Task_7

Linux Games

LIST OF PASSWORDS FOUND

- boJ9jbbUNNfktd78OOpsqOItutMc3MY1
- CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
- UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
- pIwrPrtPN36QITSp3EQaw936yaFoFgAB
- koReBOKuIDDepwhWk7jZC0RTdopnAYKh
- DXjZPULLxYr17uwoI01bNLQbtFemEgo7
- HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
- cvX2JJa4CFALtqS87jk27qwqGhBM9pIV
- UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
- truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
- IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
- 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
- 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
- 4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
- BfMYroe26WYalil77FoDi9qh59eK5xNr

```
   -m32                    compile for 32bit
   -fno-stack-protector    disable ProPolice
   -Wl,-z,norelro          disable relro

 In addition, the execstack tool can be used to flag the stack as
 executable on ELF binaries.

 Finally, network-access is limited for most levels by a local
 firewall.

--[ Tools ]--

 For your convenience we have installed a few usefull tools which you can find
 in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

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

 Enjoy your stay!

bandit0@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root    root     4096 May  7  2020 ./
4 drwxr-xr-x 41 root    root     4096 May  7  2020 ../
4 -rw-r--r--  1 root    root      220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root    root     3526 May 15  2017 .bashrc
4 -rw-r--r--  1 root    root      675 May 15  2017 .profile
4 -rw-r-----  1 bandit1 bandit0    33 May  7  2020 readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$
```

password-1

boJ9jbbUNNfktd78OOpsqOltut
Mc3MY1

```
    -m32                    compile for 32bit
    -fno-stack-protector    disable ProPolice
    -Wl,-z,norelro          disable relro

  In addition, the execstack tool can be used to flag the stack as
  executable on ELF binaries.

  Finally, network-access is limited for most levels by a local
  firewall.

--[ Tools ]--

  For your convenience we have installed a few usefull tools which you can find
  in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

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

  Enjoy your stay!

bandit1@bandit:~$ ls -alps
total 24
4 -rw-r-----  1 bandit2 bandit1   33 May  7  2020 -
4 drwxr-xr-x  2 root    root    4096 May  7  2020 ./
4 drwxr-xr-x 41 root    root    4096 May  7  2020 ../
4 -rw-r--r--  1 root    root     220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root    root    3526 May 15  2017 .bashrc
4 -rw-r--r--  1 root    root     675 May 15  2017 .profile
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ █
```

password-2

CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9

password-3

UmHadQclWmgdLOKQ3YNgjWxGoR
Mb5luK

```
bandit2@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  2 root     root     4096 May  7  2020 ./
4 drwxr-xr-x 41 root     root     4096 May  7  2020 ../
4 -rw-r--r--  1 root     root      220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root     root     3526 May 15  2017 .bashrc
4 -rw-r--r--  1 root     root      675 May 15  2017 .profile
4 -rw-r-----  1 bandit3 bandit2    33 May  7  2020 spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@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 usefull tools which you can find
in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[More information]--

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

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

Enjoy your stay!

bandit3@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root 4096 May 7 2020 ./
4 drwxr-xr-x 41 root root 4096 May 7 2020 ../
4 -rw-r--r-- 1 root root 220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root 3526 May 15 2017 .bashrc
4 drwxr-xr-x 2 root root 4096 May 7 2020 inhere/
4 -rw-r--r-- 1 root root 675 May 15 2017 .profile
bandit3@bandit:~$ cd inhere/
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root   root   4096 May 7 2020 .
drwxr-xr-x 3 root   root   4096 May 7 2020 ..
-rw-r----- 1 bandit4 bandit3   33 May 7 2020 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$

password-4

pIwrPrtPN36QITSp3EQaw936
yaFoFgAB

password-5

koReBOKuIDDepwhWk7jZC0R

TdopnAYKh

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

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

Enjoy your stay!

bandit4@bandit:~$ ls -alps
total 24
4 drwxr-xr-x  3 root root 4096 May  7  2020 ./
4 drwxr-xr-x 41 root root 4096 May  7  2020 ../
4 -rw-r--r--  1 root root  220 May 15  2017 .bash_logout
4 -rw-r--r--  1 root root 3526 May 15  2017 .bashrc
4 drwxr-xr-x  2 root root 4096 May  7  2020 inhere/
4 -rw-r--r--  1 root root  675 May 15  2017 .profile
bandit4@bandit:~$ cd inhere/
bandit4@bandit:~/inhere$ ls
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ find .type f | xargs file
find: '.type': No such file or directory
find: 'f': No such file or directory
Usage: file [-bcEhikLlNnprsvzZ0] [--apple] [--extension] [--mime-encoding] [--mime-type]
            [-e testname] [-F separator] [-f namefile] [-m magicfiles] file ...
       file -C [-m magicfiles]
       file [--help]
bandit4@bandit:~/inhere$ find . -type f | xargs file
./-file01: data
./-file00: data
./-file06: data
./-file03: data
./-file05: data
./-file08: data
./-file04: data
./-file07: ASCII text
./-file02: data
./-file09: data
bandit4@bandit:~/inhere$ man xarg
No manual entry for xarg
bandit4@bandit:~/inhere$ man xarg
No manual entry for xarg
bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$
```

