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/alexis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alexis$ mv daata5.bin data.tar
mv: cannot stat 'daata5.bin': No such file or directory
bandit12@bandit:/tmp/alexis$ mv data5.bin data.tar
bandit12@bandit:/tmp/alexis$ tar xf data.tar
bandit12@bandit:/tmp/alexis$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/alexis$ mv data6.bin data.bz2
bandit12@bandit:/tmp/alexis$ bzip2 -d data.bz2
bandit12@bandit:/tmp/alexis$ ls
data  data.tar
bandit12@bandit:/tmp/alexis$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alexis$ mv data data.tar
bandit12@bandit:/tmp/alexis$ ls
data.tar
bandit12@bandit:/tmp/alexis$ tar xf data.tar
bandit12@bandit:/tmp/alexis$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/alexis$ file data8.vbin
data8.vbin: cannot open `data8.vbin' (No such file or directory)
bandit12@bandit:/tmp/alexis$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Jun 20 04:06:52 2024, max c
```

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
11:43
bandit12@bandit: /tmp/alexis
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
data5.bin  data.tar
bandit12@bandit:/tmp/alexis$ file file
file: cannot open `file' (No such file or directory)
bandit12@bandit:/tmp/alexis$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alexis$ mv daata5.bin data.tar
mv: cannot stat 'daata5.bin': No such file or directory
bandit12@bandit:/tmp/alexis$ mv data5.bin data.tar
bandit12@bandit:/tmp/alexis$ tar xf data.tar
bandit12@bandit:/tmp/alexis$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/alexis$ mv data6.bin data.bz2
bandit12@bandit:/tmp/alexis$ bzip2 -d data.bz2
bandit12@bandit:/tmp/alexis$ ls
data  data.tar
bandit12@bandit:/tmp/alexis$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/alexis$ mv data data.tar
bandit12@bandit:/tmp/alexis$ ls
data.tar
bandit12@bandit:/tmp/alexis$ tar xf data.tar
bandit12@bandit:/tmp/alexis$ ls
data8.bin  data.tar
bandit12@bandit:/tmp/alexis$ file data8.vbin
data8.vbin: cannot open `data8.vbin' (No such file or directory)
bandit12@bandit:/tmp/alexis$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Jun 20 04:06:52 2024, max c
ompression, from Unix, original size modulo 2^32 49
bandit12@bandit:/tmp/alexis$ mv data8.bin data.gz
bandit12@bandit:/tmp/alexis$ gzip -d data.gz
bandit12@bandit:/tmp/alexis$ ls
data  data.tar
bandit12@bandit:/tmp/alexis$ file data
data: ASCII text
bandit12@bandit:/tmp/alexis$ cat data
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
bandit12@bandit:/tmp/alexis$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```

23 July, 23

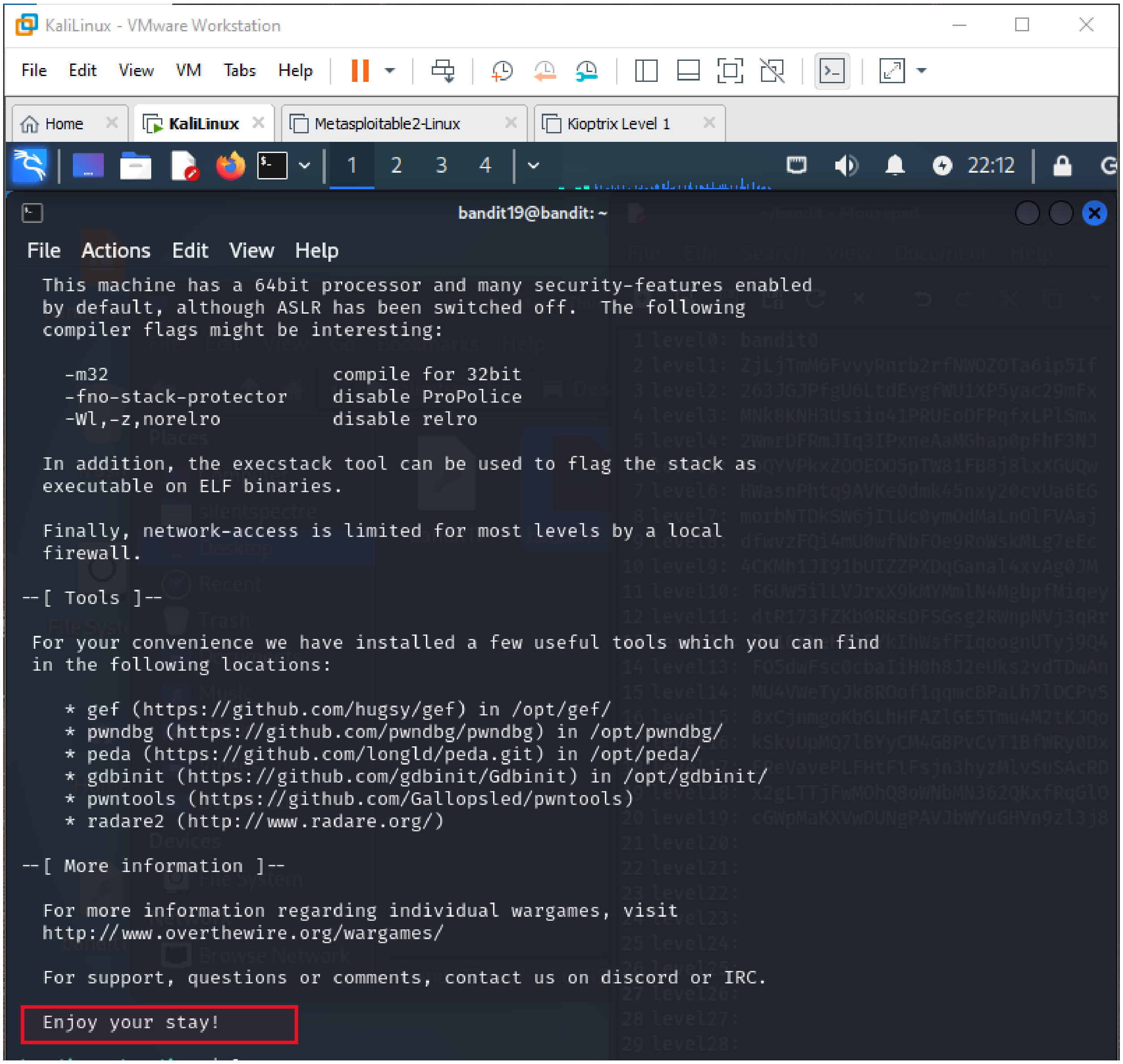


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
12:03
bandit14@bandit: ~
File Actions Edit View Help

```
┌──(silentspectre㉿kali)-[~]
└─$ ssh bandit13@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit13@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |     '   :  ;   .   \    .\  ;
   \   \  ',  /      |   |  '    \   \   ' \ |
    ;   :    /       '   :  |     :   '  |--"
     \   \ .'        ;   |.'       \   \ ;
  www. `---` ver     '---' he       '---" ire.org


Welcome to OverTheWire!

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

--[ Playing the games ]--

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

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

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:12
bandit19@bandit: ~
File Actions Edit View Help

```
  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!
```

Bandit Level 13 → Level 14

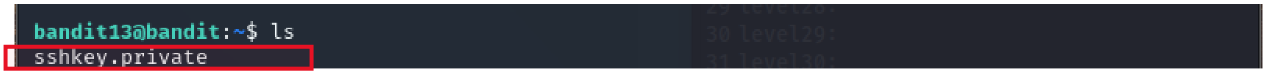
Level Goal

The password for the next level is stored in **/etc/bandit_pass/bandit14 and can only be read by user bandit14**. For this level, you don’t get the next password, but you get a private SSH key that can be used to log into the next level. **Note: localhost** is a hostname that refers to the machine you are working on

