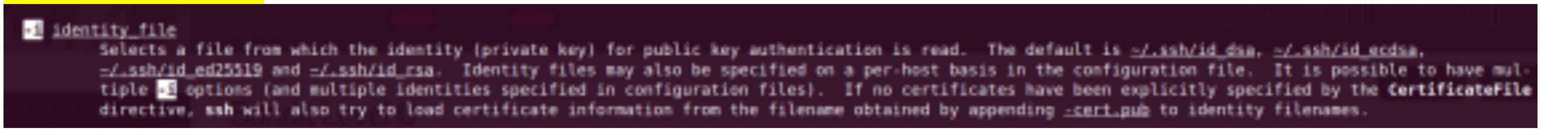
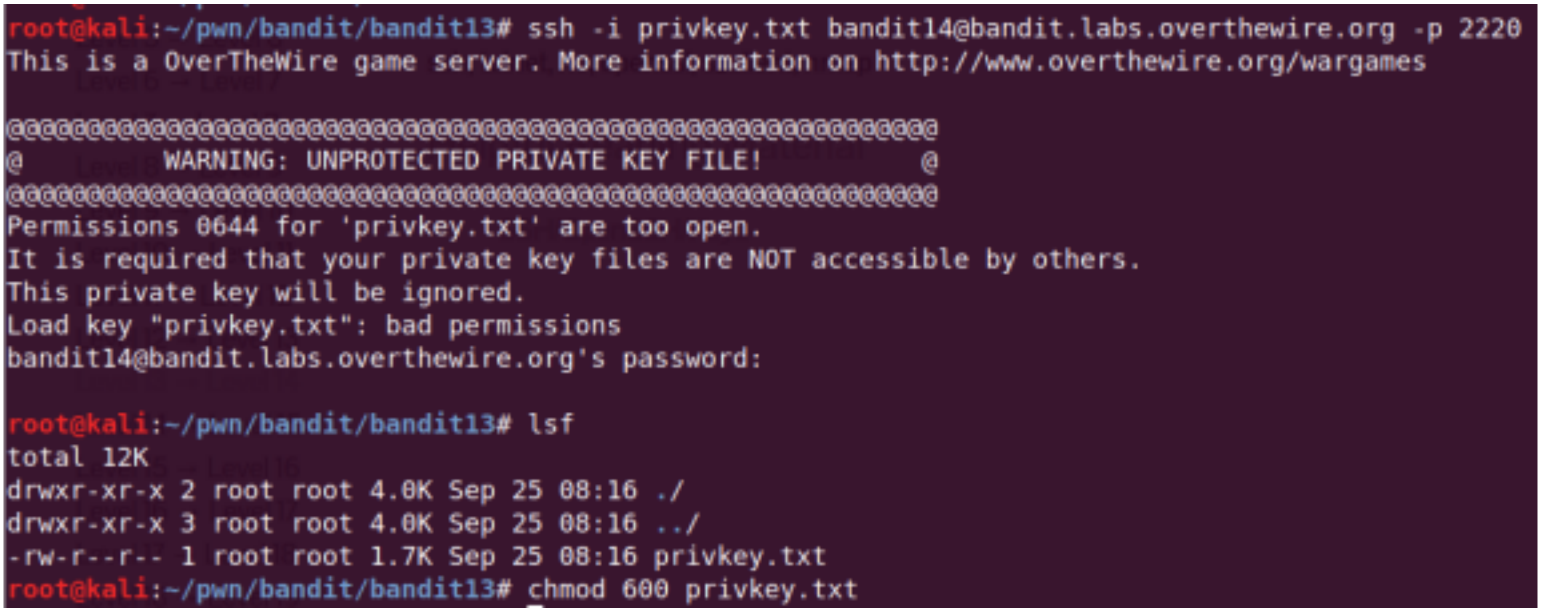
Bandit

bandit13

Uses of -i switch



```
-i identity_file
        Selects a file from which the identity (private key) for public key authentication is read.  The default is ~/.ssh/id_dsa, ~/.ssh/id_ecdsa,
        ~/.ssh/id_ed25519 and ~/.ssh/id_rsa.  Identity files may also be specified on a per-host basis in the configuration file.  It is possible to have mul-
        tiple -i options (and multiple identities specified in configuration files).  If no certificates have been explicitly specified by the CertificateFile
        directive, ssh will also try to load certificate information from the filename obtained by appending -cert.pub to identity filenames.
```