password-6

DXjZPULLxYr17uwoI01bNLQb

FemEgo7

⊞

Finally, network-access is limited for most levels by a local
firewall.

--[Tools]--

For your convenience we have installed a few usefull tools which you can find
in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[More information]--

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

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

 Enjoy your stay!

bandit5@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 3 root root   4096 May 7 2020 ./
4 drwxr-xr-x 41 root root   4096 May 7 2020 ../
4 -rw-r--r-- 1 root root   220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root root   3526 May 15 2017 .bashrc
4 drwxr-x--- 22 root bandit5 4096 May 7 2020 inhere/
4 -rw-r--r-- 1 root root   675 May 15 2017 .profile
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7

```
find: '/tmp': Permission denied
find: '/run/lvm': Permission denied
find: '/run/screen/S-bandit1': Permission denied
find: '/run/screen/S-bandit10': Permission denied
find: '/run/screen/S-bandit29': Permission denied
find: '/run/screen/S-bandit25': Permission denied
find: '/run/screen/S-bandit30': Permission denied
find: '/run/screen/S-bandit9': Permission denied
find: '/run/screen/S-bandit28': Permission denied
find: '/run/screen/S-bandit18': Permission denied
find: '/run/screen/S-bandit20': Permission denied
find: '/run/screen/S-bandit12': Permission denied
find: '/run/screen/S-bandit5': Permission denied
find: '/run/screen/S-bandit7': Permission denied
find: '/run/screen/S-bandit16': Permission denied
find: '/run/screen/S-bandit26': Permission denied
find: '/run/screen/S-bandit8': Permission denied
find: '/run/screen/S-bandit15': Permission denied
find: '/run/screen/S-bandit4': Permission denied
find: '/run/screen/S-bandit3': Permission denied
find: '/run/screen/S-bandit19': Permission denied
find: '/run/screen/S-bandit31': Permission denied
find: '/run/screen/S-bandit17': Permission denied
find: '/run/screen/S-bandit2': Permission denied
find: '/run/screen/S-bandit22': Permission denied
find: '/run/screen/S-bandit21': Permission denied
find: '/run/screen/S-bandit14': Permission denied
find: '/run/screen/S-bandit13': Permission denied
find: '/run/screen/S-bandit24': Permission denied
find: '/run/screen/S-bandit23': Permission denied
find: '/run/shm': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/tmp': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/log': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

password-7

HKBPTKQnIay4Fw76bEy8PVxKE
DQRKTzs