Commands you may need to solve this level

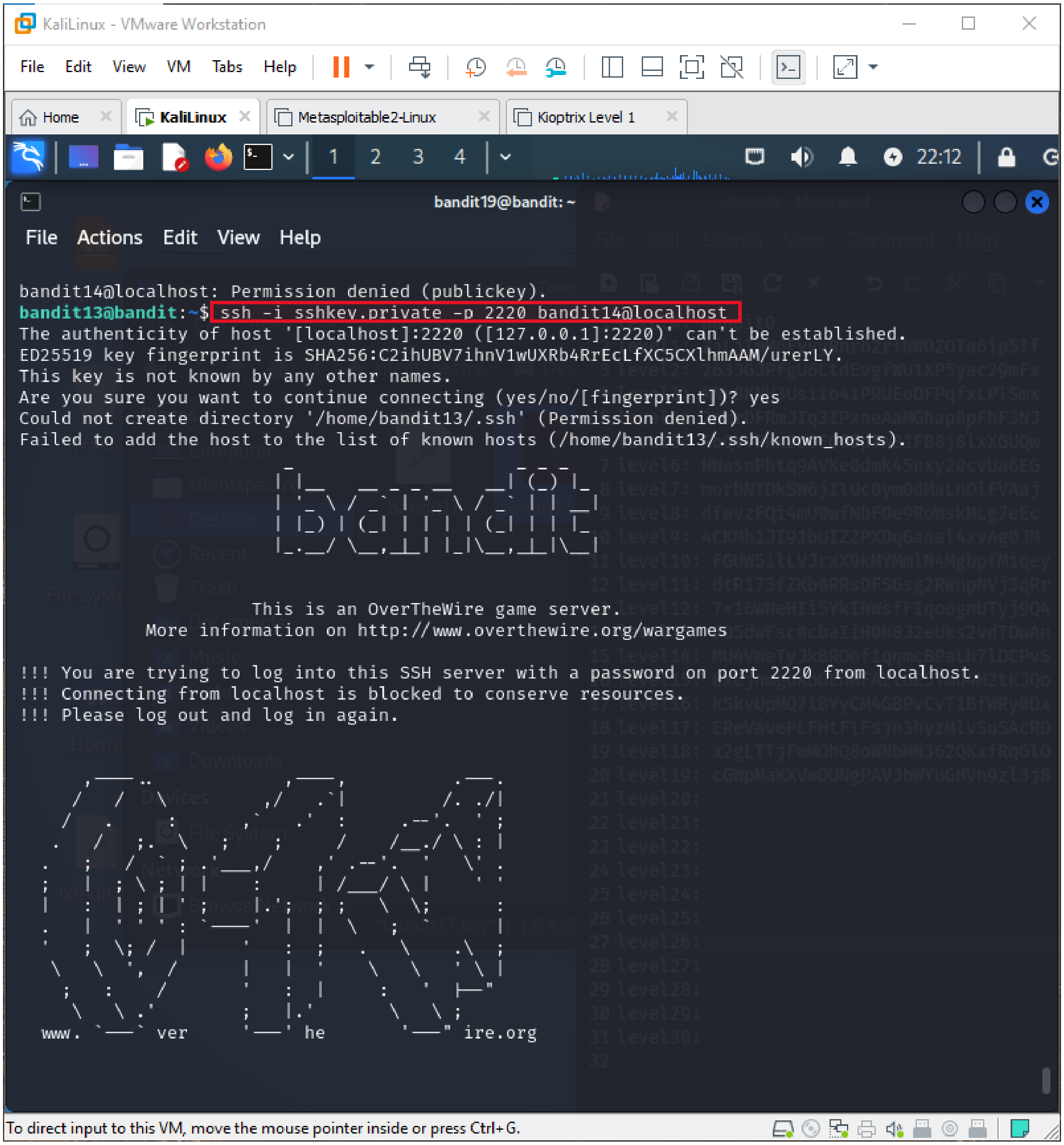
23 July, 23

ssh, telnet, nc, openssl, s_client, nmap



```
bandit13@bandit:~$ ls
sshkey.private
```

Establish an SSH connection to a remote host using the private key sshkey.private to authenticate as user bandit14: **ssh -i sshkey.private -p 2220 bandit14@localhost**


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:12
bandit19@bandit: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
bandit14@localhost: Permission denied (publickey).
bandit13@bandit:~$ ssh -i sshkey.private -p 2220 bandit14@localhost
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).

                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.


      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,'.--'.  '   \' .
  ;   |  ; \ ; | |    :     |/___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ;;   \  \;      :
  .   |  ' ' ' : `----'  |  | \   ;  `      |
  '   ;  \; /  |     '   :  ;  .   \    .\  ;
   \   \  ',  /      |   |  '   \   \   ' \ |
    ;   :    /       '   :  |    :   '  |--"
     \   \ .'        ;   |.'      \   \ ;
  www. `---` ver     '---' he      '---" ire.org
```

23 July, 23

Bandit Level 14 → Level 15

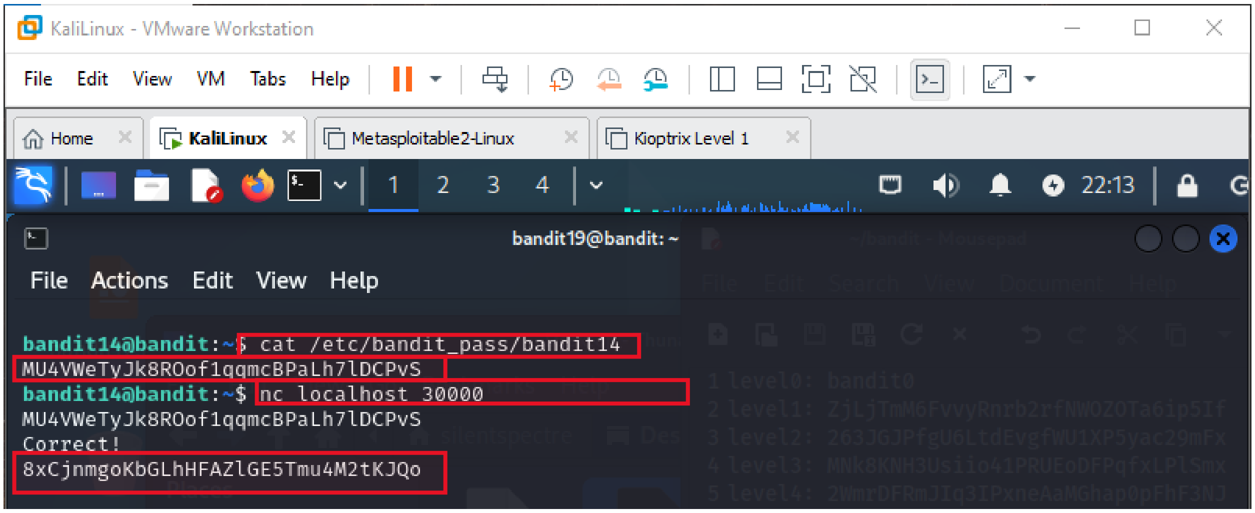
Level Goal

The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

Commands you may need to solve this level

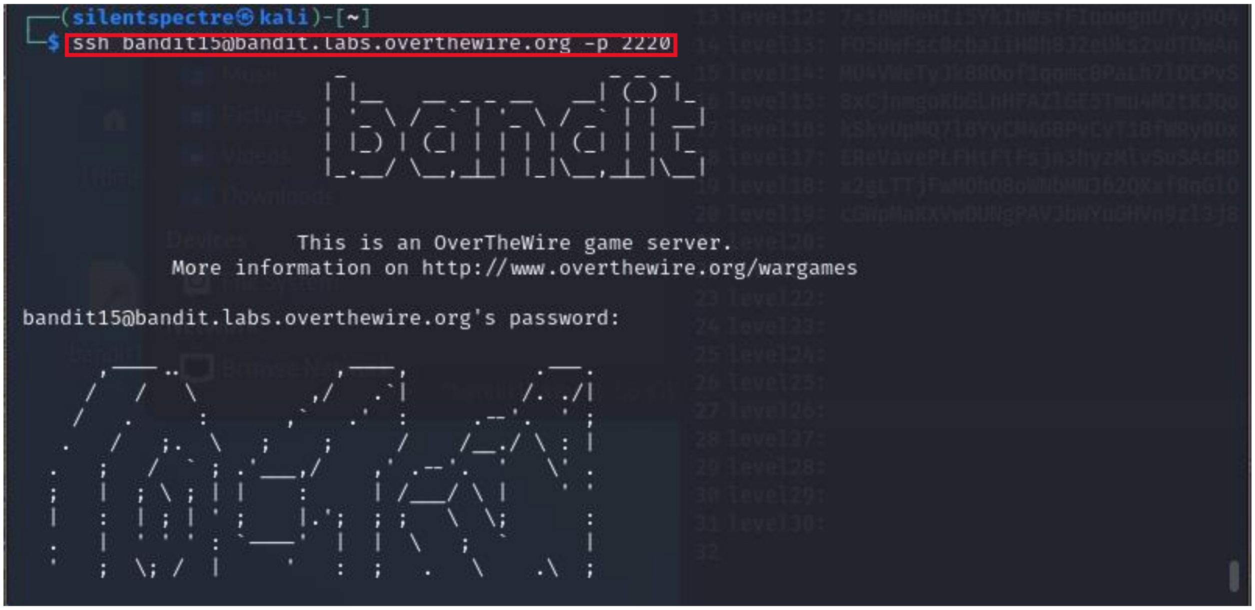
ssh, telnet, nc, openssl, s_client, nmap

See the password of bandit14 located in file **/etc/bandit_pass/bandit14.** Use Netcat to open a connection to port 30000 on localhost and use that password to login there and once authentication is complete we get password to bandit15:


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:13
bandit19@bandit: ~
File Actions Edit View Help

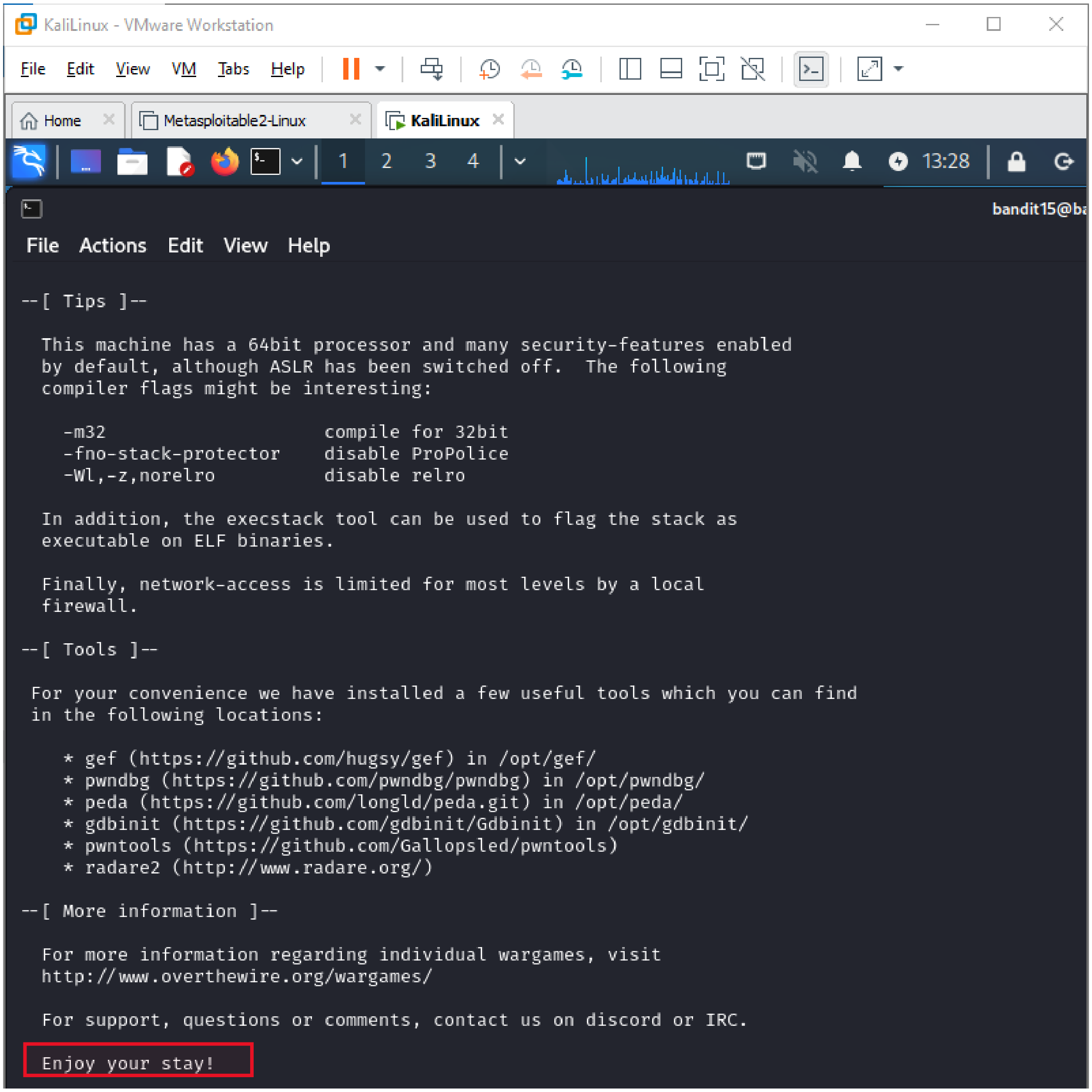
```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

