


Bandit Level 20 → Level 21

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

Website URLs	
Level 20→21	OverTheWire: Level Goal: Bandit Level 20 → Level 21
Level 21→22	OverTheWire: Level Goal: Bandit Level 21 → Level 22

Passwords		
Level	User Name	Password
Level 20→21	bandit20	VxCazJaVykl6W36BkBU0mJTCM8rR95XT
Level 21→22	bandit21	NvEJF7oVjkddlTPSrdKEFOllh9V1IBcq

WargamesInformationupdated

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

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

Bandit Level 20 → Level 21

Level Goal

There is a setuid binary in the homedirectory that does the following: it makes a connection to localhost on the port you specify as a commandline argument. It then reads a line of text from the connection and compares it to the password in the previous level (bandit20). If the password is correct, it will transmit the password for the next level (bandit21).

NOTE: Try connecting to your own network daemon to see if it works as you think

Commands you may need to solve this level

ssh, nc, cat, bash, screen, tmux, Unix 'job control' (bg, fg, jobs, &, CTRL-Z, ...)

Donate! Help!?

```
bandit20@bandit:~$ #####
#Over the Wire - Bandit - Level 20 ----> Level 21 - Solution Set
bandit20@bandit:~$ #####
bandit20@bandit:~$ #Execution of id and whoami commands to determine bandit user ID and level
bandit20@bandit:~$ id && whoami
uid=11020(bandit20) gid=11020(bandit20) groups=11020(bandit20)
bandit20
bandit20@bandit:~$ #Execute pwd command to determine present working directory and ls command, with -l option/switch to output file/directory metadata and -a option/switch to output hidden files [which are preceded by a period]
bandit20@bandit:~$ pwd && ls -la
/home/bandit20
total 36
drwxr-xr-x  2 root    root      4096 Apr 23 18:04 .
drwxr-xr-x 70 root    root      4096 Apr 23 18:05 ..
-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
-rwsr-x---  1 bandit21 bandit20 15600 Apr 23 18:04 suconnect
bandit20@bandit:~$
```

```
Open  Untitled Document 1  Save  -  +  X
1 #####
2 #Harvesting the bandit21 password via the suconnect command on port 777
3 #####
4
5 #Per the Bandit Level 20 ----> 21 directions the home directory hosts a setuid binary.
6 #A. This binary makes a connection to localhost, on the port you specify, as a commandline argument.
7 #B. It then reads a line of text from the connection and compares it to the password in the previous level [bandit20]. If the password
   is correct, it will transmit the password for the next level [bandit21].
8
9 #Per the above the setuid binary makes a connection to localhost on a port specified by us. The binary then reads the connection for a
   line of text and assesses if it is the bandit20 password.
10
11 #Since we are to specify the port to the setuid binary we would need to create something for setuid to connect to. Netcat (nc) is a
   command line utility utilized to facilitate data transfer between programs, computers, etc.
12
13 #As such, we create a netcat connection, on port 7777, with the listener [-l] enabled. Then we can call the setuid program, in the home
   directory, and call it with 7777 as an argument.
14
15 #In order to perform the aforementioned we need to have the netcat listener running while we call the setuid/binary file with port 7777.
16
17 #We facilitate this via the screen command. The screen command transforms your screen into a [virtual] spiral bound notebook with a
   table of contents on the first page [command: screen -ls] that gets you to all the other pages you have scribed on [i.e. have commands/
   sessions running on].
18
19 #Before starting the netcat listener we run the screen command. This is the equivalent of opening to a blank page in a notebook. Next, we
   execute the netcat [nc] command, enable the listener [-l] option/switch, on port 7777. Prior to executing this command we call the
   Bandit20 password, though the command [cat /etc/bandit_pass/bandit20] and pipe this to the aforementioned netcat command.
```

```
20
21 #To leave this screen, but still keep it running, invoke the key sequence of cntrl and "a" and then push the "d" key (for detach).
22
23 #We then run the screen command and call the setuid/binary program with the command, ./setuid 7777. This sends the password to the
   aforementioned netcat connection
24
25 #To migrate back to the netcat command, and retrieve the bandit21 password, type screen -ls to list the available screens and then type
   screen and the identifier to access the screen. This takes you to the screen with the bandit21 password.
```

```
bandit20@bandit:~$ #Utilization of the screen command to create a screen to cat the bandit20 password and pipe it to the netcat
listener on port 777
bandit20@bandit:~$
bandit20@bandit:~$ screen
```

```
bandit20@bandit: -
GNU Screen version 4.09.00 (GNU) 30-Jan-22

Copyright (c) 2018-2020 Alexander Naumov, Amadeusz Slawinski
Copyright (c) 2015-2017 Juergen Weigert, Alexander Naumov, Amadeusz Slawinski
Copyright (c) 2010-2014 Juergen Weigert, Sadrul Habib Chowdhury
Copyright (c) 2008-2009 Juergen Weigert, Michael Schroeder, Micah Cowan, Sadrul Habib Chowdhury
Copyright (c) 1993-2007 Juergen Weigert, Michael Schroeder
Copyright (c) 1987 Oliver Laumann

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 3, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied
warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program (see the file COPYING); if not,
see https://www.gnu.org/licenses/, or contact Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA
02111-1301 USA.

Send bugreports, fixes, enhancements, t-shirts, money, beer & pizza to screen-devel@gnu.org

Capabilities:

[Press Space for next page; Return to end.]

```

```
achhabra@pop-os: ~
bandit20@bandit:~$ #Screen 1 - First command to cat the bandit20 password, is piped to the netcat listener listening on port
7777
bandit20@bandit:~$
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost 7777

```

```
bandit20@bandit: -
bandit20@bandit:~$ #Screen 2 - Call the suconnect command on port 7777 to facilitate harvesting the bandit21 password
bandit20@bandit:~$
bandit20@bandit:~$ ./suconnect 7777
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password
bandit20@bandit:~$

```

```
bandit20@bandit:~$ #The screen -ls command outputs the list of screens to reference. The -r switch reattaches the screen fo
r review of the password.

```

```
There are screens on:
 345360.pts-129.bandit (08/14/2023 01:47:05 PM) (Detached)
 342552.pts-129.bandit (08/14/2023 01:43:33 PM) (Detached)
 321792.pts-20.bandit (08/14/2023 01:35:47 PM) (Detached)
 293499.pts-93.bandit (08/14/2023 01:22:43 PM) (Detached)
 247504.pts-93.bandit (08/14/2023 12:53:07 PM) (Detached)
5 Sockets in /run/screen/S-bandit20.
bandit20@bandit:~$
bandit20@bandit:~$ screen -r 342552.pts-129.bandit

```

```
bandit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost 7777
NvEJF7oVjkdltPSrdKEF0llh9V1IBcq
bandit20@bandit:~$
bandit20@bandit:~$ #The bandit21 password is on the line above

```

Level 21 —> Level 22 Password

NvEJF7oVjkddltPSrdKEFOllh9V1lBcq