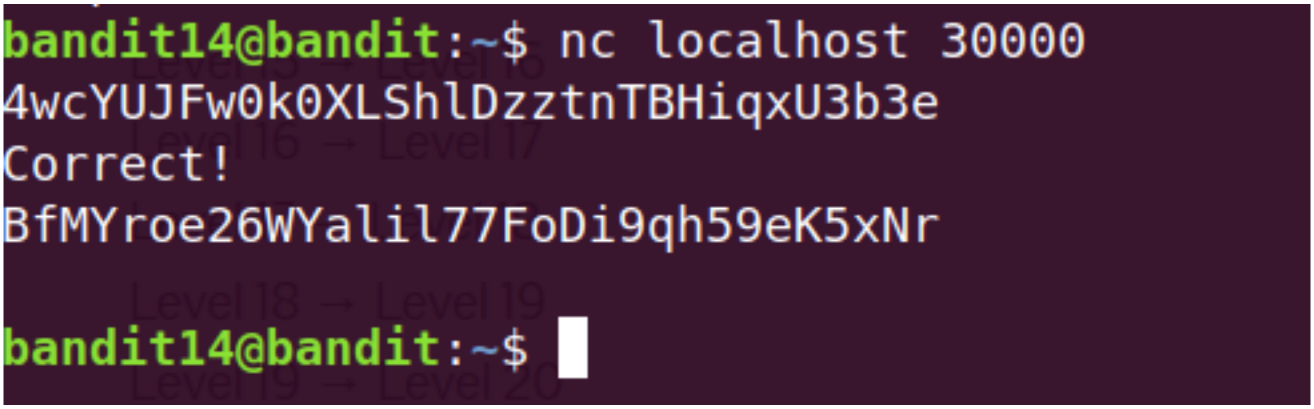


```
root@kali:~/pwn/bandit/bandit13# ssh -i privkey.txt bandit14@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'privkey.txt' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "privkey.txt": bad permissions
bandit14@bandit.labs.overthewire.org's password:

root@kali:~/pwn/bandit/bandit13# lsf
total 12K
drwxr-xr-x 2 root root 4.0K Sep 25 08:16 ./
drwxr-xr-x 3 root root 4.0K Sep 25 08:16 ../
-rw-r--r-- 1 root root 1.7K Sep 25 08:16 privkey.txt
root@kali:~/pwn/bandit/bandit13# chmod 600 privkey.txt
```

No problem loggin in after that.

bandit14

/etc/bandit_pass/bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e

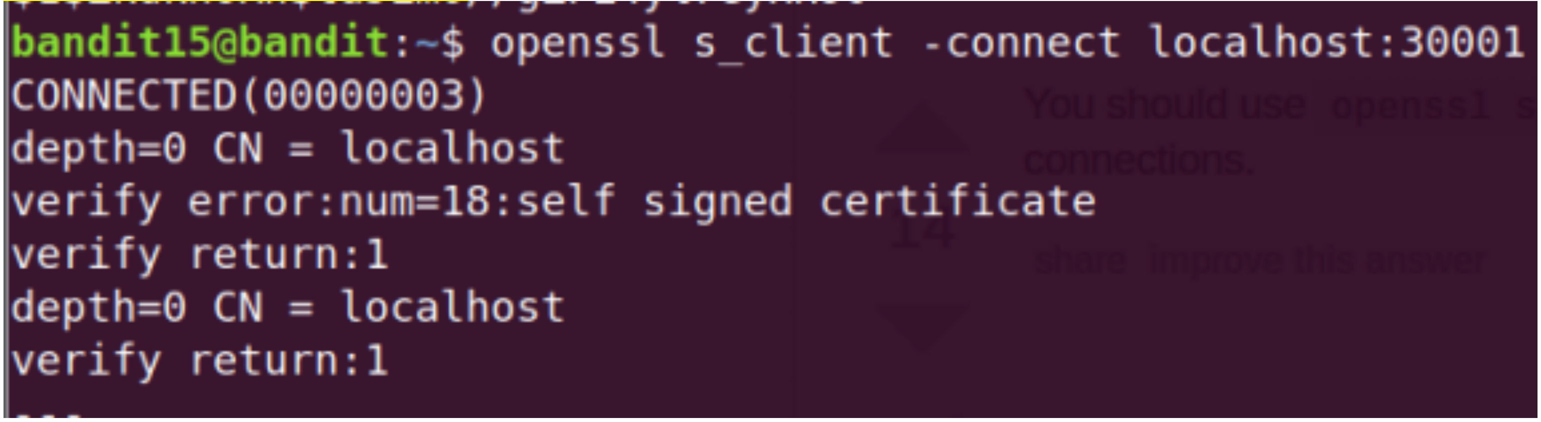


```
bandit14@bandit:~$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:~$ 
```

