

```
bandit0@bandit: ~  
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/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit0@bandit:~$ ls  
readme  
bandit0@bandit:~$ cat readme  
NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL  
bandit0@bandit:~$
```

Bandit 0 => 1

1. Logged on using ssh

Hostname : bandit0

Password : bandit0

Port : 2220

Host : bandit.labs.overthewire.org

2. Used ls command to look for files

3. Found a file named readme

4. Used cat command to read the file

5. Found the password to be NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL

```
bandit1@bandit: ~  
  
-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/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit1@bandit:~$  
bandit1@bandit:~$ ls  
-  
bandit1@bandit:~$ cat ./-  
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi  
bandit1@bandit:~$
```

Bandit 1=>2

1. Logged on using ssh

Hostname : bandit1

Password : **NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL**

Port : 2220

Host : bandit.labs.overthewire.org

2. Looked for files by using the ls command

3. Found a file named “-”

4. Found out that it starts with a special character and can't be directly opened with the cat command so added “./” after the command

5. Found the password to be **rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**

```
bandit2@bandit: ~  
  
-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/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit2@bandit:~$  
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ cat "spaces in this filename"  
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG  
bandit2@bandit:~$
```

Bandit 2=>3

1. Logged on using ssh

Hostname : bandit2

Password : **rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi**

Port : 2220

Host : bandit.labs.overthewire.org

2. Looked for files using the ls command

3. Found a file named "spaces in this filename"

4. Used the cat command on the file wrapped up in ""

5. Found the password to be **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**

```
bandit3@bandit: ~/inhere

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/)

Both python2 and python3 are installed.

--[ More information ]--

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

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

Enjoy your stay!

bandit3@bandit:~$
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -a
.  ..  .hidden
bandit3@bandit:~/inhere$ cat ./hidden
2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe
bandit3@bandit:~/inhere$
```

