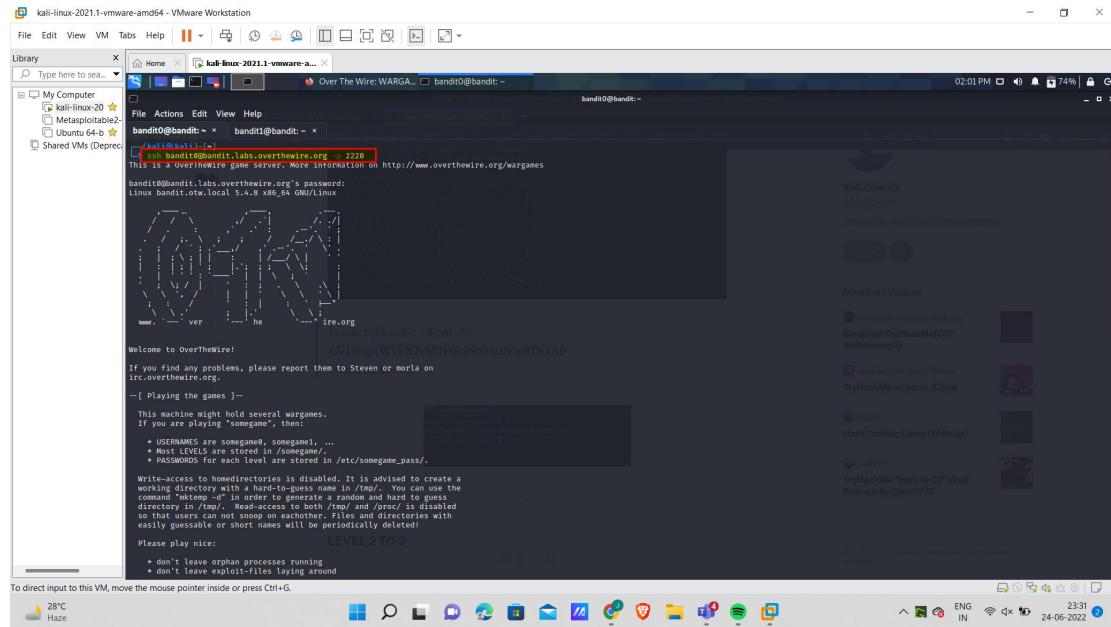


Name: Jayanta Sikdar
Discord: Jayanta Sikdar#0477
Task 5

Level 0 to 1: boJ9jbbUNNfktd78OOpsqOltutMc3MY1



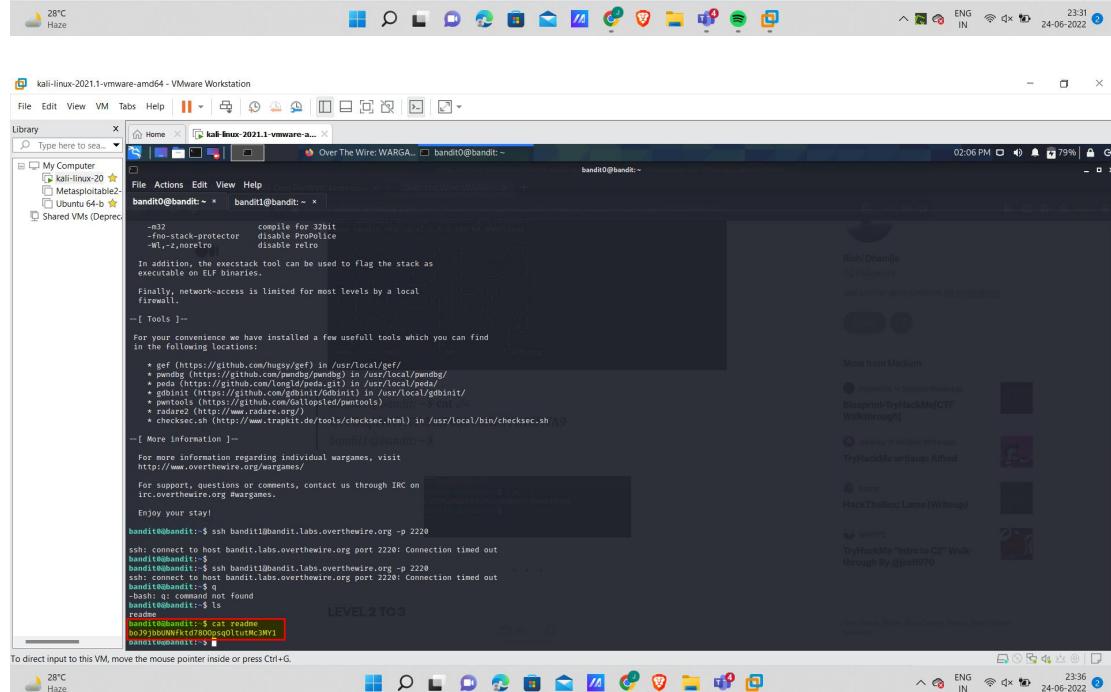
```
ssh bandit1@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
bandit1@bandit.labs.overthewire.org's password:
Linux bandit.owt.local 5.4.0 x86_64 GNU/Linux

Welcome to OverTheWire!
If you find any problems, please report them to Steven or morta on
irc.overthewire.org.
-[ 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 in /tmp and use the command "mktemp -d" in order to generate a random and hard to guess
directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
so that users can not snog on eachother. Files and directories with
easily guessable or short names will be periodically deleted!

Please play nice:
[LEVEL 2 TO 3]
* don't leave orphan processes running
* don't leave exploit-files laying around
```