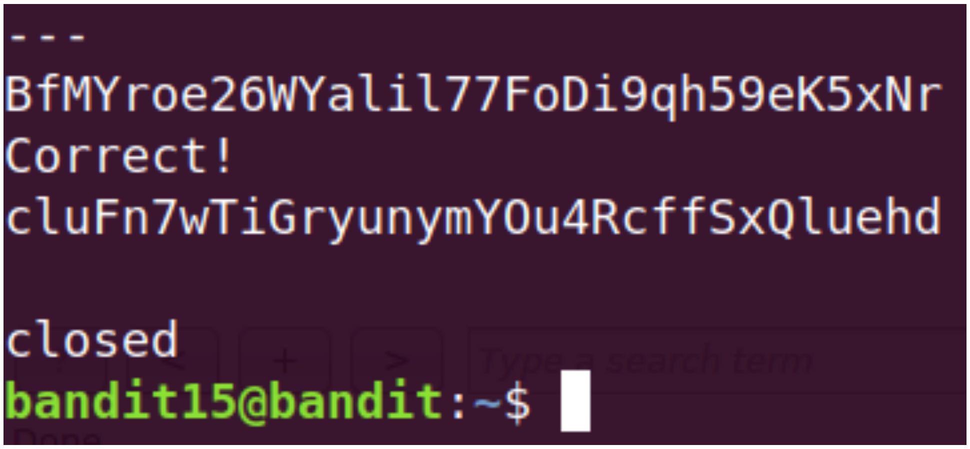
Bandit 15: BfMYroe26WYalil77FoDi9qh59eK5xNr

Bandit15

Connecting and submitting

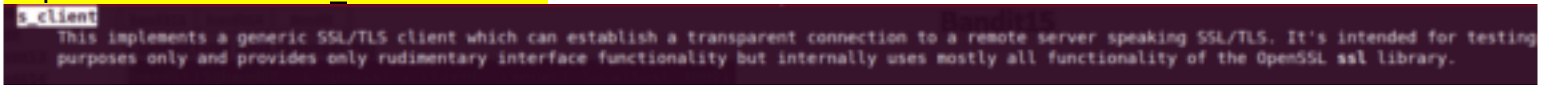


```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
```



```
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit15@bandit:~$ 
```