```
Swift's Yb8oofacCaFdLNJqllKbwf0ej2M5bwBg
wrongheadedness's        gjfU53A1Bf0iitkMov3rlgbRHq6MIhiq
scrutinizes      Z76LPyf1l8HqhuJowIqY4ModCocDFOB9
refresher's      dtfQgdVItYRi4Ufx4iD5YEOIZrmKnDcu
earthlings       IhFcUS01RouQ8UG45WVUVsPDZkTr6wnJ
Hera's  gAcRYahuux36AcOjmG0gP4ulwKevvD3X
ferment's        DTTiALtV7wmDYZoQ4MSm97bJdCmNkw2P
Anouilh MKKDDki6xvFczsBxhWEXsfeMA00MoJaC
overabundance    ES9eqyfmh8uBO3XqT0AR7EKGgyCQ1IFk
complement's     MCWy3WxEeWqckXZ5G4Sp950Y36l2F5fJ
grape   g0OpwTZt0lzUZ6sS3pijp0z7O9LAhPxu
Blaine  k61rOI4u0D2PMEXLd2RDxQWIE8tACyst
canonization's  7ITrZvFVzsjujBHVlu4gfcHbW1gWQUcN
reserve AHO3PedgUR05aCaQVGVFQRgY2oR1SBYh
Zanuck  30KRlOQjnCq5DyqNZePHAD6tCZbVjT1f
baritone         XSodKcCZa05ckkLyP4uXwrjIVaCzKcpq
lineman's        Gh8HTLmWxnXJxZF4DzhuiRpV8xejb6yw
aquas   RkI4EWYAjHPMexRFTY9Rq7vQtjhiKgZw
swaddled         snDpr6ve7nuPsjBoTGLrmpOYomdhVzAH
garishness's     UbK1yZ2nC02GEjArlASLw0bT8jgOp9rx
Benny's QQkZrdiFs47KckVLi5ifsFqtLcRxyjvZ
regulated        sxJ8HT73fvZMMIicL50nhawcrsYGUiWP
knotting         vh268WJXw1OSnszed9MVaHD4rTP69lZr
hymnals 7MqsN32lfDbPigtAX6cwFbMZcPAMUoae
Fremont tCy02wC8xdpFqjlZ8xdBQYAHFZPHk7ls
punter's         zAfzaA1IOuBSamCR6eMmRoc9oNXPQ16a
junking 6Tlr5K8YZ1d2Xsdku3TTFYXWB6WOMXyT
Aymara  zSeUS0UyD8Q6a6YPwaClRBbk1x8kFBEc
waned   gL59r6xvewh5y8t0mgiNtHtCUMG8S6Id
conceded         TWLUptX3HbwD4qsYOQ9sENOnOiNy79sC
kilned  kLjrgoJvftIyUyotuOI4cxFcxQXbC6aS
Santayana        KKn1I4fuWdzKyvffp1aYrBDzQa3Tr3Pk
Antigua dRyNieqAg0OkCgrKVQFXMXS06vFArL55
heyday  UAGwMlFzylGa4fHpQZEelUQEZ5JlUpyX
praiseworthiness's       bjRB0uGXM4dH7ip9hHB3mbFBMMwlNKNq
separatism       p2167YTCJseAv4YhLZNb2fs7JivlDLUW
plan    PLz4ZXwX02fEe4oMd1I78wQXl4MIMxTf
confrontation    KlHScgMgzyBQYxBXkxsjKcQ2A5erDIjL
briquet's        aHc51xHj1t3ANF7jH26dd7mHWBfd8VKz
encapsulate      STOVYQEMWtFz54JtjJRrhDXgZcfVw8lS
wildfowls        PqcMofjmKj8NBvO9exdu7FY2NG6WUMzb
Finland xgXsIYgqUCMriMoT7W2dSwTG1DCvbRvU
bandit7@bandit:~$ strings data.txt | grep "millionth"
millionth        cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

