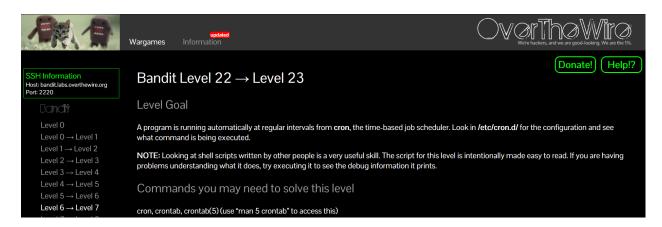
Bandit Level 22 -> Level 23

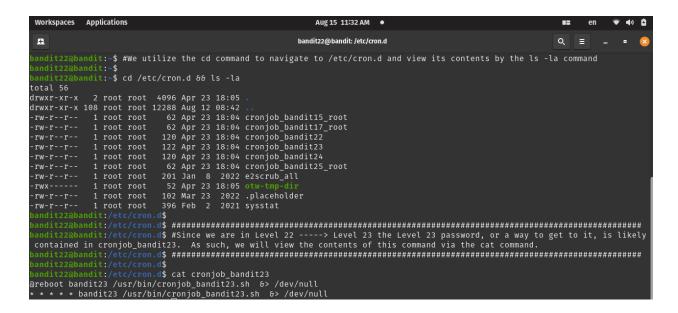
SSH Parameters			
Server:	bandit.labs.overthewire.org		
Port:	2220		

Website URLs				
Level 22—>23	OverTheWire: Level Goal: Bandit Level 22 → Level 23			
Level 23—>24	OverTheWire: Level Goal: Bandit Level 23 → Level 24			

Passwords				
Level	User Name	Password		
Level 22—>23	bandit22	WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff		
Level 23—>24	bandit23	QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G		



27 #Per the Bandit Level 22 ----> 23 instructions a program is running automatically at regular intervals via cron. Cron is a time-based 28 job scheduler. The /etc/cron.d directory contains the configuration/program that executes. As such, we displayed the contents of this directory via the ls -la command. The - option/switch provides meta-data of the files/folders and the -a option/switch outputs hidden files [whose file names are preceded with a period (.)]



Per examination of the above program it utilizes an environment variable, whoami [in our case this would be bandit22 per our examination of this command above] and inserts this into a string, "I am user bandit22". The output of this string is then piped to the md5sum command which is then piped to the cut command. The cut command then delineates this string, on a space, and extracts the first field as the password and passes it to a variable titled mytarget.

The script then outputs a statement that it is copying the password file, from /etc/bandit_pass/bandit22 to tmp/\$mytarget.

To restate, this program fetches the password from /etc/bandit_pass/bandit22 and copies it to a file (with the name of the mytarget variable) that is contained within the /tmp directory.

The command to carry out the aforementioned, cat /etc/bandit_pass/bandit22 > /tmp/\$mytarget

```
bandit22abandit:/usr/bin$ #We execute the cronjob_bandit23.sh program to examine its output.
bandit22abandit:/usr/bin$ #Command: ./cronjob_bandit23.sh
bandit22abandit:/usr/bin$ //cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddbb4412f91573b38db3
bandit22abandit:/usr/bin$ #To view the output we cat the output file at /tmp/8169b67bd894ddbb4412f91573b38db3
bandit22abandit:/usr/bin$ #To view the output we cat the output file at /tmp/8169b67bd894ddbb4412f91573b38db3
bandit22abandit:/usr/bin$ cat /tmp/8169b67bd894ddbb4412f91573b38db3
WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff
bandit22abandit:/usr/bin$ #The output above appears to bethe password for banit22. We verify this by reading /etc/bandit_pass/bandit22
bandit22abandit:/usr/bin$ #The output above appears to bethe password for banit22. We verify this by reading /etc/bandit_pass/bandit22
bandit22abandit:/usr/bin$ bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin$
bandit22abandit:/usr/bin
```

bandit22@bandit:/usr/bin\$ #As such, when this statement executes it does so as follows, and outputs the bandit22 password, bandit22@bandit:/usr/bin\$ #Command: cat /etc/bandit_pass/bandit22

SPer examination of the cronjob_bandit23.sh program a file is created, specifically titled with the value of the mytarget variable, to deposit the password. We are going to assume this program was previously executed. As such, the bandit23 password (extracted from /etc/bandit_pass/23) was deposited to the file with the value of the mytarget variable. To determine the value of the mytarget value, and the file name containing the password, we will copy the cronjob_bandit23.sh file to the /tmp folder as Password_24.sh. We will then edit this file, via the nano text editor and replace the myname variable, which the script assigns the whomai enviorment variable to, with bandit23. This will enable us to get the name of the file containing the password and harvest it.

```
bandit22@bandit:/usr/bin$ #Command to copy cronjob_bandit23.sh to the /tmp directory
bandit22@bandit:/usr/bin$
bandit22@bandit:/usr/bin$ cp -v cronjob_bandit23.sh /tmp/cronjob_bandit23.sh
'cronjob_bandit23.sh' -> '/tmp/cronjob_bandit23.sh'
bandit22@bandit:/usr/bin$ []
```

```
bandit22@bandit:/usr/bin$ #Navigate to the /tmp directory
bandit22@bandit:/usr/bin$
bandit22@bandit:/usr/bin$ cd /tmp
bandit22@bandit:/tmp$
bandit22@bandit:/tmp$ pwd
/tmp
bandit22@bandit:/tmp$ [
```

```
bandit22abandit:/tmp$ #Utilizing the nano text editor opent he cronjob_bandit23.sh file to make the above mofifications
bandit22abandit:/tmp$
bandit22abandit:/tmp$ nano cronjob_bandit23.sh[]
```

```
GNU nano 6.2

#!/bin/bash

#Comment out the myname variable and recreate it assining it to bandit23

#myname=$(whoani)

myname=$(whoani)

mytarget=$(echo I am user {myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/!myname > /tmp/!mytarget

Save modified buffer?

Y Yes
N No ^C Cancel
```

```
bandit22@bandit:/tmp$ #Per the output, of the cronjob_bandit23.sh file, above the password is in:
bandit22@bandit:/tmp$ # /tmp/8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/tmp$ #Note: The permissions denied error is due to not being logged into bandit23 and trying to access /etc/b
andit_pass/bandit23
```

```
bandit22@bandit:/tmp$ #Per the output, of the cronjob_bandit23.sh file, above the password is in:
bandit22@bandit:/tmp$ # /tmp/8ca319486bfbbc3663ea0fbe81326349
bandit22@bandit:/tmp$ #Note: The permissions denied error is due to not being logged into bandit23 and trying to access /etc/b
andit_pass/bandit23
```

```
bandit22@bandit:/tmp$ #Reading the bandit23 password:
bandit22@bandit:/tmp$
bandit22@bandit:/tmp$ cat /tmp/8ca319486bfbbc3663ea0fbe81326349
QYw0Y2a1A672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:/tmp$
```

```
bandit23@bandit:~$ #Login with password for bandit 23 was successful per user ID and output of id and whoami commands below bandit23@bandit:~$
bandit23@bandit:~$ id && whoami
uid=11023(bandit23) gid=11023(bandit23) groups=11023(bandit23)
bandit23
bandit23
bandit23@bandit:~$ [
```

Level 23 —> Level 24 Password

QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G