Bandit 3=>4

1. Logged on using ssh

Hostname : bandit3

Password : **aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG**

Port : 2220

Host : bandit.labs.overthewire.org

2. Looked for files using the ls command but didn't find any

3. So used the ls -a command to look for any hidden files found a file named .hidden

4. Used cat ./ command since it started with a special character

5. Found the password to be **2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe**


```
bandit5@bandit: ~/inhere/maybehere07
bandit5@bandit:~/inhere$ find -readable -type f -size 1033c -executable
bandit5@bandit:~/inhere$ find -readable -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
cat: ./maybehere07/.file2: No such file or directory
bandit5@bandit:~/inhere$ cd ./maybehere07
bandit5@bandit:~/inhere/maybehere07$ cat file02
cat: file02: No such file or directory
bandit5@bandit:~/inhere/maybehere07$ ls
.file1  .file2  -file3  spaces file1  spaces file3
bandit5@bandit:~/inhere/maybehere07$ cat ./-file02
cat: ./-file02: No such file or directory
bandit5@bandit:~/inhere/maybehere07$ cat ./-file2
J67tSeFKYcCAUUmclCbDzpijUE2VZeC2LHFikNP3IuTBERBw6CpeLRqDJskyUvZwpeP6helUWai750jaGVNpGJ94gorbwQLPwHfDwb2XLLzrC4jfmn8JLXT0jeVkiW4Vf
CqUSeHyKNsozJ2gYgZLInRfLWqxcKG6DR9CIRGAWUKeIBRUN8sxvxdNGvc8jhb3RIeGq05WlkPpxGNPCwxYccu1hCQdttfGbgGeyVaYIEDfethS1s1BU1IpM113A2Ysswv79
cJ6S21kviMpwg8gplWfACUCJnyhcLAes1FeQ1e5Vqxcxe011DCAs7thoQ13UnxCBqttGVrez1jmDD22AEV0AASfzbEcXNcmZOBwdbx49AZLyOmrs2XGZfDKLRVoF09LzUA
8XqMP09B10fS0itGs0Npgy6PQANJGOV1QoCU4yi4f5lw77KV3F9IGlx2FtChC3F5vyW2f04Yfbp0983sBWSc9UBRhJF1HYCJFRLZ6uuNgcsZJ2I63H7zBPr3t64qEAXABS
JcwitlTm68pUppbAPsASKjJtc1ih103w4kdjnLY2CdLFUZTse9zHzwuoKZNeKL0kkh0qFLDfCetfXlAff3PNnX6q9zw8r fwe1vQSwLOesguhdmaRiCSQ0Mk86JJQaA79wqt
9Eig2BzrSd2Fy5JbXUW73zJ3PnPA3hCA3lve1vLPRIYuU9nnTWhTLly0LRwuBEoswyFB9QaH0ufgNGL85e0JahzeXMLBh8suJLLiz7C4stadra5mdONGv40VzehCM2r6xe
QG0JfctB1q7B8LzB5nJ11g79iK6QBZ655vdMseVMOMj9187wQlWKIRcQ8KEfRhs9kili4J2L6xsBNxDLaa7Ec3CAfBBrumMLIUT4uAHAA0KpkoIMGzmmTHsVR1oF48cV8JsOU
b92wI7XCz2LjnmKuT01RWxJuL3s2K1srWljpnDM4XlQ2PULvXxRBrBYQf4AFYtLiPSKraImoTST7sxeCrP50XUpCdFresPVRs7aDQZJ24JOMFdVKP6M4NAu4LomPMGQU84q7
YLzIVckFnGt0nIGBe07Vfwf6tJbQSwjbiVt7oge2CadpHvPyZRo8QpZJYsJLdvbI8L3Fc2onq6aJi6x0Eyle8MQPyWqsIgmDmLA0pDbjYarVgKXyy73QQuv0HksFz7ks0Kf
MaQz94Y3CvemlFPSHPCRTcm0076suMpIFG0bUDaxGkfw9RCshPGmcNFu4wedjyPlK7T7v0CJVvKp00y18UW5X9LZ65su5jP5K0mhJTQD71yw7E36FeLi9mf5cS21K8vGWLbt5
ggzeUlfKdLV9wIwK4Ga4zCTfvI20uCX9mQjzqtM259piS6fLG9D8zrrwSuxgQ0qTzuWeA660o3nKzu05M3K1HXfHKFYd33wCdXglDzaI1KayF09s1DyQY9d5v3nc6lXqFuZ
0IDmeWQZulZ0408AYIQ477QRf6mEcSGwGev7V4DdGneHg40s93UyhYBthWGFz6bj5nJQNmtgnTbEGyYaHuaaTdw2VAdfXAwWLaINkzliVEEHKHOjU1hfnwL62REdahU9GyWau
8LSZ8jq31TBWxfkhghpLHAkVeFCFstsayhBX4TuHjuvHx6AcL8GIBrk5RqCNUoLupRlqMnnCXDPDIaHltpTax03EYTSU1aUcG9hTG1B0tyBBvw7yQQR349oIyczqqgyYpkg
d6Lzkc2B1kpjjrNzdUgCZmCZwEA4Ftj4JSb0LZRLt2MbefMnw33AFoAY3XoSARLupZllQe6yTlLiGCVUAbVhJkDmP0oSybURITNncwTvYbbdeXbYbo9BVXMRafxBqZNo4V2L
fQdy4WUTg8mhCq0bLvgq7lB8B2E8UuNnVloj4ahn5RrmpFNhRN59X6Ux4nN1ndGj6AOVrJ58BqGMuLKPFIgohyXmYlEnTNHbZxg841cLnI57KLQA20DLryXx2qar0X9KvZwo
K3Mfm8yduYlfeAqlZpcqf3rxJAKEV4uIyQMu5ItfXsLTTo3pRbbdF8NazwFDEIDzBBBHnA04RW2gdo4FyYKbUHZG2HI8Fc3BQjVLtJLGH7pFfubKqza6Q2NjrZ6yG1k1NA
2v4XGiAbpl1nonn12u8WnTpNqagMnxbr3fZa1HW0XByt61c1SKMcwKo1PaoPeSvbx0x9tt0CSwoshNSq6GfyWPNuc3LHD3HEIeIfsnJ4G62i0RsLTNxpYfnMk5PjwL7KN83s
w0BBWYSube2Ewb2nphWADWZo6aeOnoxTcP6RfL79rcq9P28xiNnV83QG8MVDnEph2YXQZ5yP66Tf0iv3Jth5kRWAPANFg6trs6UPHsvEIRBUjknjqdLzuGuo86C76a1nXvT
XXxiX0fKkpndd1OZ2Km9ModpTFjLcNeP0QYkrvpufMJFtBgyEFwSs52rzbpzTqZST7vmLPEI0iD2PucCBHwx1P14n1HPfWndvDezkllurmVodie
bandit5@bandit:~/inhere/maybehere07$ find -readable -type f -size 1033c ! -executable
./-file2
bandit5@bandit:~/inhere/maybehere07$ cat ./-file2
P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU
```