23 July, 23



```
┌──(silentspectre㉿kali)-[~]
└─$ ssh bandit15@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit15@bandit.labs.overthewire.org's password:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'.  ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ;   ;   \  \;      :
  .   |  ' ' ' : `----'  |  |    \   ;  `      |
  '   ;  \; /  |     '   :  ;     .   \    .\  ;
```

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
13:28
bandit15@ba
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!
```

Bandit Level 15 → Level 16

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.

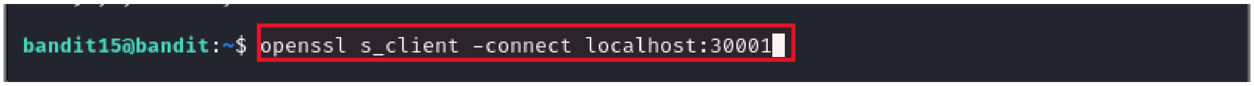
23 July, 23

Helpful note: Getting “HEARTBEATING” and “Read R BLOCK”? Use -ign_eof and read the “CONNECTED COMMANDS” section in the manpage. Next to ‘R’ and ‘Q’, the ‘B’ command also works in this version of that command…

Commands you may need to solve this level

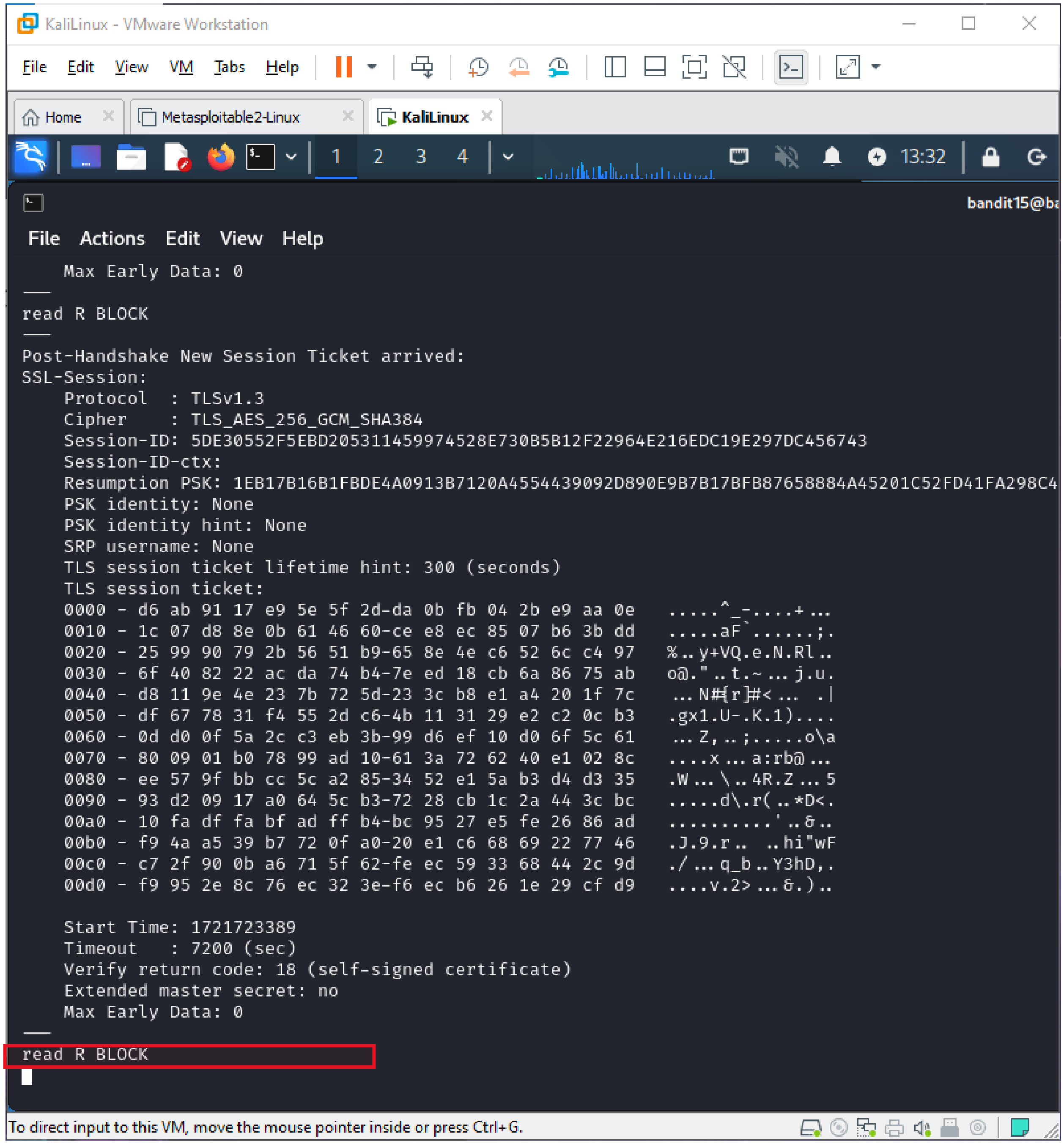
ssh, telnet, nc, openssl, s_client, nmap

Using Netcat will open a connection to port 30000 on localhost:



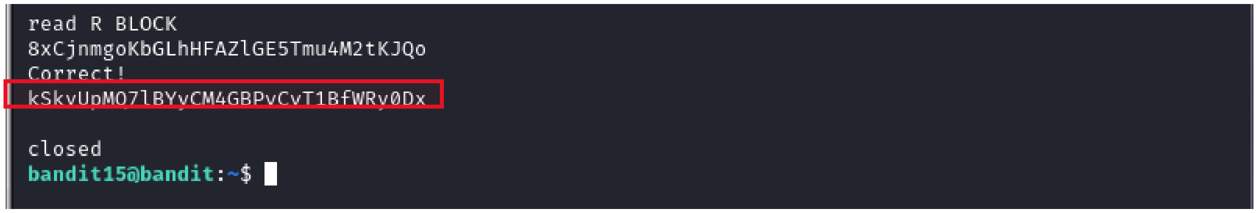
```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
```

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
13:32
bandit15@ba
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

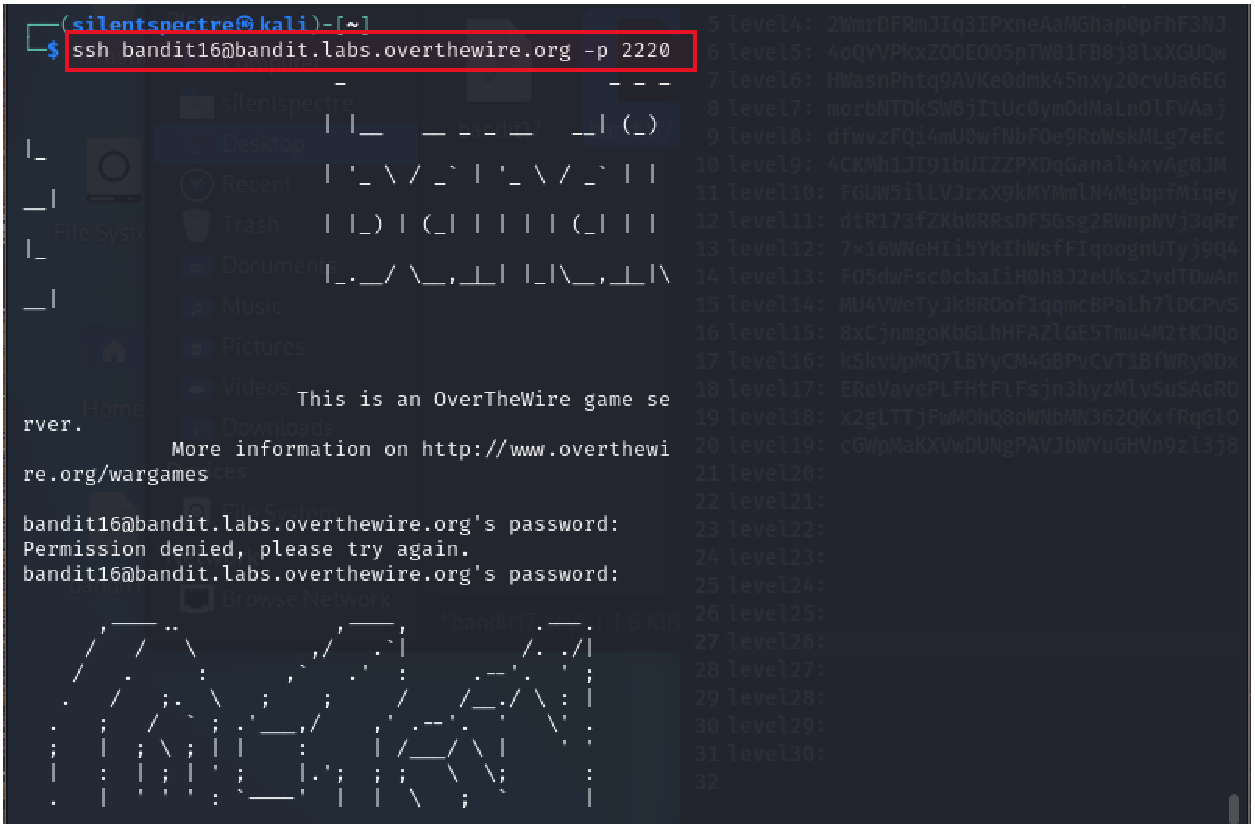
```
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 5DE30552F5EBD205311459974528E730B5B12F22964E216EDC19E297DC456743
    Session-ID-ctx:
    Resumption PSK: 1EB17B16B1FBDE4A0913B7120A4554439092D890E9B7B17BFB87658884A45201C52FD41FA298C4
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - d6 ab 91 17 e9 5e 5f 2d-da 0b fb 04 2b e9 aa 0e   .....^_-....+...
    0010 - 1c 07 d8 8e 0b 61 46 60-ce e8 ec 85 07 b6 3b dd   .....aF`......;.
    0020 - 25 99 90 79 2b 56 51 b9-65 8e 4e c6 52 6c c4 97   %..y+VQ.e.N.Rl..
    0030 - 6f 40 82 22 ac da 74 b4-7e ed 18 cb 6a 86 75 ab   o@."..t.~...j.u.
    0040 - d8 11 9e 4e 23 7b 72 5d-23 3c b8 e1 a4 20 1f 7c   ...N#{r]#<... .|
    0050 - df 67 78 31 f4 55 2d c6-4b 11 31 29 e2 c2 0c b3   .gx1.U-.K.1)....
    0060 - 0d d0 0f 5a 2c c3 eb 3b-99 d6 ef 10 d0 6f 5c 61   ...Z,..;.....o\a
    0070 - 80 09 01 b0 78 99 ad 10-61 3a 72 62 40 e1 02 8c   ....x...a:rb@...
    0080 - ee 57 9f bb cc 5c a2 85-34 52 e1 5a b3 d4 d3 35   .W...\..4R.Z...5
    0090 - 93 d2 09 17 a0 64 5c b3-72 28 cb 1c 2a 44 3c bc   .....d\.r(..*D<.
    00a0 - 10 fa df fa bf ad ff b4-bc 95 27 e5 fe 26 86 ad   ..........'..&..
    00b0 - f9 4a a5 39 b7 72 0f a0-20 e1 c6 68 69 22 77 46   .J.9.r.. ..hi"wF
    00c0 - c7 2f 90 0b a6 71 5f 62-fe ec 59 33 68 44 2c 9d   ./...q_b..Y3hD,.
    00d0 - f9 95 2e 8c 76 ec 32 3e-f6 ec b6 26 1e 29 cf d9   ....v.2>...&.)..

