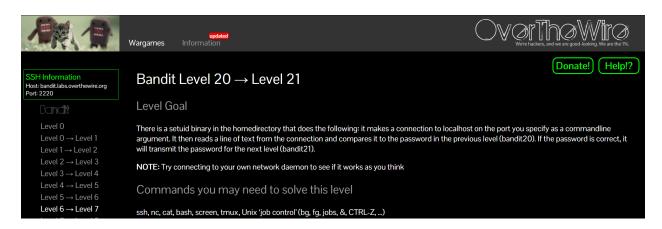
Bandit Level 20 -> Level 21

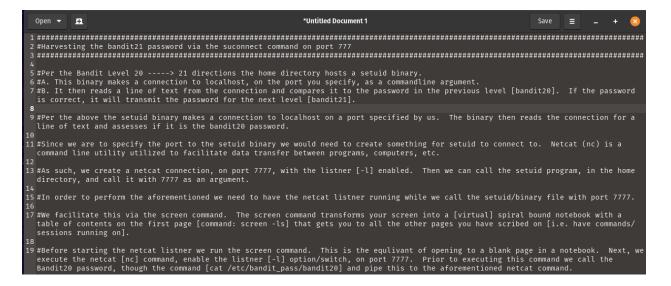
SSH Parameters			
Server:	bandit.labs.overthewire.org		
Port:	2220		

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		



```
abandit:~$
       bandit:~$ #Execution of id and whoami commands to determine bandit user ID and level
uid=11020(bandit20) gid=11020(bandit20) groups=11020(bandit20)
bandit20
          lit:~$ #Execute pwd command to determine present working directory and ls command, with -l option/switch to outp
ut file/directory metadata and -a option/switch to output hidden files [which are preceeded by a period]
       bandit:~$
bandit:~$ pwd && ls -la
/home/bandit20
total 36
         2 root
                          4096 Apr 23 18:04
                          220 Jan 6 2022 .bash_logout
3771 Jan 6 2022 .bashrc
807 Jan 6 2022 .profile
-rw-r--r-- 1 root
-rw-r--r-- 1 root
                  root
-rw-r--r-- 1 root
                  root
  dit20@bandit:~$
```



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: ~
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: ~
                                                                                                                                             Q ≣
   andit20@bandit:~$ #Screen 1 - First command to cat the bandit20 password, is piped to the netcat listener listening on port
  andit20@bandit:~$
andit20@bandit:~$ cat /etc/bandit_pass/bandit20 | nc -l localhost 7777
                                                                            bandit20@bandit: ~
  ndit20@bandit:~$ #Screen 2 - Call the suconnect command on port 7777 to facilitate harvesting the bandit21 password
 andit20@bandit:~$
andit20@bandit:~$ ./suconnect 7777
Read: VxCazJaVykI6W36BkBU0mJTCM8rR95XT
Password matches, sending next password bandit20mbandit:~$ [
                 _{
m it:}-^{*} #The screen -ls command outputs the list of screens to reference. The -r switch reattaches the screen fo
  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.
 pandit20@bandit:~$
pandit20@bandit:~$ screen -r 342552.pts-129.bandit [
bandit20@bandit:-$ cat /etc/bandit_pass/bandit20 | nc -l localhost 7777
NVEJF7oVjkddltPSrdKEFOllh9V1IBcq
     lit20@bandit:~$ #The bandit21 password is on the line above
```

Level 21 —> Level 22 Password

NvEJF7oVjkddltPSrdKEFOllh9V1IBcq