explanation on the s_client switch



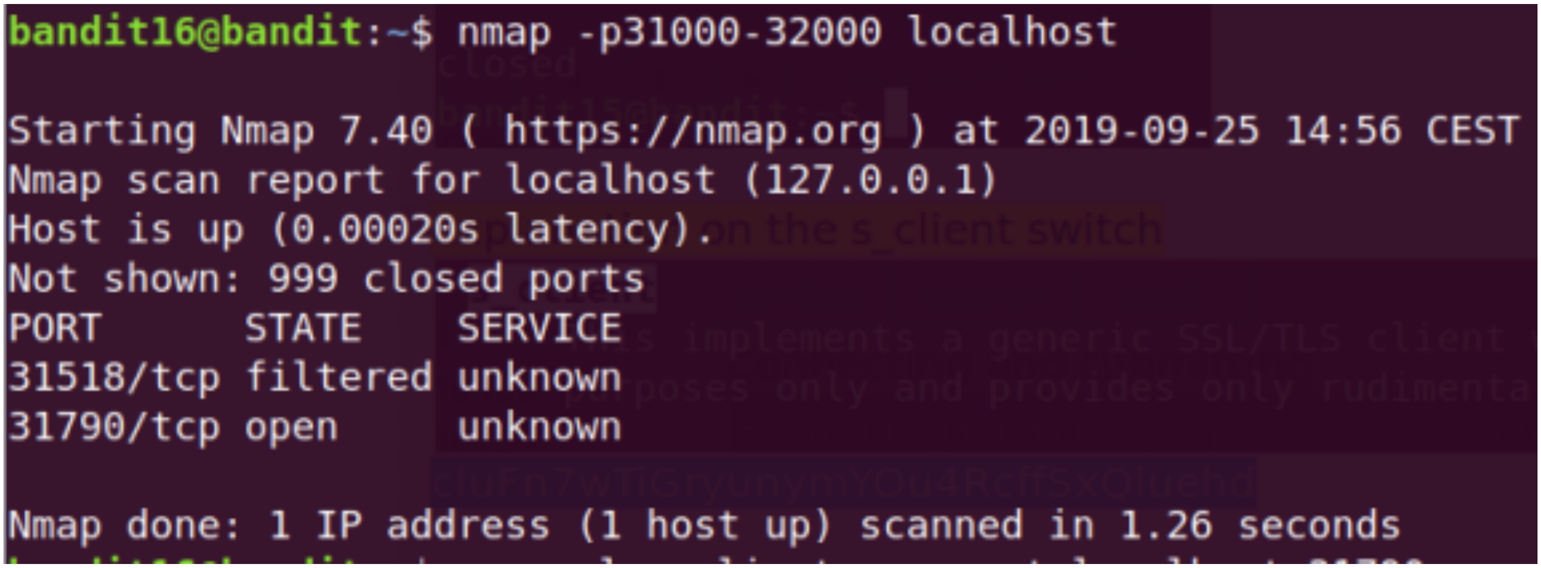
s_client
This implements a generic SSL/TLS client which can establish a transparent connection to a remote server speaking SSL/TLS. It's intended for testing purposes only and provides only rudimentary interface functionality but internally uses mostly all functionality of the OpenSSL ssl library.

cluFn7wTiGryunymYOu4RcffSxQluehd

bandit16

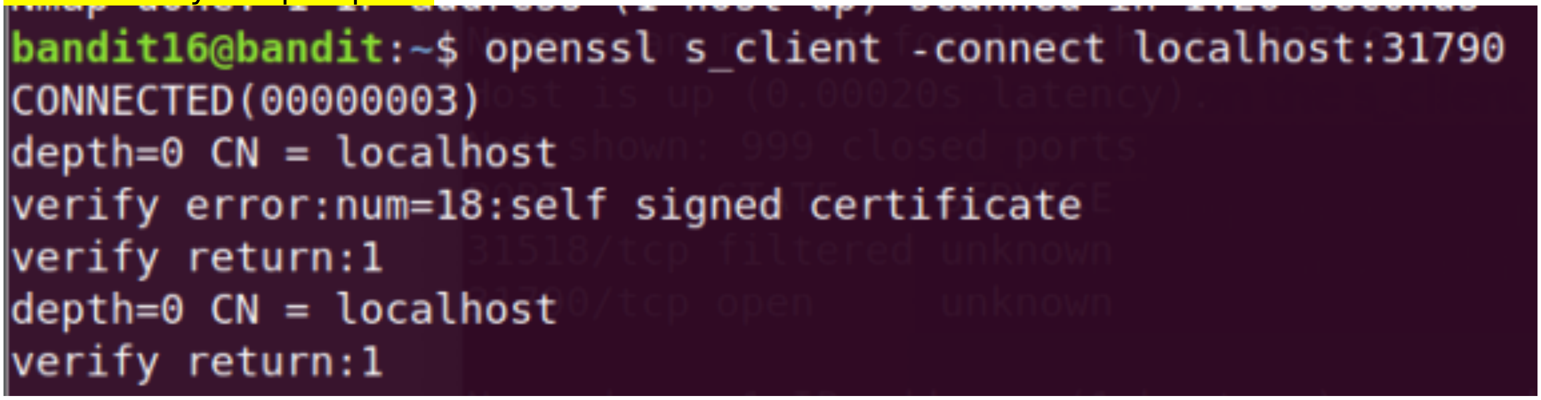
```
PORT SPECIFICATION AND SCAN ORDER:
    -p <port ranges>: Only scan specified ports
      Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
```