Bandit 5=>6

1.Logged on using ssh

Hostname : bandit5

Password : **lrIWWI6bB37kxfiCQZqUdOIYfr6eEeqR**

Port : 2220

Host : bandit.labs.overthewire.org

2.Looked for files using the ls command

3.Found a file named inhere and opened it

4.Found several files and thought they cant be checked one by one

5.Used the find command to find a file related to the clues given in the website

6.Used find -readable -type f -size 1033c ! -executable

7.Found the file in .maybeinhere07/.file02

8.First opened a wrong file and then corrected it

9.Found the password to be **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**

```
bandit6@bandit: ~  
find: '/run/user/11010': Permission denied  
find: '/run/user/11024': Permission denied  
find: '/run/user/11015': Permission denied  
find: '/run/user/11002': Permission denied  
find: '/run/user/11007': Permission denied  
find: '/run/user/11020': Permission denied  
find: '/run/user/0': Permission denied  
find: '/run/user/11025': Permission denied  
find: '/run/user/11016': Permission denied  
find: '/run/user/11003': Permission denied  
find: '/run/user/11006/systemd/inaccessible/dir': Permission denied  
find: '/run/user/11001': Permission denied  
find: '/run/user/11004': Permission denied  
find: '/run/user/11008': Permission denied  
find: '/run/user/11012': Permission denied  
find: '/run/user/11000': Permission denied  
find: '/run/user/11005': Permission denied  
find: '/run/user/11013': Permission denied  
find: '/run/user/11011': Permission denied  
find: '/run/sudo': Permission denied  
find: '/run/screen/S-bandit20': Permission denied  
find: '/run/multipath': Permission denied  
find: '/run/cryptsetup': Permission denied  
find: '/run/lvm': Permission denied  
find: '/run/credentials/systemd-sysusers.service': Permission denied  
find: '/run/systemd/propagate': Permission denied  
find: '/run/systemd/unit-root': Permission denied  
find: '/run/systemd/inaccessible/dir': Permission denied  
find: '/run/lock/lvm': Permission denied  
find: '/root': Permission denied  
find: '/sys/kernel/tracing': Permission denied  
find: '/sys/kernel/debug': Permission denied  
find: '/sys/fs/pstore': Permission denied  
find: '/sys/fs/bpf': Permission denied  
bandit6@bandit:~$ 2>/dev/null  
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S  
bandit6@bandit:~$
```

Bandit 6=>7

1.Logged on using ssh

Hostname : bandit6

Password : **P4L4vucdmLnm8I7VI7jG1ApGSfjYKqJU**

Port : 2220

Host : bandit.labs.overthewire.org

2.Looked for files using the ls command and found nothing

3.Used the find command “find / -user bandit7 -group bandit6 -size 33c 2>/dev/null”

4.Got a path to a file

5.Used cat on that path

6.Found out the password to be **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

```
bandit7@bandit: ~  
  
-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/)  
  
Both python2 and python3 are installed.  
  
--[ 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!  
  
bandit7@bandit:~$  
bandit7@bandit:~$ ls  
data.txt  
bandit7@bandit:~$ cat data.txt | grep millionth  
millionth      TESKZC0XvTetK0S9xNwm25STk5iWrBvP  
bandit7@bandit:~$
```

Bandit 7=>8

1. Logged on using ssh

Hostname : bandit7

Password : **z7WtoNQU2XfjmMtWA8u5rN4vzqu4v99S**

Port : 2220

Host : bandit.labs.overthewire.org

2. Used the ls command to search for files and found data.txt

3. It is said that the password is next to the word millionth

4. So I used "cat data.txt | grep millionth"

5. Found out the password to be **TESKZC0XvTetK0S9xNwm25STk5iWrBvP**


```
bandit9@bandit: ~  
-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/)  
  
Both python2 and python3 are installed.  
  
--[ 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!  
  
bandit9@bandit:~$  
bandit9@bandit:~$ ls  
data.txt  
bandit9@bandit:~$ strings data.txt | grep =====  
4===== the#  
===== password  
===== is  
===== G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s  
bandit9@bandit:~$
```