    Start Time: 1721723389
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
```

Paste the password for last level to get the password for next level:



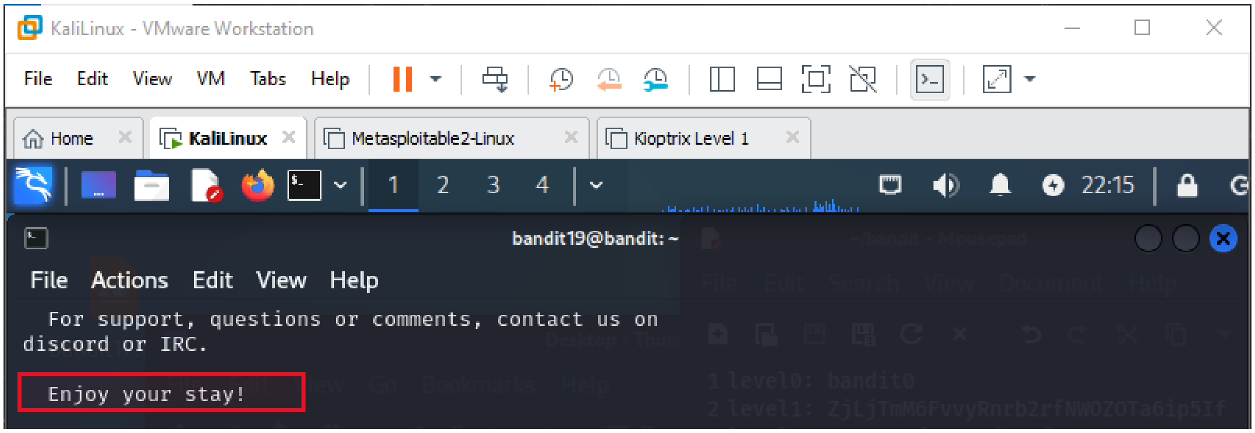
```
read R BLOCK
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$
```

23 July, 23



```
┌──(silentspectre㉿kali)-[~]
└─$ ssh bandit16@bandit.labs.overthewire.org -p 2220
                                   _                    _ _ _
                                  | |__   __ _ _ __   __| (_)
|_
                                  | '_ \ / _` | '_ \ / _` | |
__|
                                  | |_) | (_| | | | | (_| | |
|_
                                  |_.__/ \__,_|_| |_|\__,_|_|\
__|

                      This is an OverTheWire game se
rver.
            More information on http://www.overthewi
re.org/wargames

bandit16@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit16@bandit.labs.overthewire.org's password:
```