nmap from 31000 to 32000



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

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-25 14:56 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00020s latency).
Not shown: 999 closed ports
PORT      STATE    SERVICE
31518/tcp filtered unknown
31790/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

connect only to open ports



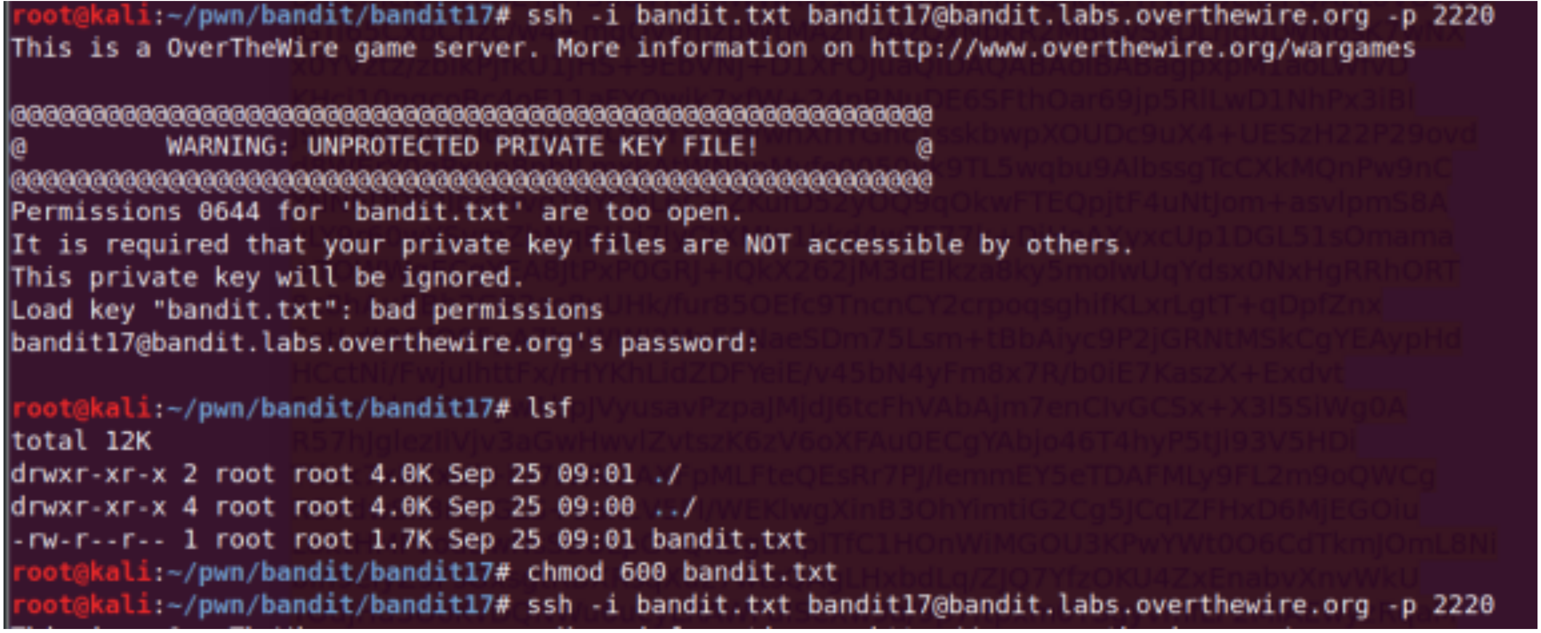
```
bandit16@bandit:~$ openssl s_client -connect localhost:31790
CONNECTED(00000003)
depth=0 CN = localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = localhost
verify return:1
```