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



```
-m32           compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,nowrto  disable retro

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 /usr/local/gef/
+ pwndbg (https://github.com/pwndbg/pwndbg/) in /usr/local/pwndbg/
+ radare2 (https://github.com/radare/radare2) in /usr/local/radare2/
+ gdbinit (https://github.com/gdbinit/gdbinit) in /usr/local/gdbinit/
+ pwntools (https://github.com/Gallopsled/pwntools)
+ exploitdb (https://github.com/ExploitDB/exploitdb) in /usr/local/exploitdb/
+ checksec.sh (http://www.trailofbits.com/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 #wargame.

Enjoy your stay!
bandit1@bandit:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
ssh: connect to host bandit.labs.overthewire.org port 2220: Connection timed out
bandit1@bandit:~$ ssh bandit1@bandit.labs.overthewire.org -p 2220
ssh: connect to host bandit.labs.overthewire.org port 2220: Connection timed out
bandit1@bandit:~$ q
bandit1@bandit:~$ ls
readme
bandit1@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit1@bandit:~$
```

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

Level 1 to 2: CV1DtqXWVFXTvM2Fok09SHzoYwRINYA9

```
[kali㉿kali:~] bandit1@bandit1:~$ cat ./level1.flag  
This is OverTheWire.org's password:  
Linux bandit1 5.4.0-xen #1 SMP PREEMPT Tue Jun 22 14:43:04 UTC 2021  
[kali㉿kali:~] bandit1@bandit1:~$
```

Welcome to OverTheWire!
If you find any problems, please report them to Steven or moria on irc.overthewire.org.
-[Playing the games]-
This machine might hold several wargames.
If you are playing "somegame", then:
* USERNAMEs are somegame, somegame_...
* Most LEVELs are stored in /somegame/...
* PASSWORDs for each level are stored in /etc/somegame_pass/.
Note: access to /tmp/ 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/ and /proc/ is disabled

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

```
[kali㉿kali:~] bandit1@bandit1:~$ cat ./level2.flag  
LEVEL2TO3
```

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/hugovs/gef) in /usr/local/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peda (https://github.com/greggman/peda.git) in /usr/local/peda/
* radare2 (https://github.com/radare/radare2) in /usr/local/radare2/
* radare2z (https://github.com/gallopd/rdpntools)
* 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@bandit1:~\$ ls
bandit1@bandit1:~\$.bash_logout .profile
bandit1@bandit1:~\$ cd ~
bandit1@bandit1:~\$ cd .bash_logout
-bash: cd: .bash_logout: Not a directory
bandit1@bandit1:~\$ cat -
[1]+ Stopped cat -
bandit1@bandit1:~\$ cat ./level2.flag
LEVEL2TO3

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

Level 2 to 3: UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK

```
bandit2@bandit:~$ cat ./spaces_in_this_filename
bandit2@bandit:~$
```

```
bandit2@bandit:~$ cat ./spaces_in_this_filename
bandit2@bandit:~$
```