```
level4: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
level5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
level6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
level7: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
level8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
level9: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
level10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
level11: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
level12: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
level13: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
level14: MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
level15: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
level16: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
level17: EReVavePLFHtFlFsjn3hyzMlvSuSACRD
level18: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
level19: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
level20:
level21:
level22:
level23:
level24:
level25:
level26:
level27:
level28:
level29:
level30:
```



KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:15
bandit19@bandit: ~
File Actions Edit View Help

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

  Enjoy your stay!
```

```
level0: bandit0
level1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

Bandit Level 16 → Level 17

Level Goal

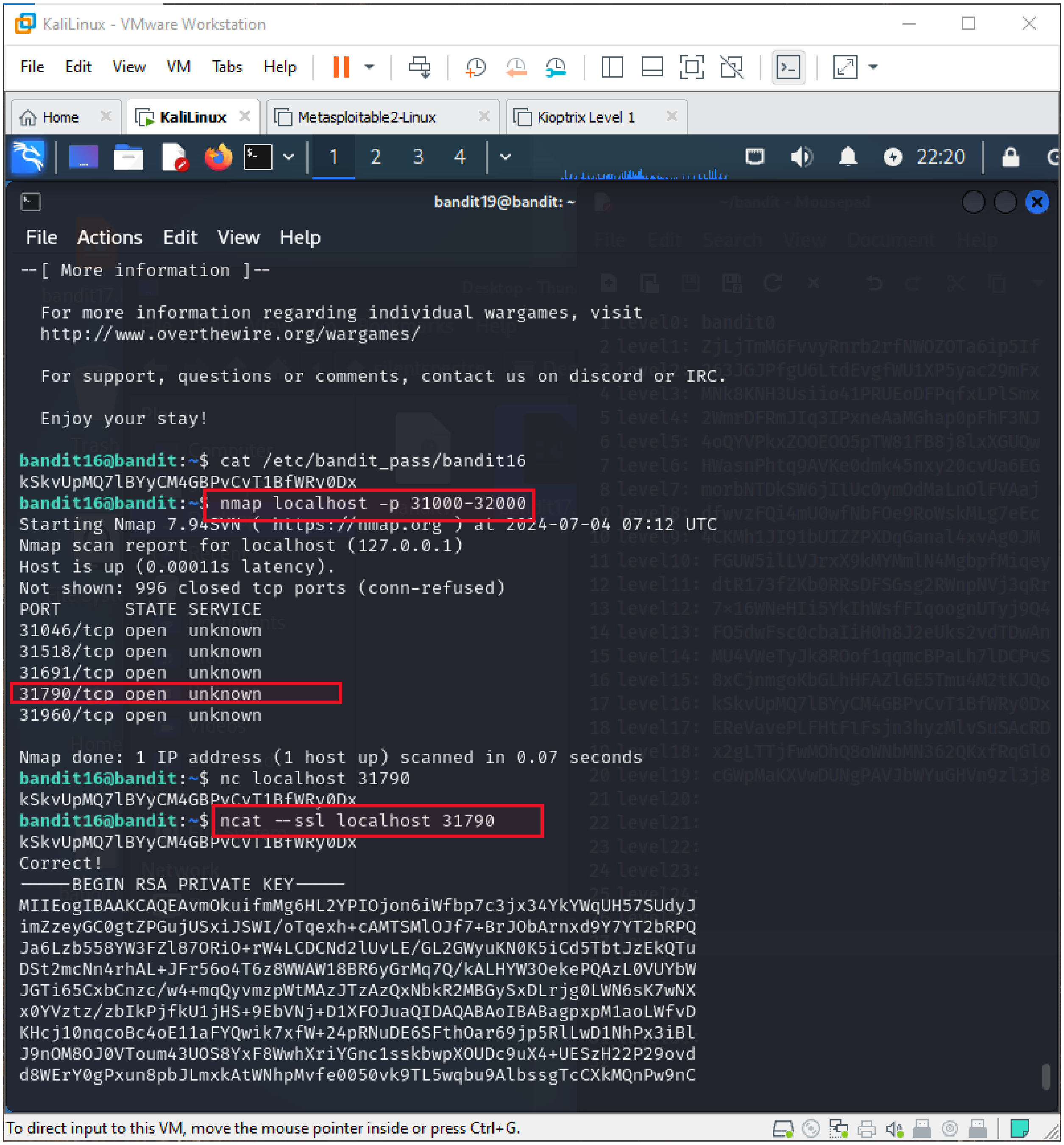
The credentials for the next level can be retrieved by submitting the password of the current level to **a port on localhost in the range 31000 to 32000**. First find out which of these ports have a server listening on them. Then find out which of those speak SSL and which don’t. There is only

23 July, 23

1 server that will give the next credentials, the others will simply send back to you whatever you send to it.

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

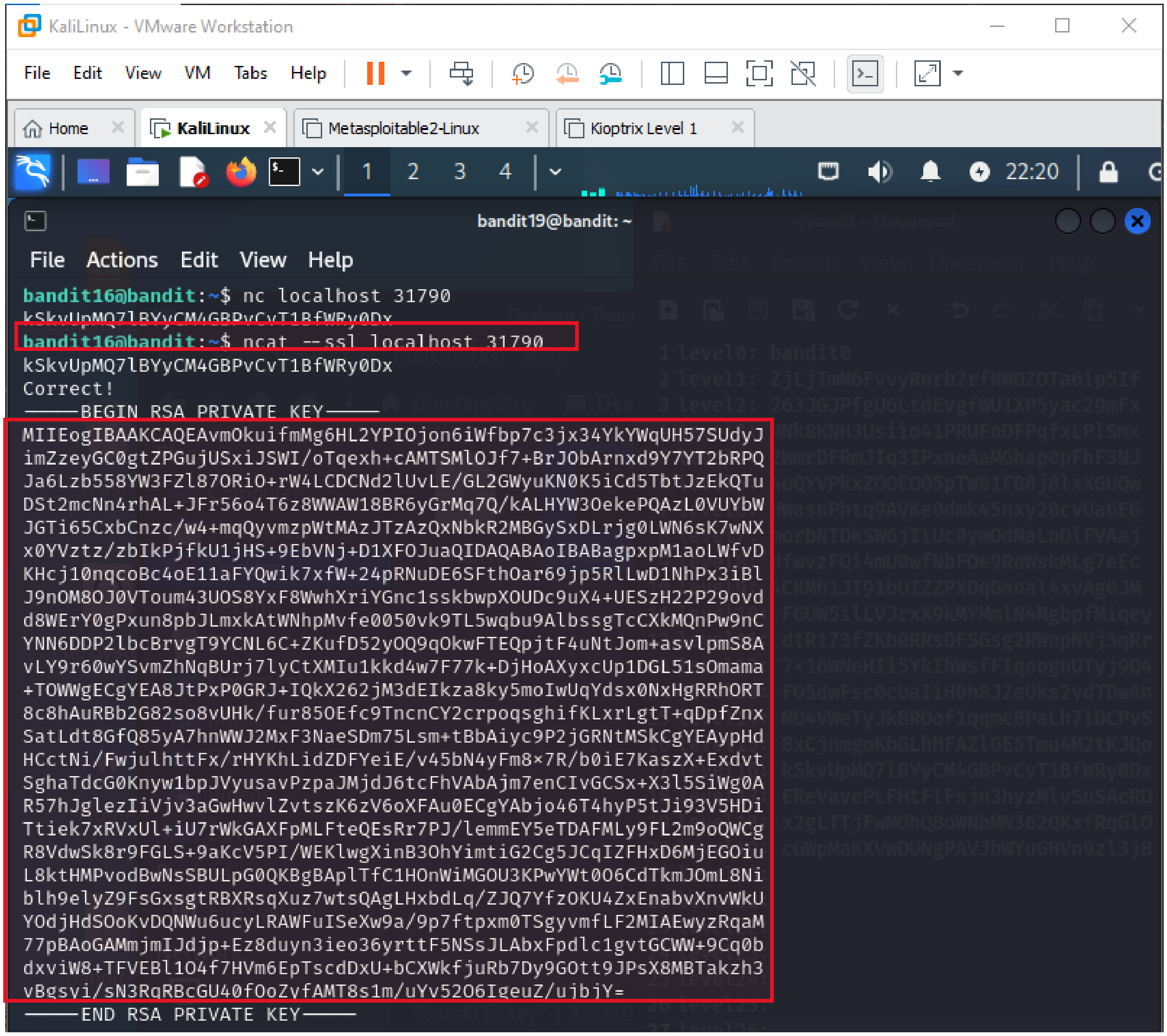

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:20
bandit19@bandit: ~
File Actions Edit View Help

```
--[ 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!

bandit16@bandit:~$ cat /etc/bandit_pass/bandit16
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ nmap localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-04 07:12 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
31046/tcp open  unknown
31518/tcp open  unknown
31691/tcp open  unknown
31790/tcp open  unknown
31960/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
bandit16@bandit:~$ nc localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
```

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

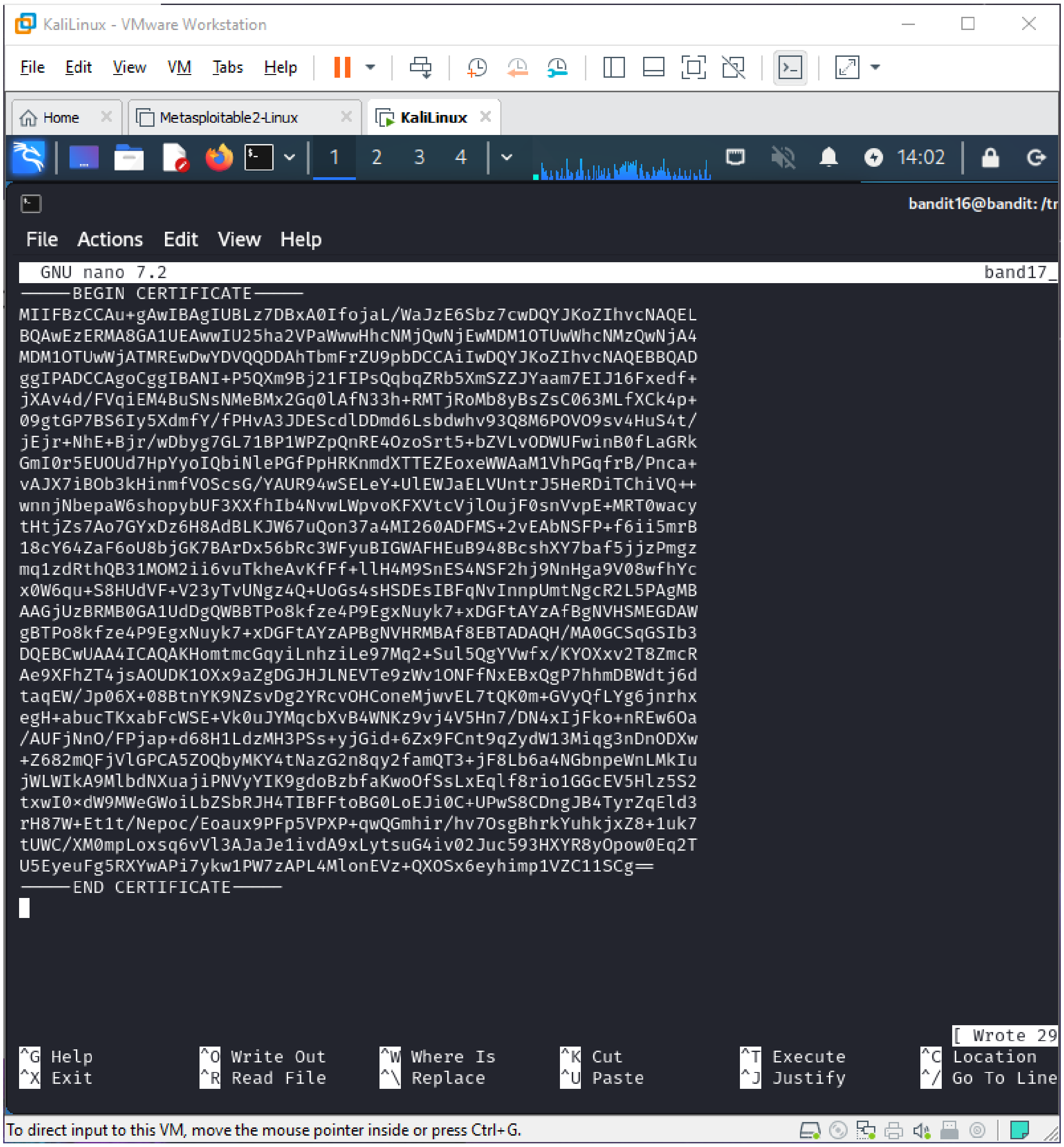
Create a directory /tmp/bandit17 and go there open file band17.key and paste this key there:

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:20
bandit19@bandit: ~
File Actions Edit View Help