Bandit 9=>10

1. Logged on using ssh

Hostname : bandit9

Password : **EN632PlfYiZbn3PhVK3XOGSINInNE00t**

Port : 2220

Host : bandit.labs.overthewire.org

2. Used ls command to look for any files

3. Found data.txt

4. It is said that the password contains a series of = symbols

5. So used strings data.txt | grep =====

6. Found out the password to be **G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**

```
bandit10@bandit: ~  
-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/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit10@bandit:~$  
bandit10@bandit:~$ ls  
data.txt  
bandit10@bandit:~$ cat data.txt  
VGhlIHBhc3N3b3JkIGlzIDZ6UGV6aUxkuJ3SS05kTllGTmI2blZDS3pwaGXYSEJNCg==  
bandit10@bandit:~$ base64 -d data.txt  
The password is 6zPezilDR2RKNdNYFNb6nVCKzphlXHBM  
bandit10@bandit:~$
```

Bandit 10=>11

1. Logged on using ssh

Hostname : bandit10

Password : **G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s**

Port : 2220

Host : bandit.labs.overthewire.org

2. Used ls command to look for any files and found out data.txt

3. Opened the file using cat command

4. Looked at the two == symbols at the end and found out that it might be base 64 encoded string

5. Decoded it using base64 -d data.txt command

6. Found out the password to be **6zPezilDR2RKNdNYFNb6nVCKzphlXHBM**

```
bandit11@bandit: ~  
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/)  
  
Both python2 and python3 are installed.  
  
--[ More information ]--  
  
For more information regarding individual wargames, visit  
http://www.overthewire.org/wargames/  
  
For support, questions or comments, contact us on discord or IRC.  
  
Enjoy your stay!  
  
bandit11@bandit:~$  
bandit11@bandit:~$ lsw  
Command 'lsw' not found, but can be installed with:  
apt install suckless-tools  
Please ask your administrator.  
bandit11@bandit:~$ ls  
data.txt  
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf WIA00SFzMjXXBC0K0SKBbJ8puQm5LIEl  
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'  
The password is JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv  
bandit11@bandit:~$
```

Bandit 11=>12

1. Logged on using ssh

Hostname : bandit11

Password : **6zPeziLdR2RKNdNYFNb6nVCKzphlXHBM**

Port : 2220

Host : bandit.labs.overthewire.org

2. Used ls command to look for any files and found out data.txt

3. Opened the file using cat command and got a weird set of characters

4. Googled it for some clues and found it to be a rot 13 encoded string

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

6. Found out the password to be **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**

```
bandit12@bandit: /tmp/ax
modulo 2^32 581
bandit12@bandit:/tmp/ax$ mv data.out data.gz
bandit12@bandit:/tmp/ax$ gzip -d data.gz
gzip: data already exists; do you wish to overwrite (y or n)? y
bandit12@bandit:/tmp/ax$ file data
data: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/ax$ bzip2 -d data
bzip2: Can't guess original name for data -- using data.out
bandit12@bandit:/tmp/ax$ file data.out
data.out: gzip compressed data, was "data4.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size
modulo 2^32 20480
bandit12@bandit:/tmp/ax$ mv data.out data.gz
bandit12@bandit:/tmp/ax$ gzip -d data.gz
bandit12@bandit:/tmp/ax$ file data
data: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ax$ tar -xf data
bandit12@bandit:/tmp/ax$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ax$ tar -xf data5.bin
bandit12@bandit:/tmp/ax$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/ax$ bzip2 -d data6.bin
bzip2: Can't guess original name for data6.bin -- using data6.bin.out
bandit12@bandit:/tmp/ax$ file data6.bin.out
data6.bin.out: POSIX tar archive (GNU)
bandit12@bandit:/tmp/ax$ file data8.bin
data8.bin: cannot open 'data8.bin' (No such file or directory)
bandit12@bandit:/tmp/ax$ tar -xf data6.bin.out
bandit12@bandit:/tmp/ax$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Sun Apr 23 18:04:23 2023, max compression, from Unix, original size
modulo 2^32 49
bandit12@bandit:/tmp/ax$ gzip -d data8.gz
gzip: data8.gz: No such file or directory
bandit12@bandit:/tmp/ax$ mv data8.bin data8.gz
bandit12@bandit:/tmp/ax$ gzip -d data8.gz
bandit12@bandit:/tmp/ax$ file data8
data8: ASCII text
bandit12@bandit:/tmp/ax$ cat data8
The password is wbWdLBxEir4CaE8LaPhauuOo6pwRmrDw
bandit12@bandit:/tmp/ax$
```