-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b

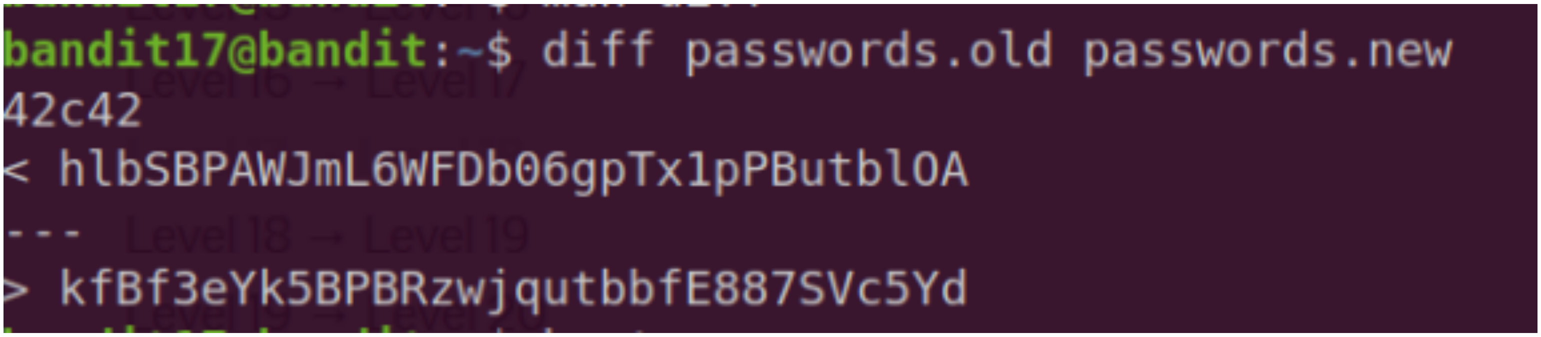
```
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

bandit17

Connecting to bandit 17



```
root@kali:~/pwn/bandit/bandit17# ssh -i bandit.txt bandit17@bandit.labs.overthewire.org -p 2220
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'bandit.txt' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "bandit.txt": bad permissions
bandit17@bandit.labs.overthewire.org's password:

