


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



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

Bandit Level 22 → Level 23

Level Goal

A program is running automatically at regular intervals from **cron**, the time-based job scheduler. Look in **/etc/cron.d/** for the configuration and see what command is being executed.

NOTE: Looking at shell scripts written by other people is a very useful skill. The script for this level is intentionally made easy to read. If you are having problems understanding what it does, try executing it to see the debug information it prints.

Commands you may need to solve this level

`cron, crontab, crontab(5)` (use "man 5 crontab" to access this)

```

bandit22@bandit:~$ #####
bandit22@bandit:~$ #Over the Wire - Bandit Level 22 ----> Level 23 - Solution Set
bandit22@bandit:~$ #####
bandit22@bandit:~$ #####
bandit22@bandit:~$ #Execution of id and whoami commands to determine Bandit Level and User ID
bandit22@bandit:~$ #####
bandit22@bandit:~$ id && whoami
uid=11022(bandit22) gid=11022(bandit22) groups=11022(bandit22)
bandit22
bandit22@bandit:~$ #####
bandit22@bandit:~$ #Execution of pwd command, to list current working directory, and ls -la command to list directory contents
, metadata [via -l option/switch] and hidden files [with file names which start with period and are output via the -a option/s
witch]
bandit22@bandit:~$ #####
bandit22@bandit:~$ pwd && ls -la
/home/bandit22
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
bandit22@bandit:~$ █

```

```

bandit22@bandit:~$ #####
bandit22@bandit:~$ #To view a users cron jobs we utilize the crontab -l command. The -l option/switch invokes output of a cron
jobs list
bandit22@bandit:~$ #####
bandit22@bandit:~$ crontab -l
crontabs/bandit22/: fopen: Permission denied
bandit22@bandit:~$ #Based on the aforementioned we do not have applicable permissions to open this file
bandit22@bandit:~$ █

```

```

26
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 -l 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 (.)]

```

```

Workspaces Applications Aug 15 11:32 AM
bandit22@bandit: /etc/cron.d
bandit22@bandit:~$ #We utilize the cd command to navigate to /etc/cron.d and view its contents by the ls -la command
bandit22@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
bandit22@bandit:/etc/cron.d$
bandit22@bandit:/etc/cron.d$ #####
bandit22@bandit:/etc/cron.d$ #Since we are in Level 22 ----> Level 23 the Level 23 password, or a way to get to it, is likely
contained in cronjob_bandit23. As such, we will view the contents of this command via the cat command.
bandit22@bandit:/etc/cron.d$ #####
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null

```

```
bandit22@bandit:/etc/cron.d$ #####
bandit22@bandit:/etc/cron.d$ #Based on inspection of the cronjob_bandit23 file we note that a shell script, at /usr/bin/cronjob_
bandit23.sh is executed when bandit23 logs in. As such, we will navigate to directory /usr/bin via the cd command and read
cronjob_bandit23.sh with the cat command.
bandit22@bandit:/etc/cron.d$ #####
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(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
bandit22@bandit:/etc/cron.d$ █
```

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

```
bandit22@bandit:/usr/bin$ #We execute the cronjob_bandit23.sh program to examine its output.
bandit22@bandit:/usr/bin$ #Command: ./cronjob_bandit23.sh
bandit22@bandit:/usr/bin$ ./cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddb4412f91573b38db3
bandit22@bandit:/usr/bin$ #To view the output we cat the output file at /tmp/8169b67bd894ddb4412f91573b38db3
bandit22@bandit:/usr/bin$ cat /tmp/8169b67bd894ddb4412f91573b38db3
WdDozAdTM2z9DiFEQ2mGLwngMfj4EZff
bandit22@bandit:/usr/bin$ #The output above appears to be the password for bandit22. We verify this by reading /etc/bandit_pass
bandit22@bandit:/usr/bin$ cat /etc/bandit_pass/bandit22
WdDozAdTM2z9DiFEQ2mGLwngMfj4EZff
bandit22@bandit:/usr/bin$ #Based on the aforementioned we note that the output of cronjob_bandit23.sh is identical to the pass
word of bandit22 [Level 22]. The reason for this is the cronjob_bandit23.sh file contains a variable titled myname. My name
is assigned the environment variable of whoami which is utilized in the password extract statement of:
bandit22@bandit:/usr/bin$ #Command: cat /etc/bandit_pass/$myname
bandit22@bandit:/usr/bin$ █
```

```
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
WdDozAdTM2z9DiFEQ2mGLwngMfj4EZff
bandit22@bandit:/usr/bin$ █
```

55 Per 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 whoami environment 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$ 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$ cd /tmp
bandit22@bandit:/tmp$ pwd
/tmp
bandit22@bandit:/tmp$ █
```

```
bandit22@bandit:/tmp$ #Utilizing the nano text editor opent he cronjob_bandit23.sh file to make the above mofifications
bandit22@bandit:/tmp$
bandit22@bandit:/tmp$ nano cronjob_bandit23.sh
```

```
GNU nano 6.2 cronjob_bandit23.sh *
#!/bin/bash

#Comment out the myname variable and recreate it assining it to bandit23
#myname=$(whoami)
myname="bandit23"
mytarget=$(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
```

^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

```
GNU nano 6.2 cronjob_bandit23.sh *
#!/bin/bash

#Comment out the myname variable and recreate it assining it to bandit23
#myname=$(whoami)
myname="bandit23"
mytarget=$(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/8ca319486bfbbc3663ea0f8e81326349
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/8ca319486bfbbc3663ea0f8e81326349
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
QYW0Y2aiA672PsMmh9puTQuhoz8SyR2G
bandit22@bandit:/tmp$
```

```
achhabra@pop-os:~$ #Checking to see that the password which was harvest succesfully logs into bandit23
achhabra@pop-os:~$ 
achhabra@pop-os:~$ ssh bandit23@bandit.labs.overthewire.org -p 2220
```

OXFORD
UNIVERSITY PRESS

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

```
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@bandit:~$
```

Level 23 —> Level 24 Password

QYw0Y2aiA672PsMmh9puTQuhoz8SyR2G