

1회차 - 20. 케로로

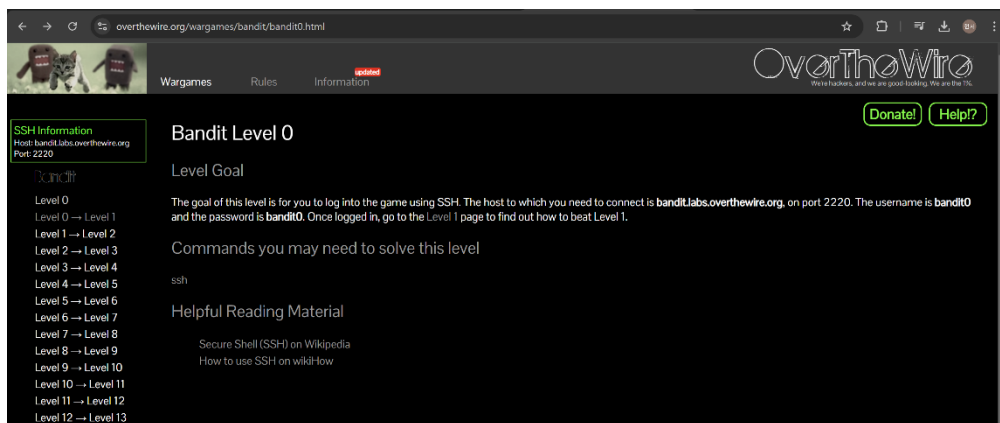
Bandit 레벨 0 ~ 5 라이트업

정보보호학부 2024111262

들어가며

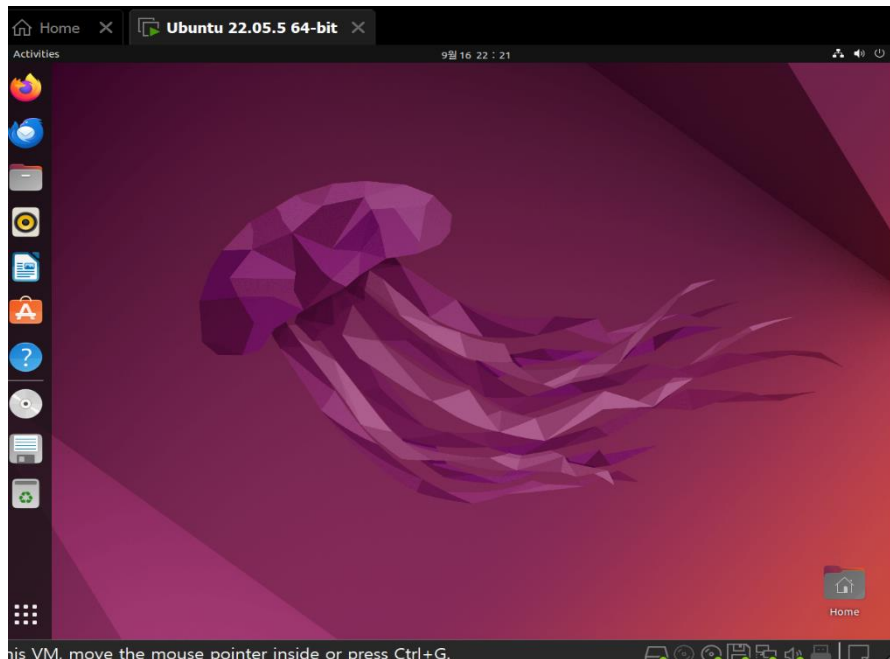
“Bandit” 은 “OverTheWire”라는 온라인 플랫폼에서 제공하는 워게임 중 하나로, 주로 리눅스와 보안 관련 기술을 학습하기 위한 워게임이다. 리눅스는 OS이기 때문에, 단순 이론을 위주로 하는 학습보다는 실습 위주의 학습을 통해, 이를 능숙하게 다루는 것이 중요하다는 생각이 들어서 워게임을 스터디에서 진행하고자 한다. 이를 통해, 기본적인 리눅스 명령어 사용법, 파일 시스템 구조, 권한 관리 등을 익히고자 한다.