root@kali:~/pwn/bandit/bandit17# lsf
total 12K
drwxr-xr-x 2 root root 4.0K Sep 25 09:01 ./
drwxr-xr-x 4 root root 4.0K Sep 25 09:00 ../
-rw-r--r-- 1 root root 1.7K Sep 25 09:01 bandit.txt
root@kali:~/pwn/bandit/bandit17# chmod 600 bandit.txt
root@kali:~/pwn/bandit/bandit17# ssh -i bandit.txt bandit17@bandit.labs.overthewire.org -p 2220
```

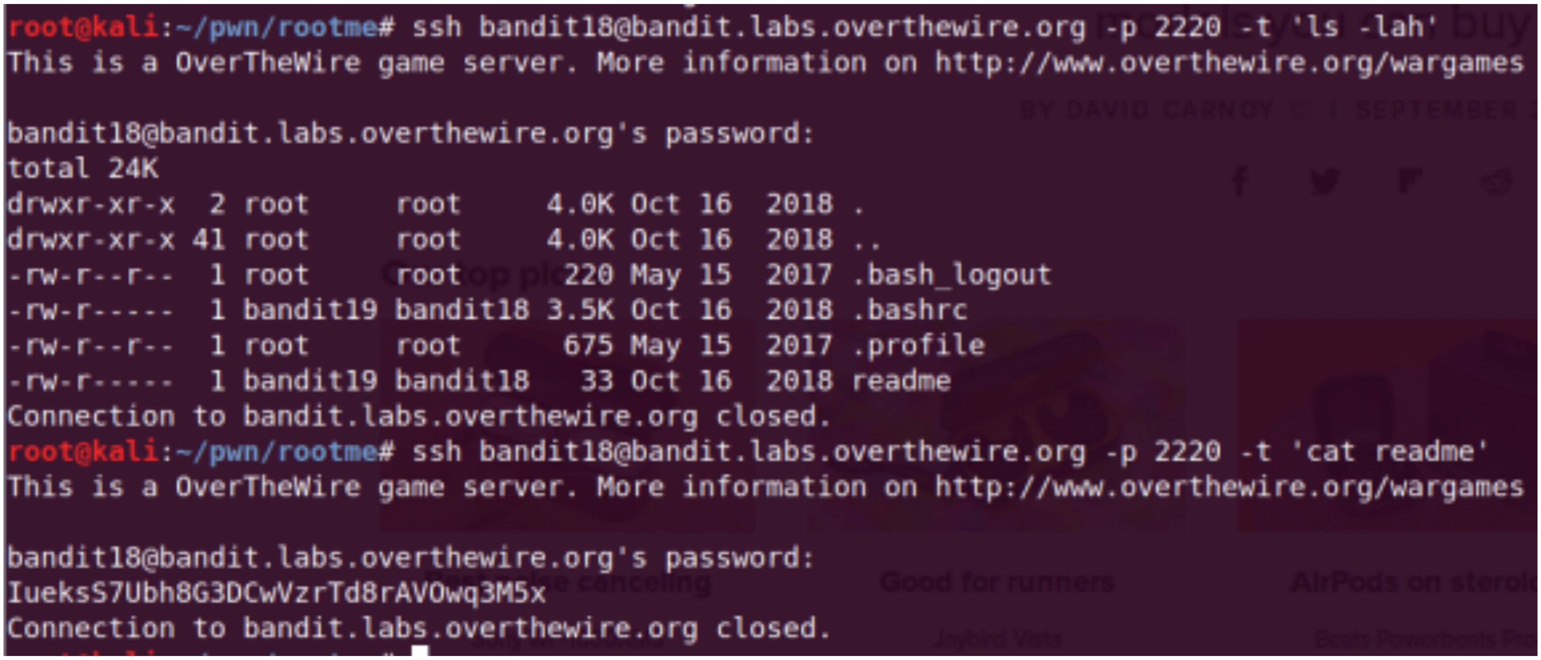


```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< hlbSBPAWJmL6WFDb06gpTx1pPButblOA
---
> kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
```

kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd

bandit18

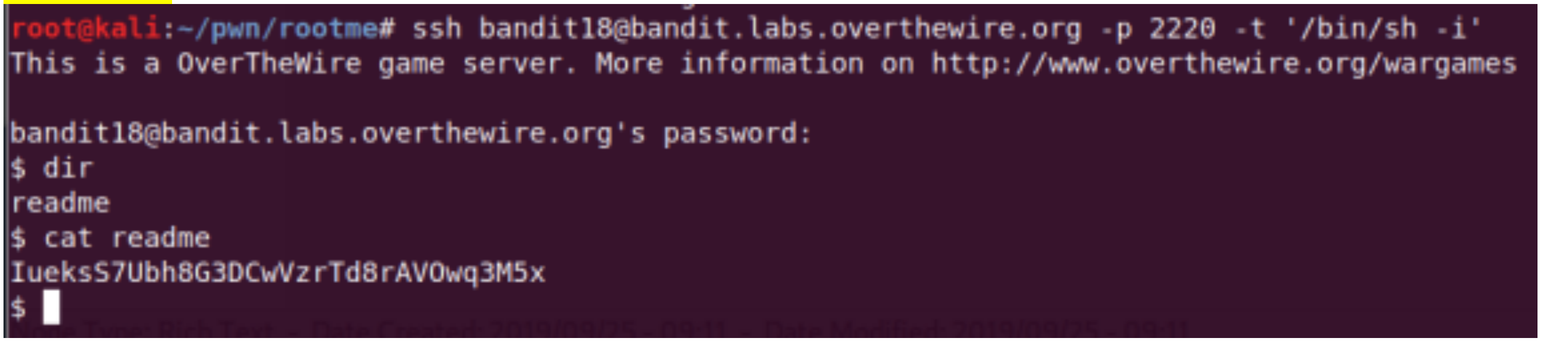
Using ssh for rce