password-8

cvX2JJa4CFALtqS87jk27qwqGhBM9plV

```
10 l1I3Red7uSH9n3OOylHP2hQDbOU0qGaq
10 l2lECnJkQk8EBl6IO3gHUlnjoCTF1has
10 LfrBHfAh0pP9bgGAZP4QrVkut3pysAYC
10 Lg4vWWvEY7s0bG6BRiA35AHzo2gM6lHg
10 mpgNGRH628hTQxajScbagkxaPKklUhjn
10 mzOW32HQZi14kwrdeiquO1LCbyaOtbiT
10 nJRb4MipHMdTmFylFc1NlqmywgxDSdoI
10 NLWvtQvL7EaqBNx2x4eznRlQONULlCYZ
10 NOdH1kFWibx4XnNaJoLFmghBn7oIs5hb
10 ojGabNG5NJ9ppKUBXGr8lwMRRS5GuiA5
10 OZ1wgx8bDI0vFOFxDQH32eMMcIPiIuPE
10 PfbMe4Xb3mw5mJmabIbKAXKCU7zynDHl
10 PQKOeIQwTw490Y8yobuxZAOL4cNmVo1D
10 PSdVQSeUUBPRZD58WWP0OXLKxSgU3RxX
10 ptb5ZW8TcgD3U6gOGCcN31xCDGIoQSEa
10 qaWWAOOquC3yHnfJI4zvPWzCBdfHQ8wa
10 RMiSPoAvF7WhgIcOdSQR2r6Zx0DNS5UW
10 s1603Q2r4RPKqyoA8cspIRk0VdgEmFC3
10 SA05uWMVCao2rzS8YRqUXh19SvnDpuOl
10 SHMAMUEzQe4mV7SJpETTZFsyNRJsZE2k
10 si952kS1y6pt4AFenmm0oIp8n7W5d3bd
10 sYSokIATVvFUKU4sAHTtMarfjlZWWj5i
10 SzwgS2ADSjP6ypOzp2bIvdqNyusRtrHj
10 TKUtQbeYnEzzYIne7BinoBx2bHFLBXzG
10 TThRArdF2ZEXMO47TIYkyPPLtvzzLcDf
10 tVW9iY1Ml0uHPK4usZnN8oZXbjRt2ATY
10 U0NYdD3wHZKpfEg9qGQOLJimAJy6qxhS
10 UASW6CQwD6MRzftu6FAfyXBK0cVvnBLP
10 UJiCNvDNfgb3fcCj8PjjnAXHqUM63Uyj
10 UjsVbcqKeJqdCZQCDMkzv6A9X7hLbNE4
 1 UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
10 UVnZvhiVQECraz5jl8U14sMVZQhjuXia
10 V2d9umHiuPLYLIDsuHj0frOEmreCZMaA
10 v9zaxkVAOdIOlITZY2uoCtB1fX2gmly9
10 VkBAEWyIibVkeURZV5mowiGg6i3m7Be0
10 w4zUWFGTUrAAh8lNkS8gH3WK2zowBEkA
10 WBqr9xvf6mYTT5kLcTGCG6jb3ex94xWr
10 wjNwumEX58RUQTrufHMciWz5Yx10GtTC
10 X1JHOUkrb4KgugMXIzMWWIWvRkeZleTI
10 XyeJdbrUJyGtdGx8cXLQST0pwu5cvpcA
10 yo0HbSe2GM0jJNhRQLxwoPp7ayYEmRKY
10 ySvsTwlMgnUF0n86Fgmn2TNjkSOlrV72
10 Z9OC6DQpppreChPhwRJJV9YYTtrxNVcO
10 zdd2ctVveROGeiS2WE3TeLZMeL5jL7iM
bandit8@bandit:~$
```

password-9

UsvVyFSfZZWbi6wgC7dAFyFu
R6jQQUhR

password-10

truKLdjsbJ5g7yyJ2X2R0o3a5H
QJFuLk

bandit9@bandit: ~

```
--[ Tools ]--

 For your convenience we have installed a few usefull tools which you can find
 in the following locations:

     * gef (https://github.com/hugsy/gef) in /usr/local/gef/
     * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
     * peda (https://github.com/longld/peda.git) in /usr/local/peda/
     * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
     * pwntools (https://github.com/Gallopsled/pwntools)
     * radare2 (http://www.radare.org/)
     * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

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

 Enjoy your stay!

bandit9@bandit:~$ ls -alps
total 40
 4 drwxr-xr-x  2 root     root      4096 May  7  2020 ./
 4 drwxr-xr-x 41 root     root      4096 May  7  2020 ../
 4 -rw-r--r--  1 root     root       220 May 15  2017 .bash_logout
 4 -rw-r--r--  1 root     root      3526 May 15  2017 .bashrc
20 -rw-r-----  1 bandit10 bandit9  19379 May  7  2020 data.txt
 4 -rw-r--r--  1 root     root       675 May 15  2017 .profile
bandit9@bandit:~$ strings data.txt | grep "="
========== the*2i"4
=:G e
========== password
<I=zsGi
Z)========== is
A=|t&E
Zdb=
c^ LAh=3G
*SF=s
&========== +truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
```

Show Applications

```
bandit9@bandit:~$
```

password-11

lFukwKGsFW8MOq3IRFqrxE1h

xTNEbUPR

In addition, the execstack tool can be used to flag the stack as
executable on ELF binaries.

