


Bandit Level 15 → Level 16

SSH Parameters	
Server:	bandit.labs.overthewire.org
Port:	2220

Website URLs	
Level 15→16	OverTheWire: Level Goal: Bandit Level 15 → Level 16
Level 16→17	OverTheWire: Level Goal: Bandit Level 16 → Level 17

Passwords		
Level	User Name	Password
Level 15→16	bandit15	jN2kgmIXJ6fShzhT2avhotn4Zcka6tn
Level 16→17	bandit16	JQttfApK4SeyHwDII9SXGR50qclOAil1

Wargames updated Information

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

Donate! Help!?

SSH Information
Host: bandit.labs.overthewire.org
Port: 2220

Bandit
Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5
Level 5 → Level 6
Level 6 → Level 7
Level 7 → Level 8
Level 8 → Level 9
Level 9 → Level 10
Level 10 → Level 11
Level 11 → Level 12

Bandit Level 15 → Level 16

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to **port 30001 on localhost** using SSL encryption.

Helpful note: Getting "HEARTBEATING" and "Read R BLOCK"? Use `-ign_eof` and read the "CONNECTED COMMANDS" section in the manpage. Next to 'R' and 'Q', the 'B' command also works in this version of that command...

Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

Helpful Reading Material

Secure Socket Layer/Transport Layer Security on Wikipedia
OpenSSL Cookbook - Testing with OpenSSL

```
bandit15@bandit:~$ sudo -l
bandit15@bandit:~$ #Power the Wire - Bandit - Level 15 --> 16 - Solution Set
bandit15@bandit:~$ #Execution of id and whoami commands to determine Bandit Level and User ID
bandit15@bandit:~$ id && whoami
uid=11015(bandit15) gid=11015(bandit15) groups=11015(bandit15)
bandit15
bandit15@bandit:~$ #Execution of pwd command, to determine current working directory, and ls -la to view contents of this directory, metadata of files [via -l option/switch] and hidden files [which are preceded by a period and displayed via the -a option/switch]
bandit15@bandit:~$ pwd && ls -la
/home/bandit15
total 24
drwxr-xr-x 2 root root 4096 Apr 23 18:04 .
drwxr-xr-x 70 root root 4096 Apr 23 18:05 ..
-rw-r----- 1 bandit15 bandit15 33 Apr 23 18:04 .bandit14.password
-rw-r--r-- 1 root root 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 root root 3771 Jan 6 2022 .bashrc
-rw-r--r-- 1 root root 807 Jan 6 2022 .profile
bandit15@bandit:~$
bandit15@bandit:~$ #Per Bandit Level 15 --> Level 16 instructions the password to Level 16 can be harvested via submittal of the Level 15 password, to localhost port 30001 via Secure Sockets Layer (SSL) encryption. Note: SSL is different than Secure Shell (SSH), utilized at onset to log into each level.
bandit15@bandit:~$ #Connecting to, and sending data via the SSL protocol/encryption, is accomplished through use of the openssl s_client commands, the target computer [localhost] and port [30001] in tandem. OpenSSL is a software library for applications that provide secure communications over computer networks. The s_client command implements a generic SSL/Transport Layer Security (TLS) client which connects to a remote host using SSL/TLS.
bandit15@bandit:~$ #Retrieve the Level 15 password via the cat command
bandit15@bandit:~$ cat /etc/bandit_pass/bandit15
jN2kgmIX36fShzhT2avhtnQZcka6tnt
bandit15@bandit:~$ #Connect to port 30001, on localhost [this computer], over Secure Socket Layer (SSL) protocol/encryption utilizing the openssl s_client command and then copy and paste Level 15 password to harvest Level 16 password
bandit15@bandit:~$ openssl s_client localhost:30001
CONNECTED(00000003)
```

```
00a0 - aa 6a f1 0d 8a 97 bb 0e-de 89 d5 66 5d fe 08 59 .j.....f]..Y
00b0 - ea aa 34 7f d0 f9 1d 81-09 12 b0 99 df 96 cf 42 .4.....8
00c0 - 01 12 99 20 1f fb ad 0f-74 0e 6a 62 b7 ec 5b b1 ...t.jp.[.

Start Time: 1691835970
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
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: CCAAFEB89E5DB888A810E48H991468AD8963A715049282F762E578D2C3ACFF
  Session-ID-ctx:
  Resumption PSK: AE5941068EDE649FBF5A712A4A7195002687347DE6ACFAC7F9EB5D375E2AEB17ADE51D617170B8FB8F94ACC0B4953388
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  TLS session ticket lifetime hint: 7200 (seconds)
  TLS session ticket:
0000 - 95 ee 97 c4 19 c8 b1 09-b7 99 24 84 e8 71 f0 a5 .....$.q..
0010 - 23 a8 d0 c7 ba cf 13 8c-8a 10 fc bc ea 90 14 11 #.....
0020 - c0 3c 57 b1 1a 47 53 09-c0 fa e1 95 e8 2b 08 06 <M..GU.....
0030 - b5 aa 80 f3 5f be a7 d0-7b a6 95 2f e0 6a c8 d0 .....u./j..
0040 - ab 54 a6 65 02 b5 25 73-33 53 b7 be fa a6 64 ea .T.e..ks3S...d.
0050 - b7 a9 7f ec f3 83 0b d6-d3 3d e7 79 22 59 e0 6d .....=y^v.m
0060 - 0c 5b e6 6c 52 3b 53 6d-ba 36 c9 c3 9b 91 95 d7 [.lRjSm.6.....
0070 - dc c3 aa f7 13 c3 78 a0-da 8a 66 31 ef 6d 61 4b .....x..fa.]ak
0080 - 20 e1 1a 5f 19 87 19 35-08 4b 3b 61 be 5d a1 f0 .....5.K[A]..
0090 - 80 fb 6c 7a b1 55 a1 86-e5 38 62 1c 9d 4e 87 b2 ..lZ.U...8b..N..
00a0 - 0c e2 ae 7d 4d 69 0c 7c-11 e3 16 ff e5 89 41 dc ...M]......A.
00b0 - 23 bb a8 71 e2 c3 c5 7b-d4 56 a6 2a 84 0c a5 92 #.q...[.V..T...
00c0 - 1f e6 25 bd 05 08 1c a0-7a 0d 64 94 df 26 66 bc ..N.....z.d.0sf.

Start Time: 1691835974
Timeout : 7200 (sec)
Verify return code: 10 (certificate has expired)
Extended master secret: no
Max Early Data: 0

---
read R BLOCK
jN2kgmIX36fShzhT2avhtnQZcka6tnt
Correct!
JQtTfApK4SeyHwDI9SXGR50qclOAi11
closed
```

Level 16 —> Level 17 Password

JQtTfApK4SeyHwDI9SXGR50qclOAi11