Bandit 12=>13

1.Logged on using ssh

Hostname : bandit12

Password : **JVNBBFSmZwKKOP0XbFXOoW8chDz5yVRv**

Port : 2220

Host : bandit.labs.overthewire.org

2.Created a working folder using the mkdir command in *tmp/ax/*

3.Converted hex to binary using the xxd -x data.txt data.out

4.Checked the file type of data.out using the file command

5.It was in the gzip compressed format

6.Renamed data.out to data.gz using the mv command

7.So decompressed using the gzip -d data.gz command

8.Again used the file command and found out that data is in bzip2 compressed file

9.So decompressed it using the bzip2 -d data

10.It gave a prompt that the file name has been changed to data.out

11.Checked the file type and found out that it is again gzip compressed format

12.Changed its name to data.gz and decompressed it again

13.Now the file type is in POSIX tar archive

14.So I used the tar command to decompress and repeated this until the file is in the ASCII text format

15 Used cat command on the file after it is converted to ASCII file

16.Found the password to be **wbWdLBxEir4CaE8LaPhauuOo6pwRmrDw**


```
bandit14@bandit: ~  
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/)  
  
Both python2 and python3 are installed.  
  
--[ 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!  
  
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14 | nc localhost 30000  
Correct!  
jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt  
  
bandit14@bandit:~$
```

Bandit 14=>15

1. Logged in directly from level 13 using the sshkey.private
2. The password must be submitted to the port 30000
3. The password is in the *etc/bandit_pass/bandit14*
4. The pass can be submitted directly using *cat etc/bandit_pass/bandit14*
5. Got the password **jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**

```
bandit15@bandit: ~  
--[ 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/)  
  
Both python2 and python3 are installed.  
  
--[ 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!  
  
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15 | openssl s_client -connect localhost:30001 -quiet  
Can't use SSL_get_servername  
depth=0 CN = localhost  
verify error:num=18:self-signed certificate  
verify return:1  
depth=0 CN = localhost  
verify error:num=10:certificate has expired  
notAfter=Sep 12 14:56:16 2023 GMT  
verify return:1  
depth=0 CN = localhost  
notAfter=Sep 12 14:56:16 2023 GMT  
verify return:1  
Correct!  
JQtTfApK4SeyHwDII9SXGR50qclOAil1  
bandit15@bandit:~$
```

Bandit 15=>16

1. Logged on using ssh

Hostname : bandit15

Password : **jN2kgmIXJ6fShzhT2avhotn4Zcka6tnt**

Port : 2220

Host : bandit.labs.overthewire.org

2. 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.

3. The pass is in *etcbandit_pass/bandit15*

4. The pass can be submitted using the command `cat etc/bandit_pass/bandit15 | openssl s_client -connect localhost:>30001 -quiet`