Finally, network-access is limited for most levels by a local
firewall.

--[Tools]--

For your convenience we have installed a few usefull tools which you can find
in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[More information]--

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

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

Enjoy your stay!

bandit10@bandit:~$ ls -alps
total 24
4 drwxr-xr-x 2 root   root   4096 May 7 2020 ./
4 drwxr-xr-x 41 root   root   4096 May 7 2020 ../
4 -rw-r--r-- 1 root   root   220 May 15 2017 .bash_logout
4 -rw-r--r-- 1 root   root   3526 May 15 2017 .bashrc
4 -rw-r----- 1 bandit11 bandit10   69 May 7 2020 data.txt
4 -rw-r--r-- 1 root   root   675 May 15 2017 .profile
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIElGdWt3S0dzRlc4TU9xM0lSRnFyeEUxaHhUTkViVVBSCg==
bandit10@bandit:~$ base
-bash: base: command not found
bandit10@bandit:~$ base64 -d data.txt
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$

password-12

5Te8Y4drgCRfCx8ugdwuEX8KF
                    C6k2EUu

Options ⚙   About / Support ❓

Recipe 💾 📁 🗑

Input   start: 49   length: 49   ➕ 📁 ⤵ 🗑 ▦
             end: 49   lines: 2
             length: 0

ROT13 🚫 ❚❚

☑ Rotate lower case chars   ☑ Rotate upper case chars

☐ Rotate numbers

Amount
13

Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh

Output   start: 49   time: 2ms   💾 📋 ⬆ ↺ ⛶
             end: 49   length: 49
             length: 0   lines: 2

The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu

bandit12@bandit: /tmp/yashaa   🔍 ☰ — ▢ ✕

```
bandit12@bandit:/tmp/yashaa$ tar -x -f tas.tar
bandit12@bandit:/tmp/yashaa$ ls
data5.bin  data.txt  tas.tar
bandit12@bandit:/tmp/yashaa$ file glue.bin
glue.bin: cannot open 'glue.bin' (No such file or directory)
bandit12@bandit:/tmp/yashaa$ file data5.bin
data5.bin: POSIX tar archive (GNU)
bandit12@bandit:/tmp/yashaa$ ls
data5.bin  data.txt  tas.tar
bandit12@bandit:/tmp/yashaa$ mv data5.bin data5.tar
bandit12@bandit:/tmp/yashaa$ tar -x -f data5.tar
bandit12@bandit:/tmp/yashaa$ ls
data5.tar  data6.bin  data.txt  tas.tar
bandit12@bandit:/tmp/yashaa$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k
bandit12@bandit:/tmp/yashaa$ ls
data5.tar  data6.bin  data.txt  tas.tar
bandit12@bandit:/tmp/yashaa$ mv data6.bzip.out data6.bz2
mv: cannot stat 'data6.bzip.out': No such file or directory
bandit12@bandit:/tmp/yashaa$ mv data6.bzip2.out data6.bz2
mv: cannot stat 'data6.bzip2.out': No such file or directory
bandit12@bandit:/tmp/yashaa$ bzip -d data6.bz2
-bash: bzip: command not found
bandit12@bandit:/tmp/yashaa$ ls
data5.tar  data6.bin  data.txt   tas.tar
bandit12@bandit:/tmp/yashaa$  mv data5.bin data5.tar
mv: cannot stat 'data5.bin': No such file or directory
bandit12@bandit:/tmp/yashaa$ mv data66.bin data6.tar
mv: cannot stat 'data66.bin': No such file or directory
bandit12@bandit:/tmp/yashaa$ mv data6.bin data6.tar
bandit12@bandit:/tmp/yashaa$ tar -x -f data6.tar
bandit12@bandit:/tmp/yashaa$ ls
data5.tar  data6.tar  data8.bin  data.txt  tas.tar
bandit12@bandit:/tmp/yashaa$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu May  7 18:14:30 2020, max c
ompression, from Unix
bandit12@bandit:/tmp/yashaa$ mv data8.bin data8.gz
bandit12@bandit:/tmp/yashaa$ gzip -d data8.gz
bandit12@bandit:/tmp/yashaa$ ls
data5.tar  data6.tar  data8  data.txt  tas.tar
bandit12@bandit:/tmp/yashaa$ file data8
data8: ASCII text
bandit12@bandit:/tmp/yashaa$ cat data8
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/yashaa$
```