Lv. 0



“OverTheWire” 사이트에 Bandit 레벨 0 페이지에 들어가보니, “SSH”를 사용하여 게임에 로그인하는 것이 레벨 0의 문제인 것으로 보인다. 접속해야 하는 호스트는 “bandit.labs.overthewire.org”이며, 포트 번호는 2220인 것 같다. 사용자명은 “bandit0”이고, 비밀번호 또한 “bandit0”라고 말하고 있다. “SSH”가 무엇인지 찾아보니, Secure Shell의 약자로서, 네트워크 상의 다른 컴퓨터에 로그인하여 명령을 실행하고, 정보를 보고 받을

수 있도록 해 주는 통신 프로토콜이라고 한다. 해당 프로토콜은 리눅스를 처음 설치하였을 때, 자동으로 설치되어 있지 않기 때문에, 따로 설치해주어야 한다고 한다. 리눅스 강의에서는 칼리 리눅스를 사용하지만, 강의에서 사용하는 리눅스와 위게임을 할 때 활용할 리눅스를 구분하고 싶어서, 우분투 리눅스를 활용하여 진행하도록 하겠다.



다음은, 해당 리눅스에 SSH부터 설치해보도록 하겠다.

```
ubuntu@ubuntu-virtual-machine:~$ sudo apt update
[sudo] password for ubuntu:
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://kr.archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://kr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://kr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
ubuntu@ubuntu-virtual-machine:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard nonkeysphere ssh-keypass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 2 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.10 [38.9 kB]
Get:2 http://kr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.10 [435 kB]
Get:3 http://kr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 6.3-2ubuntu0.1 [267 kB]
Get:4 http://kr.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10.1 kB]
Fetched 751 kB in 3s (235 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 163752 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1:8.9p1-3ubuntu0.10_amd64.deb ...
Unpacking openssh-sftp-server (1:8.9p1-3ubuntu0.10) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1:8.9p1-3ubuntu0.10_amd64.deb ...
```

우선, SSH를 설치하기 전 터미널에 "sudo apt update" 라는 명령어로 저장소를 업데이트 해준다. 이를 통해, 설치 전에 시스템의 패키지 목록을 최신 상태로 업데이트해준다. 이 목록에는 각 패키지의 최신 버전 정보와 다운로드할 수 있는 위치가 포함되어 있다

고 한다.

그 후, "sudo apt install openssh-server" 라는 명령어를 통해, SSH를 설치한다.

```
ubuntu@ubuntu-virtual-machine:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-09-16 22:23:58 KST; 8min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 3548 (sshd)
      Tasks: 1 (limit: 4551)
     Memory: 1.7M
        CPU: 46ms
   CGroup: /system.slice/ssh.service
           └─3548 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

9월 16 22:23:58 ubuntu-virtual-machine systemd[1]: Starting OpenBSD Secure Shell server...
9월 16 22:23:58 ubuntu-virtual-machine sshd[3548]: Server listening on 0.0.0.0 port 22.
9월 16 22:23:58 ubuntu-virtual-machine sshd[3548]: Server listening on :: port 22.
9월 16 22:23:58 ubuntu-virtual-machine systemd[1]: Started OpenBSD Secure Shell server.
ubuntu@ubuntu-virtual-machine:~$
```

```
ubuntu@ubuntu-virtual-machine:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
ubuntu@ubuntu-virtual-machine:~$
```

그 후, "sudo systemctl status ssh" 명령어를 통해, SSH 서비스가 제대로 실행되는지 확인하여, 설치가 제대로 되었는지 확인한다. 현재 화면에는 잘 설치된 것으로 보인다. 시스템에서 방화벽을 사용하도록 설정한 경우에는, SSH가 포트 연결이 되지 않을 수도 있다. 따라서, "sudo ufw allow ssh" 명령어를 통해 포트를 열게 하였다.

```
ubuntu@ubuntu-virtual-machine:~$ ssh bandit0@bandit.labs.overthewire.org -p2220
The authenticity of host '[bandit.labs.overthewire.org]:2220 ([13.50.165.192]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2lhUBV7lhnV1wUXRb4RrEclFXC5CXlhmAAM/urerLY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: yes
```

Bandit에 접속하기 위해, 'ssh username@IP_address -p[포트번호]' 명령어를 활용해야 한다. 맨 처음 OverTheWire 페이지에서 봤던 정보들을 가지고, "ssh bandit0@bandit.labs.overthewire.org -p2220" 명령어를 작성하여 입력하였다.

```
bandit0

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

bandit@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit@bandit.labs.overthewire.org's password:

04M
www.OverTheWire.org

Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* peda (https://github.com/longld/peda.git) in /opt/peda/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit0@bandit:--$
```

그 후, 비밀번호까지 입력해주자, 무사히 bandit으로 연결되었다.

Lv.0 해결

Lv. 0 → 1

[Wargames](#)[Rules](#)[Information](#)

updated

OVERTHEWIRE

We're hackers, and we are good-looking. We are the 1%.