```
root@kali:~/pwn/rootme# ssh bandit18@bandit.labs.overthewire.org -p 2220 -t 'ls -lah'
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
total 24K
drwxr-xr-x  2 root     root     4.0K Oct 16  2018 .
drwxr-xr-x 41 root     root     4.0K Oct 16  2018 ..
-rw-r--r--  1 root     root      220 May 15  2017 .bash_logout
-rw-r-----  1 bandit19 bandit18 3.5K Oct 16  2018 .bashrc
-rw-r--r--  1 root     root      675 May 15  2017 .profile
-rw-r-----  1 bandit19 bandit18   33 Oct 16  2018 readme
Connection to bandit.labs.overthewire.org closed.
root@kali:~/pwn/rootme# ssh bandit18@bandit.labs.overthewire.org -p 2220 -t 'cat readme'
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
Connection to bandit.labs.overthewire.org closed.
```

IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x

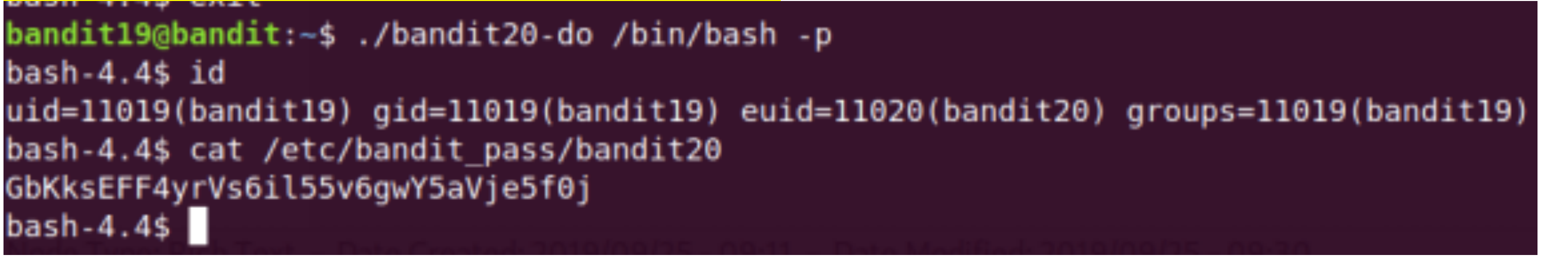
solution 2:



```
root@kali:~/pwn/rootme# ssh bandit18@bandit.labs.overthewire.org -p 2220 -t '/bin/sh -i'
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
$ dir
readme
$ cat readme
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
$ 
```

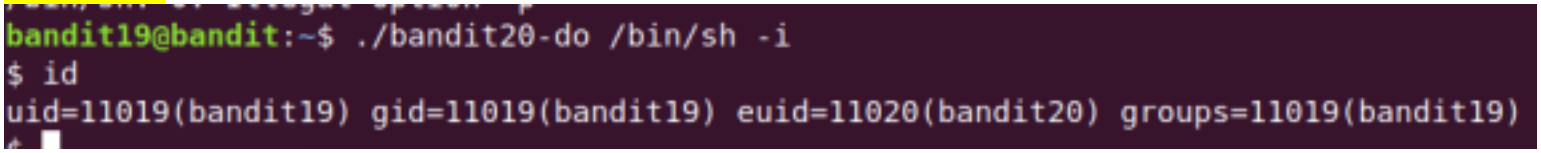
bandit19

Executing bash shell and then reading password



```
bandit19@bandit:~$ ./bandit20-do /bin/bash -p
bash-4.4$ id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
bash-4.4$ cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bash-4.4$ 
```

Solution 2



```
bandit19@bandit:~$ ./bandit20-do /bin/sh -i
$ id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit19)
```

GbKksEFF4yrVs6il55v6gwY5aVje5f0j