password-13

8ZjyCRiBWFYkneahHwxCv3w
b2a1ORpYL

bandit14@bandit: ~

      * again, DONT POST SPOILERS!
        This includes writeups of your solution on your blog or website!

--[Tips]--

    This machine has a 64bit processor and many security-features enabled
    by default, although ASLR has been switched off. The following
    compiler flags might be interesting:

        -m32   compile for 32bit
        -fno-stack-protector   disable ProPolice
        -Wl,-z,norelro   disable relro

    In addition, the execstack tool can be used to flag the stack as
    executable on ELF binaries.

    Finally, network-access is limited for most levels by a local
    firewall.

--[Tools]--

    For your convenience we have installed a few usefull tools which you can find
    in the following locations:

        * gef (https://github.com/hugsy/gef) in /usr/local/gef/
        * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
        * peda (https://github.com/longld/peda.git) in /usr/local/peda/
        * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
        * pwntools (https://github.com/Gallopsled/pwntools)
        * radare2 (http://www.radare.org/)
        * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[More information]--

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

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

    Enjoy your stay!

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

password-14

4wcYUJFw0k0XLShlDzztnTBHiq
xU3b3e

password-15

BfMYroe26WYalil77FoDi9qh59e

K5xNr

bandit14@bandit: ~

Finally, network-access is limited for most levels by a local
firewall.

--[Tools]--

For your convenience we have installed a few usefull tools which you can find
in the following locations:

    * gef (https://github.com/hugsy/gef) in /usr/local/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /usr/local/pwndbg/
    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[More information]--

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

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

  Enjoy your stay!

bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000

Wrong! Please enter the correct current password
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000

Wrong! Please enter the correct current password
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$

```
        * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
        * pwntools (https://github.com/Gallopsled/pwntools)
        * radare2 (http://www.radare.org/)
        * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/checksec.sh

--[ More information ]--

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

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

  Enjoy your stay!

bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
BfMYroe26WYalil77FoDi9qh59eK5xNr
bandit15@bandit:~$ man nc | grep ssl
bandit15@bandit:~$ man nc
bandit15@bandit:~$ man ncat
bandit15@bandit:~$ man ncat | grep ssl
            --ssl                      Connect or listen with SSL
            --ssl-cert                 Specify SSL certificate file (PEM) for listening
            --ssl-key                  Specify SSL private key (PEM) for listening
            --ssl-verify               Verify trust and domain name of certificates
            --ssl-trustfile            PEM file containing trusted SSL certificates
            --ssl-ciphers              Cipherlist containing SSL ciphers to use
        --ssl (Use SSL)
        --ssl-verify (Verify server certificates)
            In client mode, --ssl-verify is like --ssl except that it also
            --ssl-trustfile to give a custom list. Use -v one or more times to
        --ssl-cert certfile.pem (Specify SSL certificate)
            connect mode). Use it in combination with --ssl-key.
        --ssl-key keyfile.pem (Specify SSL private key)
            that goes with the certificate named with --ssl-cert.
        --ssl-trustfile cert.pem (List trusted certificates)
            combined with --ssl-verify. The argument to this option is the name
        --ssl-ciphers cipherlist (Specify SSL ciphersuites)
            http://www.openssl.org
bandit15@bandit:~$ ncat --ssl localhost 30001
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd
```