5. Now we get the pass for the next level **JQtTfApK4SeyHwDII9SXGR50qclOAil1**


```
bandit17@bandit: ~  
DSt2McN4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30eKePQAzL0VUYBW  
JGTi65CxbCnzc/w4+mqQyvmzpwMtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX  
x0YVztz/zb1kPjfkU1jHS+9EbVNj+D1XF0JuaQIDAQABaoIBABagpXpM1aoLWfvD  
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUDE6SFth0ar69jp5RLwD1NhPx3iB1  
J9n0M80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd  
d8WErY0gPxun8pbJLmXkAtWNhpMvFe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC  
YNN6DDP2lbcBrvgT9YCNLC6C+ZKuFD52yQ09q0kwFTEQpjtF4uNtJom+asvlpM58A  
vLY9r60wYSvmZhnqBj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama  
+TOWHgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxBgRRhORT  
8c8hAuR8b2G62so8vUHK/fur850Efc9TncnCY2crpqsghifKLxrlgtT+qDpfZnx  
SatLdt8GFQ85yA7hnWJ2Mx3F3NaeSDm75Lsm+tBbAlyc9P2jGRNtMskCgYEAYpHd  
HCctNi/FwJulhtFf/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt  
SghaTdcG0Knyw1bpJvyusavPzpaJMjdJ6tcFhVAbAjm7enCIVGCSx+X3L5SiWg0A  
R57hJglezIiVjv3aGwHwvLzVtSzK6zV6oXFAu0ECgYAbj046T4hyP5tJi93V5Hdi  
Ttlek7xRVXuL+iu7rWkGAXFpMLFteQEsRr7Pj/LemMEY5eTDAFMLy9FL2m9oQWcG  
R8vdsK8r9FGLS+9aKcV5PI/WEKlwgXlnB30hYimtiG2Cg5JCqIZFHxD6MjEG0tu  
L8ktHMPvodbWnsSBULpG0QKGBApLTfC1H0nWimGOU3KPwYwt006CdTkmJ0mL8Ni  
blh9eLyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU  
Y0dJHdS0oKvDQNWu6ucylRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM  
77pBAoGAMmjmJdjp+Ez8duyn3ieo36yrttf5NSsJLabxPdlc1gvtGCWH+9Cq0b  
dxviW8+TFVEBL104f7HvM6EpTscdDxu+bCXWkfjURb7Dy9Gott9JPsx8MBTakh3  
vBgsyI/sN3RqRBcGU40f0oZyFAMT8s1m/uYv5206Igeuz/ujbjY=  
-----END RSA PRIVATE KEY-----  
  
bandit16@bandit:~$ mkdir /tmp/bandit100  
bandit16@bandit:~$ cd /tmp/bandit100  
bandit16@bandit:/tmp/bandit100$ nano sshkey.private  
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory  
It is required for saving/loading search history or cursor positions.  
  
bandit16@bandit:/tmp/bandit100$ nano sshkey.private  
Unable to create directory /home/bandit16/.local/share/nano/: No such file or directory  
It is required for saving/loading search history or cursor positions.  
  
bandit16@bandit:/tmp/bandit100$ ls  
sshkey.private  
bandit16@bandit:/tmp/bandit100$ chmod 400 sshkey.private  
bandit16@bandit:/tmp/bandit100$ ssh -i sshkey.private bandit17@bandit.labs.overthewire.org -p 2220  
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([127.0.0.1]:2220)' can't be established.  
ED25519 key fingerprint is SHA256:C2ihUBV7ihNv1wUXRb4RrEcLFXC5CXlhmAAM/ureryLY.
```

Bandit 16=>17

1.Logged on using ssh

Hostname : bandit16

Password : **JqttfApK4SeyHwDII9SXGR50qclOAil1**

Port : 2220

Host : bandit.labs.overthewire.org

2.Search for open ports in between 31000 and 32000 which have server listening on them and must speak ssl

3.So I used “for i in {31000..32000} ; do”

> SERVER="localhost"

> PORT=\$i

> (echo > /dev/tcp/\$SERVER/\$PORT) >& /dev/null &&

> echo "Port \$PORT open"

4. This gave me 5 ports out of which only two have echo and one have ssl listening to it

5.So the password has been sent to the port 31790 using the command “cat /etc/bandit_pass/bandit16 | openssl s_client -connect localhost:31790 -quiet”

5.Sending the pass gave me a private rsa key

6.Now I created a directory using the mkdir command

7.Used the nano command to save the private key and named it to be sshkey.private

8.Now used chmod 400 sshkey.private to change the permission of the key to only admin

9.Now I used this key to directly access level 17

```
nikhil@Ubuntu22: ~  
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/)  
  
Both python2 and python3 are installed.  
--[ 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.old passwords.new  
42c42  
< glZreTEH1V3cGKL6g4conYqZqaEj0mte  
---  
> hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg  
bandit17@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
bandit16@bandit:/tmp/bandit100$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.  
nikhil@Ubuntu22:~$
```