```
bandit16@bandit:~$ nc localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
bandit16@bandit:~$ ncat --ssl localhost 31790
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

23 July, 23

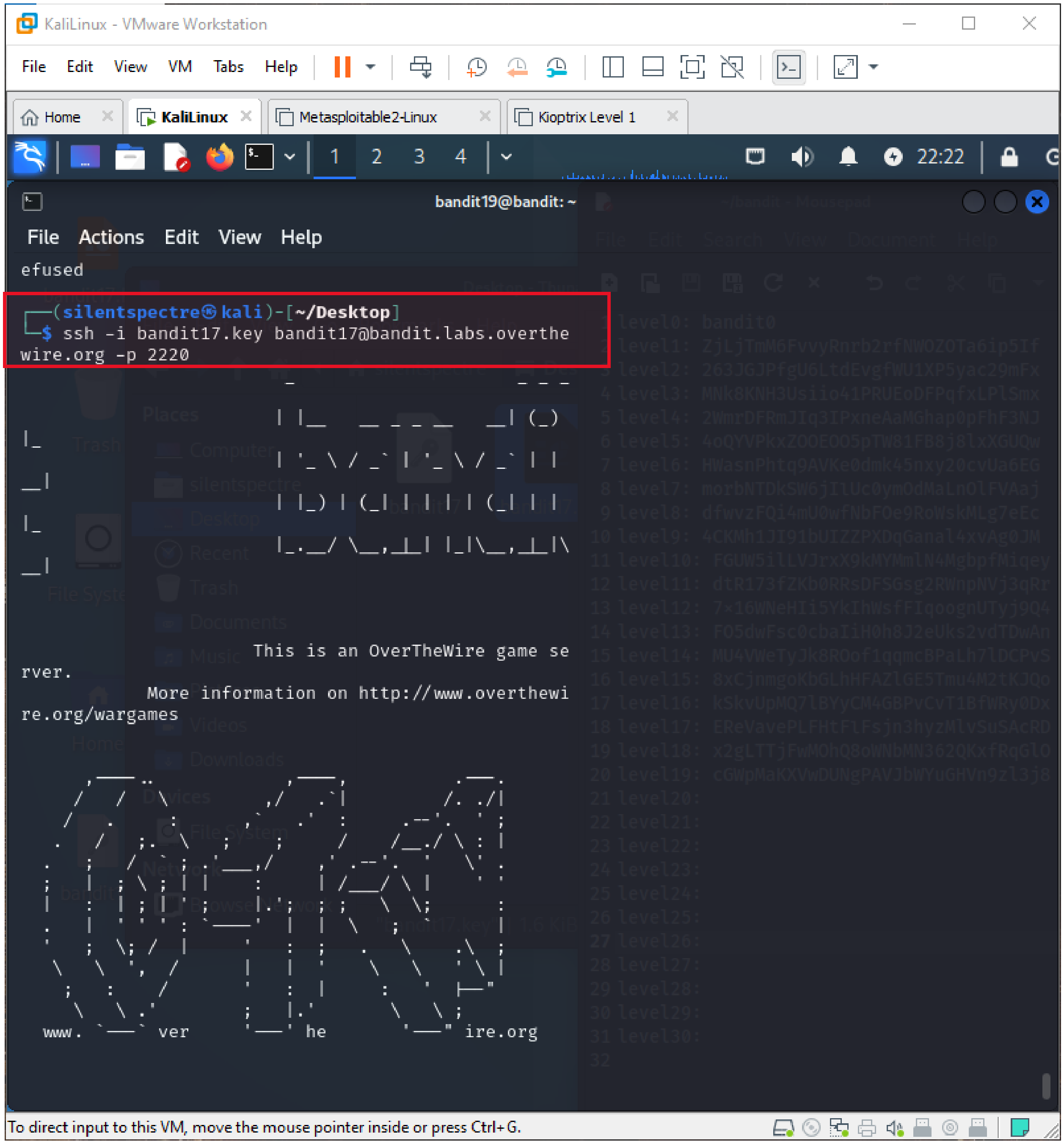

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
Metasploitable2-Linux
KaliLinux
1 2 3 4
14:02
bandit16@bandit: /tr
File Actions Edit View Help

```
  GNU nano 7.2                                                        band17_
-----BEGIN CERTIFICATE-----
MIIFBzCCAu+gAwIBAgIUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4
MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBANI+P5QXm9Bj21FIPsQqbqZRb5XmSZZJYaam7EIJ16Fxedf+
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0lAfN33h+RMTjRoMb8yBsZsC063MLfXCk4p+
09gtGP7BS6Iy5XdmfY/fPHvA3JDEScdlDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE4OzoSrt5+bZVLvODWUFwinB0fLaGRk
GmI0r5EUOUd7HpYyoIQbiNlePGfPpHRKnmdXTTEZEoxeWWAaM1VhPGqfrB/Pnca+
vAJX7iBOb3kHinmfVOScsG/YAUR94wSELeY+UlEWJaELVUntrJ5HeRDiTChiVQ++
wnnjNbepaW6shopybUF3XXfhIb4NvwLWpvoKFXVtcVjlOujF0snVvpE+MRT0wacy
tHtjZs7Ao7GYxDz6H8AdBLKJW67uQon37a4MI260ADFMS+2vEAbNSFP+f6ii5mrB
18cY64ZaF6oU8bjGK7BArDx56bRc3WFyuBIGWAFHEuB948BcshXY7baf5jjzPmgz
mq1zdRthQB31MOM2ii6vuTkheAvKfFf+llH4M9SnES4NSF2hj9NnHga9V08wfhYc
x0W6qu+S8HUdVF+V23yTvUNgz4Q+UoGs4sHSDEsIBFqNvInnpUmtNgcR2L5PAgMB
AAGjUzBRMB0GA1UdDgQWBBTPo8kfze4P9EgxNuyk7+xDGFtAYzAfBgNVHSMEGDAW
gBTPo8kfze4P9EgxNuyk7+xDGFtAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4ICAQAKHomtmcGqyiLnhziLe97Mq2+Sul5QgYVwfx/KYOXxv2T8ZmcR
Ae9XFhZT4jsAOUDK1OXx9aZgDGJHJLNEVTe9zWv1ONFfNxEBxQgP7hhmDBWdtj6d
taqEW/Jp06X+08BtnYK9NZsvDg2YRcvOHConeMjwvEL7tQK0m+GVyQfLYg6jnrhx
egH+abucTKxabFcWSE+Vk0uJYMqcbXvB4WNKz9vj4V5Hn7/DN4xIjFko+nREw6Oa
/AUFjNnO/FPjap+d68H1LdzMH3PSs+yjGid+6Zx9FCnt9qZydW13Miqg3nDnODXw
+Z682mQFjVlGPCA5ZOQbyMKY4tNazG2n8qy2famQT3+jF8Lb6a4NGbnpeWnLMkIu
jWLWIkA9MlbdNXuajiPNVyYIK9gdoBzbfaKwoOfSsLxEqlf8rio1GGcEV5Hlz5S2
txwI0xdW9MWeGWoiLbZSbRJH4TIBFFtoBG0LoEJi0C+UPwS8CDngJB4TyrZqEld3
rH87W+Et1t/Nepoc/Eoaux9PFp5VPXP+qwQGmhir/hv7OsgBhrkYuhkjxZ8+1uk7
tUWC/XM0mpLoxsq6vVl3AJaJe1ivdA9xLytsuG4iv02Juc593HXYR8yOpow0Eq2T
U5EyeuFg5RXYwAPi7ykw1PW7zAPL4MlonEVz+QXOSx6eyhimp1VZC11SCg==
-----END CERTIFICATE-----
█




                                                                  [ Wrote 29
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

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

Open bandit17 on localhost using this key i.e. bandit17.key:

23 July, 23