Level 3 to 4: pIwrPrtPN36QITSp3EQaw936yaFoFgAB

```
kali-linux-2021.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help | 02:41 PM 79% | 
Library Type here to see... 
My Computer 
  kali-linux-20... 
  Metasploitable2... 
  Ubuntu 64-b... 
Shared VMs (Deprec... 
  bandit3@bandit:~$ ls
  bandit@bandit:~$ cd /tmp
  bandit@bandit:~/tmp$ curl bandit3@bandit.labs.overthewire.org:2220
  This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
  bandit@bandit:~/tmp$ bandit3@bandit.labs.overthewire.org's password:
  bandit@bandit:~/tmp$ xterm_64_0MwLnx
  Welcome to OverTheWire!
  If you find any problems, please report them to Steven or m0rla on
  irc.overthewire.org.
  --[ 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 to quickly create a random temporary directory. It is
  safe to delete a random temporary directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
  easily guessable or short names will be periodically deleted!
  Please play nice:
  * don't leave orphan processes running
  * don't leave exploit/files laying around
  To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
  bandit@bandit:~/tmp$ 

  28°C Haze
  File Edit View VM Tabs Help | 02:41 PM 79% | 
  Library Type here to see... 
  My Computer 
  kali-linux-20... 
  Metasploitable2... 
  Ubuntu 64-b... 
  Shared VMs (Deprec... 
  bandit3@bandit:~$ ls
  bandit@bandit:~$ cd /tmp
  bandit@bandit:~/tmp$ curl bandit3@bandit.labs.overthewire.org:2220
  This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
  bandit@bandit:~/tmp$ bandit3@bandit.labs.overthewire.org's password:
  bandit@bandit:~/tmp$ xterm_64_0MwLnx
  Welcome to OverTheWire!
  If you find any problems, please report them to Steven or m0rla on
  irc.overthewire.org.
  --[ 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 to quickly create a random temporary directory. It is
  safe to delete a random temporary directory in /tmp/. Read-access to both /tmp/ and /proc/ is disabled
  so that users can not snoop on eachother. Files and directories with
  easily guessable or short names will be periodically deleted!
  Please play nice:
  * don't leave orphan processes running
  * don't leave exploit/files laying around
  To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
  bandit@bandit:~/tmp$ 
```

```
kali-linux-2021.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help | 02:42 PM 79% | 
Library Type here to see... 
My Computer 
  kali-linux-20... 
  Metasploitable2... 
  Ubuntu 64-b... 
Shared VMs (Deprec... 
  bandit3@bandit:~$ ls
  bandit@bandit:~$ cd /tmp
  bandit@bandit:~/tmp$ by default, although ASLR has been switched off. The following
  compiler flags might be interesting:
  -fno-stack-protector disable prologue
  -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 this directory. More information on this directory is in this file located in
  the following locations:
  * pef (https://github.com/hugsy/pef) in /usr/local/pef/
  * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
  * peda (https://github.com/tongld/peda.git) in /usr/local/peda/
  * radare2 (https://github.com/radare/radare2) in /usr/local/radare2/
  * 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!
  bandit@bandit:~$ ls
  bandit@bandit:~$ cd /tmp
  bandit@bandit:~/tmp$ ls
  bandit@bandit:~/tmp$ ls a
  ls: cannot access 'a': No such file or directory
  bandit@bandit:~/tmp$ ls b
  bandit@bandit:~/tmp$ ls c
  bandit@bandit:~/tmp$ ls .hidden
  bandit@bandit:~/tmp$ cat .hidden
  pIwrPrtPN36QITSp3EQaw936yaFoFgAB
  bandit@bandit:~/tmp$ 
```

Level 4 to 5: koReBOKuIDDepwhWk7jZCoRTdopnAYKh

Level 5 to 6: DXjZPULLxYr17uw0Io1bNLQbtFemEgo7

Level 6 to 7: HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs

```
[kali-linux-2021.1-vmware-amd64 - VMware Workstation]
File Edit View VM Tabs Help | Home | Over The Wire: WARGAMES | bandit6@bandit7 |
bandit6@bandit7: ~ kali:kali: ~ bandit2@bandit7: ~ bandit3@bandit7: ~/here ~ bandit4@bandit7: ~/here ~ bandit5@bandit7: ~/here/maybehere08 ~ bandit6@bandit7: ~

[ Tips ] -
This machine has a i686 processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32
-fno-stack-protector disable ProPolice
-Wl,-z,noreloc 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:
* ggef (https://github.com/Husky/ggef) in /usr/local/ggef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peds (https://github.com/tongli/peda.git) in /usr/local/peda/
* radare2 (https://github.com/radare/radare2) in /usr/local/radare2/
* radare2j (https://www.radare.org/)
* radare2j (http://www.radare.org/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.
irc://irc.overthewire.org #wargames.

Enjoy your stay!
bandit6@bandit7: ~ cat /var/lib/dkms/info/bandit7.password
bandit6@bandit7: ~

bandit6@bandit7: $ DNIZPULLYr1nwI010LNQfEmEg07; command not found
bandit6@bandit7: ~ group bandit6 -size 33c 2361 | grep -F -v Permission | grep -F -v directory
bandit6@bandit7: ~ cat /var/lib/pkgs/info/bandit7.password
bandit6@bandit7: ~
bandit6@bandit7: ~ cat /var/lib/dkms/info/bandit7.password
bandit6@bandit7: ~

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
28°C Haze 0:29 79% 25-06-2022
```