Bandit 17=>18

1. Logged in directly from level 16 using the private key given previously
2. Ran the ls command to look for the password files
3. Used diff command to compare the two files line by line
4. Used the first line of password and my permission to level 18 got denied
5. Now used the second line of password and got "ByeBye" at the end
6. Second line is **hga5tuuCLF6fFzUpnagiMN8ssu9LFrdg**


```
bandit19@bandit: ~  
-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/)  
  
Both python2 and python3 are installed.  
  
--[ 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  
Run a command as another user.  
Example: ./bandit20-do id  
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20  
VxCazJaVyKI6W36BkBU0mJTCM8rR95XT  
bandit19@bandit:~$
```

Bandit 19=>20

1. Logged on using ssh

Hostname : bandit19

Password : **awhqfNnAbc1naukrpqDYcF95h7HoMTrC**

Port : 2220

Host : bandit.labs.overthewire.org

2. Used ls command to check for files

3. The password must be accessed as another user bandit20-do

4. So I used the command `./bandit20-do cat "/etc/bandit_pass/bandit20"`

5. Found out the password to be **VxCazJaVyKI6W36BkBU0mJTCM8rR95XT**

```
nikhil@Ubuntu22:~$ cat /etc/ld.so.conf.d/x86_64-linux-gnu.conf
# This file is meant to maintain the linker configuration in a
# central place, to allow us to change it without having to
# recompile everything. Comments are permitted, but they
# must be put after the *standard* configuration files.
# Please never change the order in which these are listed.
# The linker always starts with these files:
# /usr/share/ld.so.conf.d/*.conf
# /etc/ld.so.conf
# /etc/ld.so.conf.d/*.conf
# This file is meant to maintain the linker configuration in a
# central place, to allow us to change it without having to
# recompile everything. Comments are permitted, but they
# must be put after the *standard* configuration files.
# Please never change the order in which these are listed.
# The linker always starts with these files:
# /usr/share/ld.so.conf.d/*.conf
# /etc/ld.so.conf
# /etc/ld.so.conf.d/*.conf

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/
* pmttools (https://github.com/Gallopsled/pmttools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ 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!

bandit20@bandit: $
bandit20@bandit: $ ./suconnect 31337
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
timed out waiting for input: auto-logout
Connection to bandit.labs.overthewire.org closed.
nikhil@Ubuntu22:~$
```

```
nikhil@Ubuntu22:~$ cat /etc/ld.so.conf.d/x86_64-linux-gnu.conf
# This file is meant to maintain the linker configuration in a
# central place, to allow us to change it without having to
# recompile everything. Comments are permitted, but they
# must be put after the *standard* configuration files.
# Please never change the order in which these are listed.
# The linker always starts with these files:
# /usr/share/ld.so.conf.d/*.conf
# /etc/ld.so.conf
# /etc/ld.so.conf.d/*.conf
# This file is meant to maintain the linker configuration in a
# central place, to allow us to change it without having to
# recompile everything. Comments are permitted, but they
# must be put after the *standard* configuration files.
# Please never change the order in which these are listed.
# The linker always starts with these files:
# /usr/share/ld.so.conf.d/*.conf
# /etc/ld.so.conf
# /etc/ld.so.conf.d/*.conf

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/
* pmttools (https://github.com/Gallopsled/pmttools)
* radare2 (http://www.radare.org/)

Both python2 and python3 are installed.

--[ 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!

bandit20@bandit: $
bandit20@bandit: $ nc -lp 31337 < /etc/bandit_pass/bandit20
NvEJF7oVjkddltPSrdKEF0llh9V1IBcq
timed out waiting for input: auto-logout
Connection to bandit.labs.overthewire.org closed.
nikhil@Ubuntu22:~$
```

Bandit 20=>21

1. Logged on using ssh

Hostname : bandit20

Password : VxCazJaVykI6W36BkBU0mJTCM8rR95XT

Port : 2220

Host : bandit.labs.overthewire.org

2. Established a connection with ./suconnect 31337 command

3. Sent the password through another terminal using nc command

4. Then got the password NvEJF7oVjkddltPSrdKEF0llh9V1IBcq