[Donate!](#)[Help!?](#)

Bandit Level 0 → Level 1

Level Goal

The password for the next level is stored in a file called **readme** located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

Commands you may need to solve this level

ls, cd, cat, file, du, find

TIP: Create a file for notes and passwords on your local machine!

Passwords for levels are *not* saved automatically. If you do not save them yourself, you will need to start over from bandit0.

Passwords also occasionally change. It is recommended to take notes on how to solve each challenge. As levels get more challenging, detailed notes are useful to return to where you left off, reference for later problems, or help others after you've completed the challenge.

“OverTheWire” 사이트를 확인해보니, 다음 레벨의 비밀번호는 홈 디렉토리에 있는 ‘readme’라는 파일에 저장되어 있다고 한다. 이 비밀번호를 사용하여 SSH를 통해 bandit1에 로그인하면 되는 것 같다. 또한, 레벨의 비밀번호를 찾을 때마다 포트 2220번에서 SSH를 사용하여 해당 레벨에 로그인하고 워게임을 진행하라고 한다.

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

Bandit0 계정의 홈 디렉토리에 존재하는 파일을 화면에 나열해주는 명령어 “ls”를 통해, readme 파일 하나가 존재하는 것을 확인할 수 있다. 그 후, 파일의 내용을 간단히 출력해주는 명령어 “cat”을 사용하여, readme 파일의 내용을 확인할 수 있었다. 다음 레벨로 넘어가는 비밀번호는 “ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If” 이다!

```
bandit0@bandit:~$ logout
Connection to bandit.labs.overthewire.org closed.
ubuntu@ubuntu-virtual-machine:~$ ssh bandit1@bandit.labs.overthewire.org -p2220

[O] [V] [E] [R] [T] [H] [E] [W] [I] [R] [E]

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

bandit1@bandit.labs.overthewire.org's password:

[O] [V] [E] [R] [T] [H] [E] [W] [I] [R] [E]

www. ver he ire.org

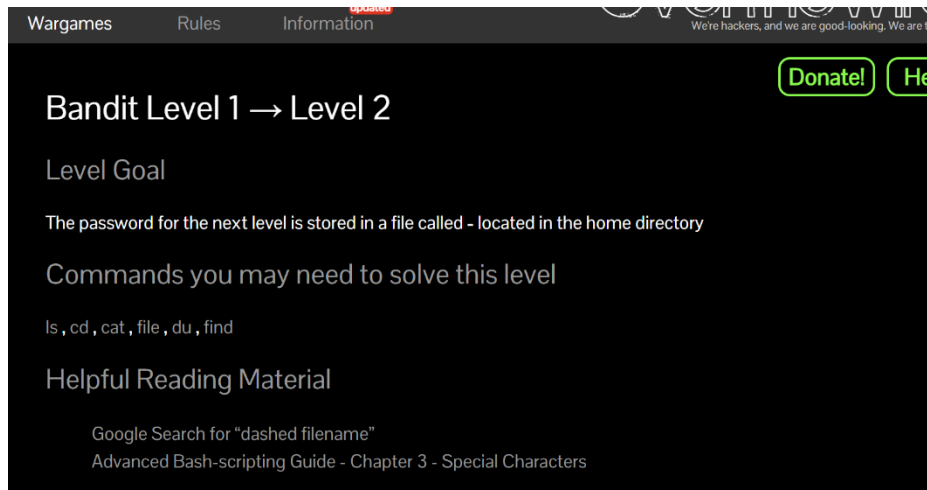
Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

다음 레벨 1로 이동하기 위해, 유저네임 bandit1로 새로 접속해야 하기 때문에, “logout” 명령어를 사용하여, 현재 계정에서 로그아웃을 하고, 다시 “ssh bandit1@bandit.labs.overthewire.org -p2220” 명령어와 앞에서 구한 비밀번호를 통해, 레벨 1로 이동할 수 있었다.

Lv.0 → 1 해결

Lv. 1 → 2



다음 레벨의 비밀번호는 홈 디렉토리에 있는 " - " 라는 이름의 파일에 저장되어 있다고 한다.

```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat -
^C
bandit1@bandit:~$ cat ./-
263JGJPfgU6LtdEvqfWU1XP5yac29mFx
bandit1@bandit:~$
```

아까와 같이, "ls" 명령어를 사용해, - 라는 이름의 파일이 홈 디렉토리에 있는 것을 확인하였다. 그리고, 아까와 같이 명령어를 "cat -" 입력하여, 해당 파일 내용을 출력하려고 하였는데, 명령어 입력이 끝나지 않았다. 그래서, 명령을 중단시켜준 뒤, 파일명인 - 앞에 '현재 디렉토리'를 뜻하는 "./"을 추가하여, 입력해보니 잘 출력되었다. 비밀번호는 "263JGJPfgU6LtdEvqfWU1XP5yac29mFx" 이다.