Level 7 to 8: cvX2JJa4CFALtqS87jk27qwqGhBM9pIV

```
[kali-linux-2021.1-vmware-amd64 - VMware Workstation]
File Edit View VM Tabs Help | Home | OverTheWire: Level Goal | bandit7@bandit8 |
bandit7@bandit8: ~ kali:kali: ~ bandit2@bandit8: ~ bandit3@bandit8: ~/here ~ bandit4@bandit8: ~/here ~ bandit5@bandit8: ~/here/maybehere08 ~ bandit6@bandit8: ~ bandit7@bandit8: ~

[ Tips ] -
This machine has a i686 processor and many security-features enabled
by default, although ASLR has been switched off. The following
compiler flags might be interesting:
-m32
-fno-stack-protector disable ProPolice
-Wl,-z,noreloc 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:
* ggef (https://github.com/Husky/ggef) in /usr/local/ggef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
* peds (https://github.com/tongli/peda.git) in /usr/local/peda/
* radare2 (https://github.com/radare/radare2) in /usr/local/radare2/
* radare2j (https://www.radare.org/)
* radare2j (http://www.radare.org/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.
irc://irc.overthewire.org #wargames.

Enjoy your stay!
bandit7@bandit8: ~ cat /var/lib/dkms/info/bandit8.password
bandit7@bandit8: ~

bandit7@bandit8: ~ DNIZPULLYr1nwI010LNQfEmEg07; command not found
bandit7@bandit8: ~ group bandit7 -size 33c 2361 | grep -F -v Permission | grep -F -v directory
bandit7@bandit8: ~ cat /var/lib/pkgs/info/bandit8.password
bandit7@bandit8: ~
bandit7@bandit8: ~ cat /var/lib/dkms/info/bandit8.password
bandit7@bandit8: ~

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
28°C Haze 0:47 79% 25-06-2022
```

Level 8 to 9: UsVYFSfZZWbi6wgC7dAFyFuR6jQQUhR

```
[ bandit8@bandit: ~ ]$ cat data.txt
UsVYFSfZZWbi6wgC7dAFyFuR6jQQUhR
```

Level 9 to 10: truKLdjsbJ5g7yyJ2X2Roo3a5HQJFuLk

```
[ bandit9@bandit: ~ ]$ strings data.txt | grep "*"
truKLdjsbJ5g7yyJ2X2Roo3a5HQJFuLk
```

Level 10 to 11: IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR

```
bandit10@bandit:~$ cat data.txt
VIGHlIHbzc3JkIG1zElGdwz3SdzRlc4TU9xM0ISmFyeUxahHUtKv1vB5Cg==

The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
```

Level 11 to 12: 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

```
bandit11@bandit:~$ cat data.txt
Gur cnfjbeq vf S6p8LqetP5sPK8htjh8KX3SP6x28Bh

The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
```

Level 12 to 13: 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL

kali-linux-2021.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help Library Type here to search