```
efused
┌──(silentspectre㉿kali)-[~/Desktop]
└─$ ssh -i bandit17.key bandit17@bandit.labs.overthe
wire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_)
|_                      | '_ \ / _` | '_ \ / _` | |
__|                     | |_) | (_| | | | | (_| | |
|_                      |_.__/ \__,_|_| |_|\__,_|_|\
__|

                  This is an OverTheWire game se
rver.
            More information on http://www.overthewi
re.org/wargames
```

```
level0: bandit0
level1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
level2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx
level3: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
level4: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
level5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
level6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
level7: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
level8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
level9: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
level10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
level11: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
level12: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
level13: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
level14: MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
level15: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
level16: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
level17: EReVavePLFHtFlFsjn3hyzMlvSuSAcRD
level18: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
level19: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
level20:
level21:
level22:
level23:
level24:
level25:
level26:
level27:
level28:
level29:
level30:
```

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

Bandit Level 17 → Level 18

Level Goal

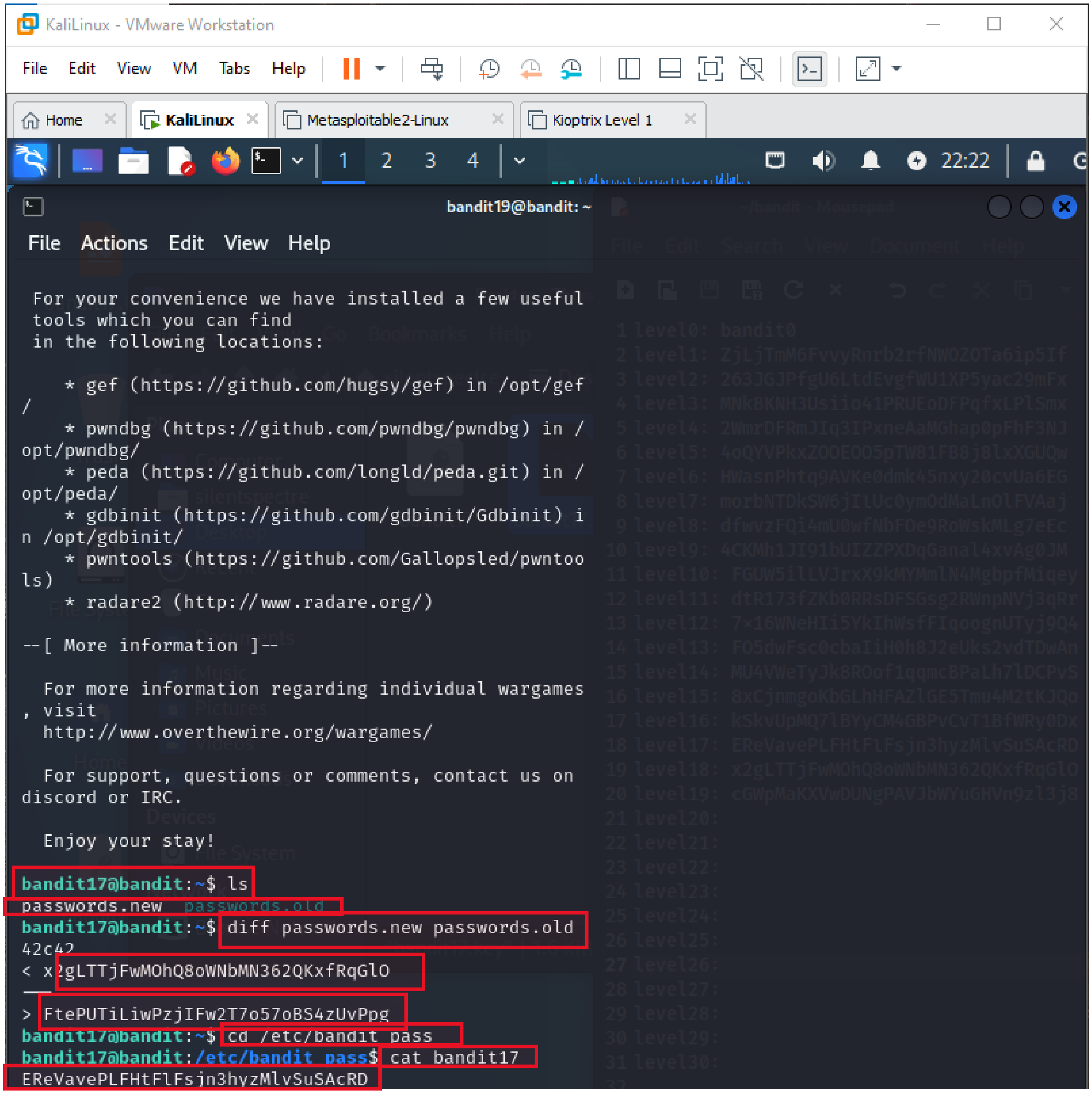
There are 2 files in the homedirectory: **passwords.old and passwords.new**. The password for the next level is in **passwords.new** and is the only line that has been changed between **passwords.old and passwords.new**

23 July, 23

NOTE: if you have solved this level and see ‘Byebye!’ when trying to log into bandit18, this is related to the next level, bandit19

Commands you may need to solve this level

cat, grep, ls, diff



KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:22
bandit19@bandit: ~
File Actions Edit View Help
~/bandit - Mousepad
File Edit Search View Document 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/
    * peda (https://github.com/longld/peda.git) in /
opt/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) i
n /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntoo
ls)
    * 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!

bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
---
> FtePUTiLiwPzjIFw2T7o57oBS4zUvPpg
bandit17@bandit:~$ cd /etc/bandit_pass
bandit17@bandit:/etc/bandit_pass$ cat bandit17
EReVavePLFHtFlFsjn3hyzMlvSuSAcRD
```

```
level0: bandit0
level1: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
level2: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx
level3: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
level4: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
level5: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
level6: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
level7: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
level8: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
level9: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
level10: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey
level11: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
level12: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
level13: FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
level14: MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
level15: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
level16: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
level17: EReVavePLFHtFlFsjn3hyzMlvSuSAcRD
level18: x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
level19: cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
level20:
level21:
level22:
level23:
level24:
level25:
level26:
level27:
level28:
level29:
level30:
```

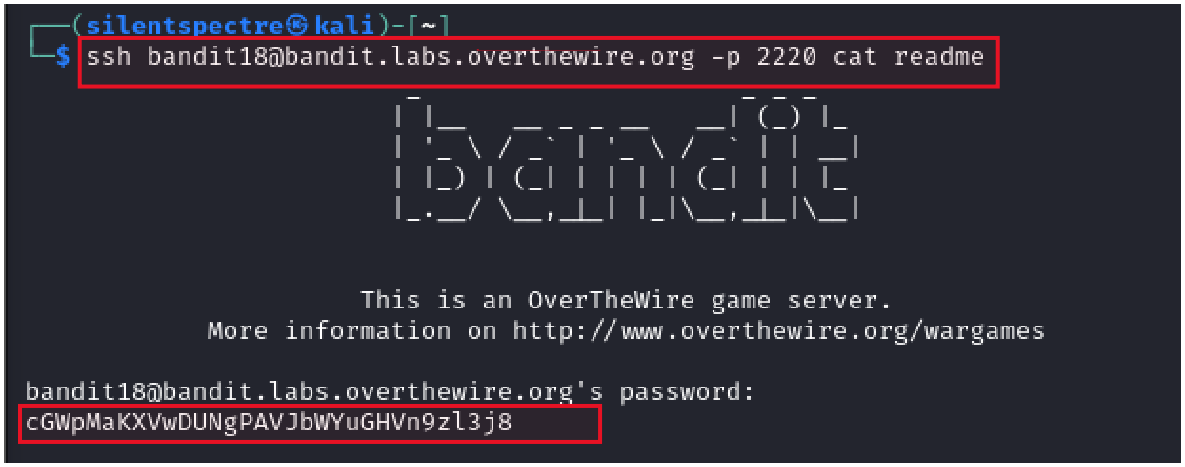
Bandit Level 18 → Level 19

Level Goal

The password for the next level is stored in a file **readme** in the homedirectory. Unfortunately, someone has modified **.bashrc** to log you out when you log in with SSH.

