


Bandit Level 21 → Level 22

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

Website URLs	
Level 21→22	OverTheWire: Level Goal: Bandit Level 21 → Level 22
Level 22→23	OverTheWire: Level Goal: Bandit Level 22 → Level 23

Passwords		
Level	User Name	Password
Level 21→22	bandit21	NvEJF7oVjkddltPSrdKEFOllh9V1IBcq
Level 22→23	bandit22	WdDozAdTM2z9DiFEQ2mGlwngMfj4EZff



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 21 → Level 22

Bandit

Level 0
Level 0 → Level 1
Level 1 → Level 2
Level 2 → Level 3
Level 3 → Level 4
Level 4 → Level 5

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.

Commands you may need to solve this level

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

```
bandit21@bandit:~$ #####
#
bandit21@bandit:~$ #Over the Wire - Bandit - Level 21 ----> Level 22 Solution Set
bandit21@bandit:~$ #####
#
bandit21@bandit:~$
bandit21@bandit:~$ #id and whomei command to determine bandit level and bandit user ID
bandit21@bandit:~$
bandit21@bandit:~$ id && whoami
uid=11021(bandit21) gid=11021(bandit21) groups=11021(bandit21)
bandit21
bandit21@bandit:~$
```

```
bandit21@bandit:~$ #####
bandit21@bandit:~$ #Determine current working directory, via pwd command, and contents of this directory via the ls -la command. The -l option/switch outputs metadata of the files/directories. The -a option/switch outputs hidden files/directories which are denoted by a period [.] at the beginning of a file or directory.
bandit21@bandit:~$ #####
bandit21@bandit:~$ #
bandit21@bandit:~$ pwd && ls -la
/home/bandit21
total 24
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
-r-----  1 bandit21 bandit21  33 Apr 23 18:04 .prevpass
-rw-r--r--  1 root    root     807 Jan  6 2022 .profile
bandit21@bandit:~$
```

```
bandit21@bandit:~$ #####
##[A] Per Level 21 ----> Level 22 instructions, a program is running automatically at regular intervals from cron. Cron is a time-based job scheduler.
bandit21@bandit:~$ #[B] Configuration/commands being executed are located at /etc/cron.d
bandit21@bandit:~$ #####
##
bandit21@bandit:~$
bandit21@bandit:~$
bandit21@bandit:~$ #To view contents of the /etc/cron.d directory we utilize the ls -la command to view directory contents including hidden files [files whose name is preceded with a period [.]] and is displayed when the -a option/switch is invoked] and file metadata [output via the -l option/switch]
```

```
1 #####
2 #The cron utility is utilized to schedule jobs/tasks to automatically execute in the future. In example, if you wanted to schedule a file transfer to execute monthly on the 1st of the month or a backup script to run daily at 2AM, you could schedule those through cron.
3
4 #The command, crontab -l, lists the cron jobs for the current user. As such, we execute this command to view the cron jobs for Bandit Level 21.
5
6 #The /etc/cron.d/ directory is the repository where the actual commands are placed/stored. As such, we leverage the cat command to view the contents of this directory.
7 #####
8
```

```
bandit21@bandit:~$ #####
bandit21@bandit:~$ #Command: crontab -l
bandit21@bandit:~$ crontab -l
crontabs/bandit21/: fopen: Permission denied
bandit21@bandit:~$
bandit21@bandit:~$ #Per the message above we do not have permissions to view crontab/cron jobs
bandit21@bandit:~$ #####
bandit21@bandit:~$ #Command: ls -la /etc/cron.d
bandit21@bandit:~$ #Command to view contents of /etc/cron.d - repository of cron jobs
bandit21@bandit:~$
bandit21@bandit:~$ ls -la /etc/cron.d
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
bandit21@bandit:~$
```

```
bandit21@bandit: /etc/cron.d
bandit21@bandit:~$
bandit21@bandit:~$ #####
bandit21@bandit:~$ #We navigate to the /etc/cron.d directory via the cd command [cd /etc/cron.d] and utilize ls -la to view
bandit21@bandit:~$ #####
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$
bandit21@bandit:/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
bandit21@bandit:/etc/cron.d$
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
```

```
bandit21@bandit: /usr/bin
bandit21@bandit:/etc/cron.d$ #####
bandit21@bandit:/etc/cron.d$ #Per examination of the cronjob_bandit22 file we noted the shell file at /usr/bin/cronjob_bandi
t22 is executed when bandit22 logs in/reboots. As such, we will examine this file [/usr/bin/cronjob_bandit22.sh].
bandit21@bandit:/etc/cron.d$ #####
bandit21@bandit:/etc/cron.d$ #Utilize cd command to change directory to /usr/bin
bandit21@bandit:/etc/cron.d$ cd /usr/bin
bandit21@bandit:/usr/bin$
bandit21@bandit:/usr/bin$ #Utilize cat command to view cronjob_bandit22.sh
bandit21@bandit:/usr/bin$ cat cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv
bandit21@bandit:/usr/bin$
```

```
bandit21@bandit:/usr/bin$ #####
bandit21@bandit:/usr/bin$ #Per examination of the cronjob_bandit22.sh file, above, we note when bandit22 logs in and the fil
e executes the chmod command is invoked to give 644 privileges to /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv. Next the file, con
taining the bandit password, /etc/bandit_pass/bandit22, is read via cat. Its contents, through redirection, are written to
/tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv. Since we are logged in as bandit21, we will assume bandit22 has logged in previous u
s, and examine the contents of /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv with the cat command for the bandit22 password.
bandit21@bandit:/usr/bin$ #####
bandit21@bandit:/usr/bin$ cat /tmp/t706lds9S0RqQh9aMcZ6ShpAoZKF7fgv
WdDozAdTM2z9DiFEQ2mGlWngMfj4EZff
bandit21@bandit:/usr/bin$
bandit21@bandit:/usr/bin$ #The cat command above output the bash22 password.
```

Level 22 → Level 23 Password

WdDozAdTM2z9DiFEQ2mGlWngMfj4EZff