Home kali-linux-2021.1-vmware-amd64... Firefox bandit12@bandit: /tmp/jay

File Actions Edit View Help

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

Enjoy your stay!

```
bandit12@bandit:~/tmp/jay$ mkdir /tmp/jay
bandit12@bandit:~/tmp/jay$ cd /tmp/jay
bandit12@bandit:~/tmp/jay$ ls
data.txt
bandit12@bandit:~/tmp/jay$ mv data.txt jay1.txt
jay1.txt
bandit12@bandit:~/tmp/jay$ ls
jay1.txt
bandit12@bandit:~/tmp/jay$ xxd -r jay1.txt > jay2.bin
bandit12@bandit:~/tmp/jay$ ls
jay1.txt jay2.bin
bandit12@bandit:~/tmp/jay$ xxd jay2.bin > jay3
bandit12@bandit:~/tmp/jay$ ls
jay1.txt jay2.bin jay3
bandit12@bandit:~/tmp/jay$ bzip2 jay3 > jay4
bandit12@bandit:~/tmp/jay$ ls
jay1.txt jay2.bin jay4
bandit12@bandit:~/tmp/jay$ xxd jay4
jay4: gzip compressed data, was "data.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:~/tmp/jay$ xzat jay4 > jay5
bandit12@bandit:~/tmp/jay$ ls
jay5: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/jay$ tar -xvf jay5
data5.bin
bandit12@bandit:~/tmp/jay$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/jay$ tar -xvf data5.bin
data5.bin
bandit12@bandit:~/tmp/jay$ file data5.bin
data5.bin: gzip compressed data, block size = 9000
bandit12@bandit:~/tmp/jay$ bzip2 data5.bin > jay6
bandit12@bandit:~/tmp/jay$ ls
jay6: POSIX tar archive (GNU)
bandit12@bandit:~/tmp/jay$ tar -xvf jay6
data6.bin
bandit12@bandit:~/tmp/jay$ file data6.bin
data6.bin: gzip compressed data, was "data5.bin", last modified: Thu May 7 18:14:30 2020, max compression, from Unix
bandit12@bandit:~/tmp/jay$ bzip2 data6.bin > jay7
bandit12@bandit:~/tmp/jay$ ls
jay7: ASCII text
bandit12@bandit:~/tmp/jay$ cat jay8
The password is: 82jyZk1nfYKosahhWxJ3m02z109SYL

bandit12@bandit:~/tmp/jay$
```

The password is: 82jyZk1nfYKosahhWxJ3m02z109SYL

Reference: The Linux Command Line: A Complete Introduction

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

Level 13 to 14: 4wcYUJFwokoXLShlDzztnTBHiqxU3b3e

kali-linux-2021.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help Library Type here to search Home OverTheWire - Bandit ... bandit14@bandit:~ bandit14@bandit:~ 05:52 PM 79% 🔍

File Actions Edit View Help bandit14:~ -> bandit3@.../inhere x bandit4@.../inhere x bandit5@bandit.../re/maybehere08 x bandit11:~ x bandit12:~ x bandit13:~ x bandit14:~ x bandit15:~ x bandit16:~ x bandit17:~ x bandit18:~ x bandit19:~ x bandit20:~ x

END RSA PRIVATE KEY

bandit14:~ -> ssh -i /root/.ssh/localhost -i /root/.ssh/private
Could not create directory '/root/.ssh/localhost'.
The authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is 3e6c19f9493a2a030303030303030303.
Are you sure you want to continue connecting (yes/no)?
Failed to add the host to the list of known hosts (/home/bandit14/.ssh/known_hosts).
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

Linux bandit14.localhost 5.4.8 #66~1~amd64-Ubuntu SMP Mon Jun 21 10:45:00 UTC 2021 x86_64 x86_64 GNU/Linux
Welcome to OverTheWire!
If you find any problems, please report them to Steven or m0rta on irc.overthewire.org.
-[Playing the games]-
This machine has a 64bit processor and many security-features enabled.
If you're using a 32bit OS have it switched off. The following compiler flags might be interesting:
-m32 -fstack-protector disable ProPolice
-fno-stack-protector 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 - that means I am using an identity file in order to log into bandit14 on the server since all of the bandit machines are behind a machine. After I logged into bandit14 I ran "cat /etc/bandit_pass" as specified on the hint and then I read file bandit4 which gave us the next password.
-[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 /usr/local/gef/
+ pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
+ peda (https://github.com/longld/peda_gdb) in /usr/local/peda/
+ radare2 (https://github.com/radare/radare2) in /usr/local/radare2/
+ pwntools (https://github.com/Gallopsled/pwntools)
+ radare2 (http://www.radare.org/)
+ checksec (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh
-[More information]-
This machine has a 64bit processor and many security-features enabled
If you're using a 32bit OS have it switched off. The following compiler flags might be interesting:
-m32 -fstack-protector disable ProPolice
-fno-stack-protector 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 - that means I am using an identity file in order to log into bandit14 on the server since all of the bandit machines are behind a machine. After I logged into bandit14 I ran "cat /etc/bandit_pass" as specified on the hint and then I read file bandit4 which gave us the next password.
-[Enjoy your stay!]-
bandit14\$ cat /etc/bandit_pass/bandit14
wvYUFWnX0LSHdzxTBiqU3Bse
bandit14\$ ls

Level 14 to 15: BfMYroe26WYalil77FoDi9qh59eK5xNr

Level 15 to 16: cluFn7wTiGryunymYOu4RcffSxQluehd