Commands you may need to solve this level

ssh, ls, cat



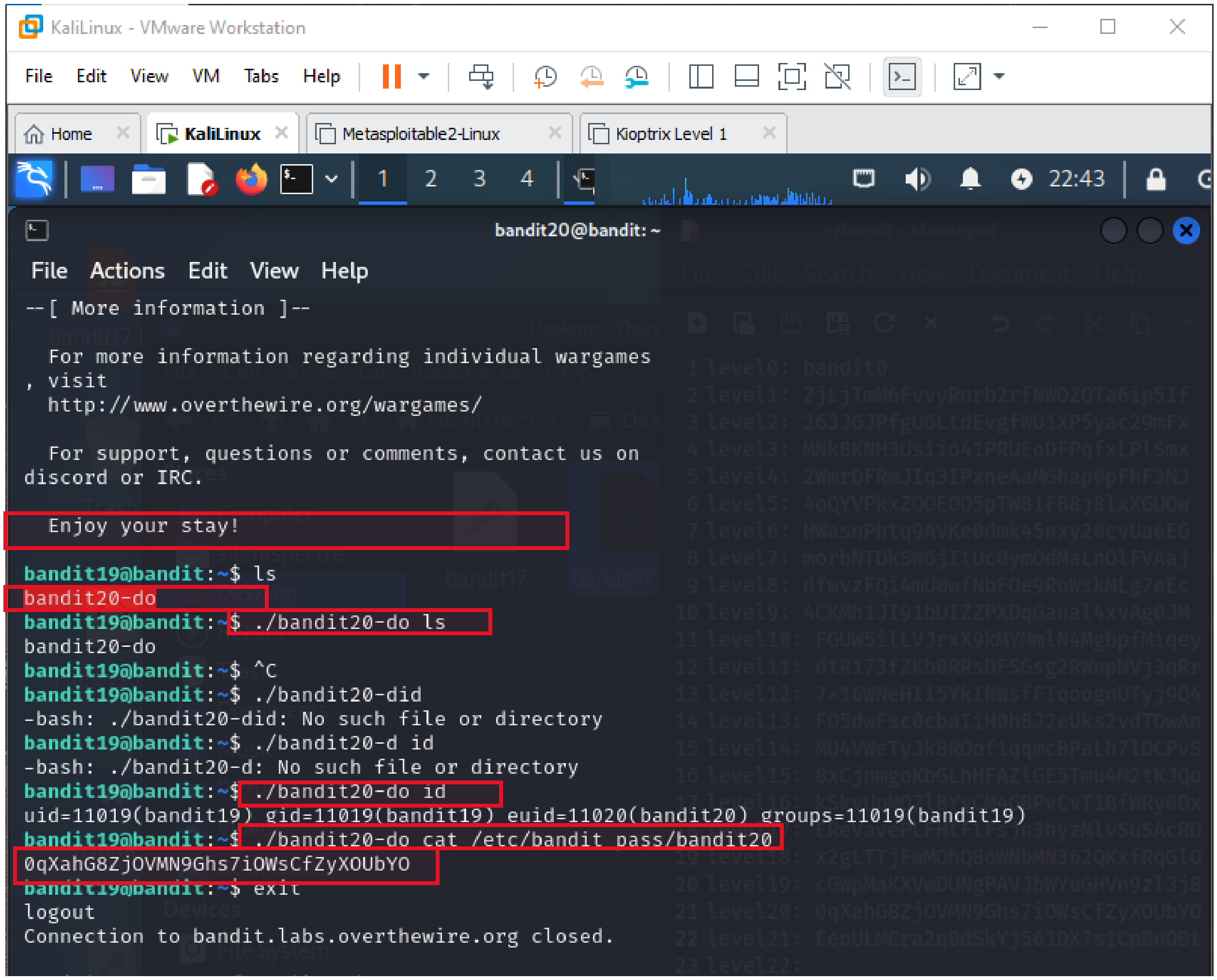
```
┌──(silentspectre㉿kali)-[~]
└─$ ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit18@bandit.labs.overthewire.org's password:
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
```

Bandit Level 19 → Level 20

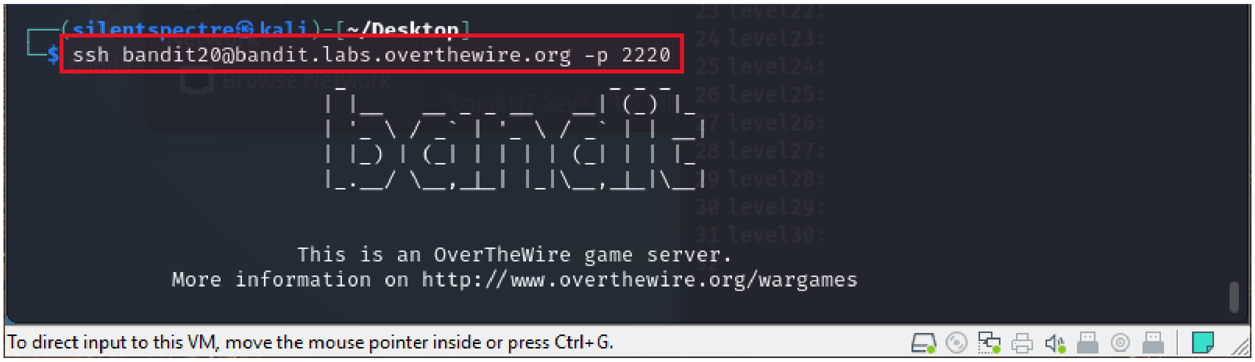
Level Goal

To gain access to the next level, you should use the setuid binary in the homedirectory. Execute it without arguments to find out how to use it. The password for this level can be found in the usual place (/etc/bandit_pass), after you have used the setuid binary.

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:43
bandit20@bandit: ~
File Actions Edit View Help

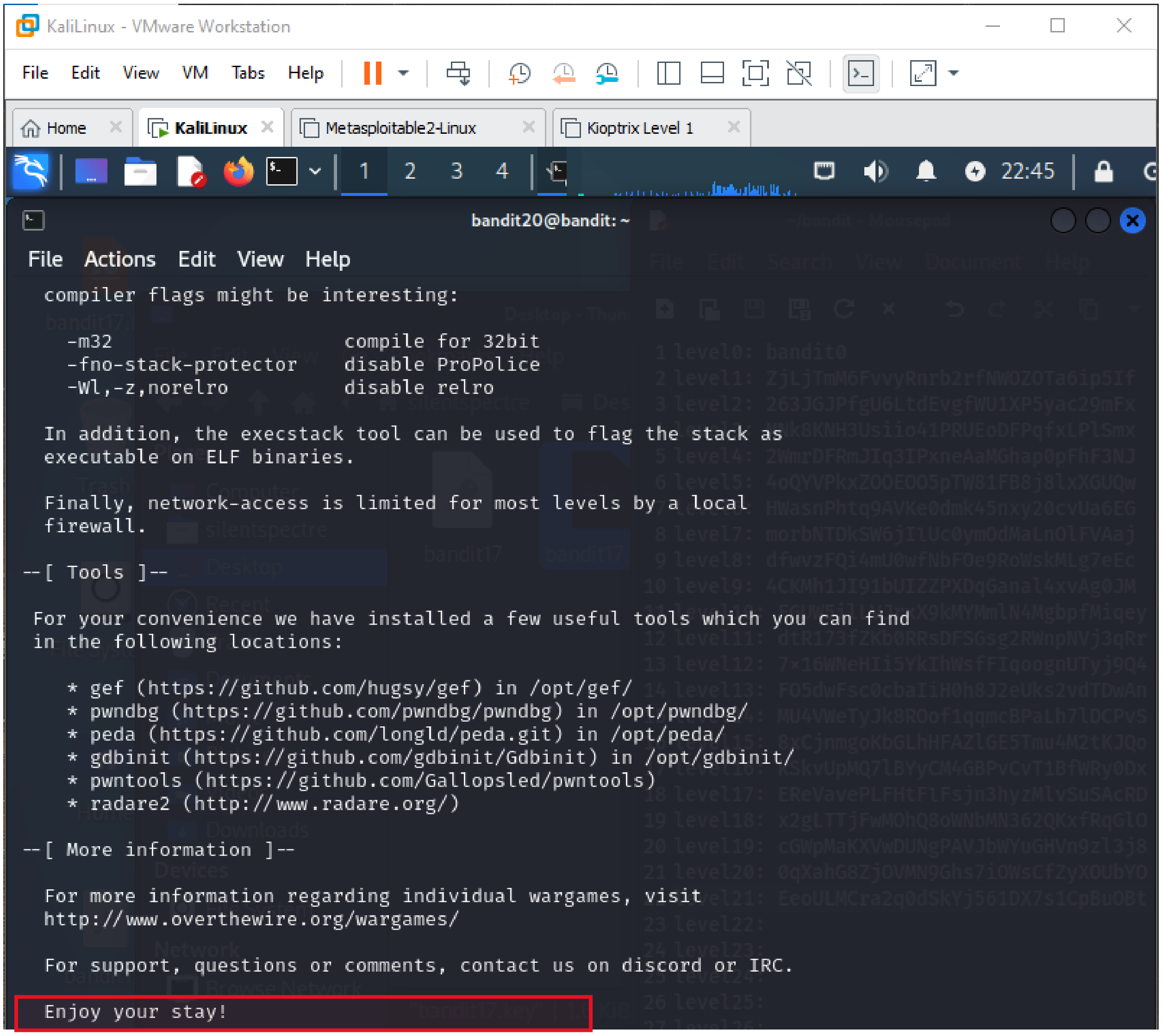
```
--[ More information ]--

  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!

bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ ./bandit20-do ls
bandit20-do
bandit19@bandit:~$ ^C
bandit19@bandit:~$ ./bandit20-did
-bash: ./bandit20-did: No such file or directory
bandit19@bandit:~$ ./bandit20-d id
-bash: ./bandit20-d: No such file or directory
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
bandit19@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
```



```
┌──(silentspectre㉿kali)-[~/Desktop]
└─$ ssh bandit20@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

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

23 July, 23


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
22:45
bandit20@bandit: ~
File Actions Edit View Help

```
  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!
```