```
ubuntu@ubuntu-virtual-machine:~$ ssh bandit2@bandit.labs.overthewire.org -p2220
bandit
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit2@bandit.labs.overthewire.org's password:
www. ver he tre.org
Welcome to OverTheWire!
```

앞에서 했던 것처럼 “logout” 명령어를 사용하여, 현재 계정에서 로그아웃을 하고, 다시 “ssh bandit2@bandit.labs.overthewire.org -p2220” 명령어와 앞에서 구한 비밀번호를 통해, 레벨 2로 이동할 수 있었다.

Lv.1 → 2 해결

Lv. 2 → 3

[Wargames](#) [Rules](#) [Information](#) updated

OverTheWire

We're hackers, and we are here to help you.

Bandit Level 2 → Level 3

Level Goal

The password for the next level is stored in a file called **spaces in this filename** located in the home directory

Commands you may need to solve this level

ls, cd, cat, file, du, find

Helpful Reading Material

Google Search for "spaces in filename"

사이트를 확인해보니, 다음 레벨의 비밀번호는 홈 디렉토리에 있는 “spaces in this filename” 이라는 이름의 파일에 저장되어 있다고 한다.

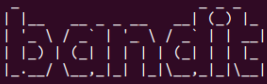
```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces in this filename
cat: spaces: No such file or directory
cat: in: No such file or directory
cat: this: No such file or directory
cat: filename: No such file or directory
```

위 풀이들과 같이, 명령어 "ls"를 통해, spaces in this filename 라는 파일을 발견하고, 명령어 "cat spaces in this filename" 를 통해, 파일 내용을 출력하려고 하였다. 하지만, cat 명령어가 spaces in this filename을 각각 spaces, in, this, filename 이라는 이름의 4개의 파일로 생각하고 따로따로 읽어오려고 하고 있다.

```
cat: filename: No such file or directory
bandit2@bandit:~$ cat spaces\ in\ this\ filename
MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx
```


그래서, 파일명에 공백이 있는 경우, 이를 한 파일명으로 인식시켜주게 하기 위해, 각 공백 앞에 \를 붙여주었다. 비밀번호는 "MNk8KNH3Usiio41PRUEoDFPqfxLPLSmx" 이다.

```
ubuntu@ubuntu-virtual-machine:~$ ssh bandit3@bandit.labs.overthewire.org -p2220
bandit3@bandit.labs.overthewire.org:~$
```



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

bandit3@bandit.labs.overthewire.org's password:



Welcome to OverTheWire!

If you find any problems, please report them to the #wargames channel on discord or IRC.

Lv.2 → 3 해결

Lv. 3 → 4

[Wargames](#) [Rules](#) [Information](#) [updated](#)

OverTheWire
We're hackers, and we are good-looking. We are the 1%.

[Donate!](#) [Help!](#)

Bandit Level 3 → Level 4

Level Goal

The password for the next level is stored in a hidden file in the **inhere** directory.

Commands you may need to solve this level

ls, cd, cat, file, du, find

다음 레벨의 비밀번호는 "inhere" 디렉토리에 있는 숨겨진 파일에 저장되어 있다고 한다.

```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ ls -al
total 12
drwxr-xr-x 2 root root 4096 Jul 17 15:57 .
drwxr-xr-x 3 root root 4096 Jul 17 15:57 ..
-rw-r----- 1 bandit4 bandit3 33 Jul 17 15:57 ...Hiding-From-You
```

일단 inhere 디렉토리를 찾기 위해, 현재 디렉토리에 있는 디렉토리와 파일을 출력해주는 명령어 "ls"를 통해, inhere라는 디렉토리를 발견하였다. 현재 위치를 이동시켜주는 명령어 "cd"를 통해, inhere 디렉토리로 이동하였다. 그 후, inhere 디렉토리의 파일들을 살펴보기 위해, 명령어 "ls"를 해보니, 숨겨진 파일이라 그런지 출력되지 않는다. 그래서 숨겨진 파일을 포함한 모든 파일을 출력해주는 명령어 "ls -al" 입력해보니, "...Hiding-From-You" 라는 파일을 발견하였다.

```
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
bandit3@bandit:~/inhere$ logout
Connection to bandit.labs.overthewire.org closed.
ubuntu@ubuntu-virtual-machine:~$ ssh bandit4@bandit.labs.overthewire.org -p2220

[O] [V] [E] [R] [W] [I] [R] [E]
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

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

bandit4@bandit.labs.overthewire.org's password:

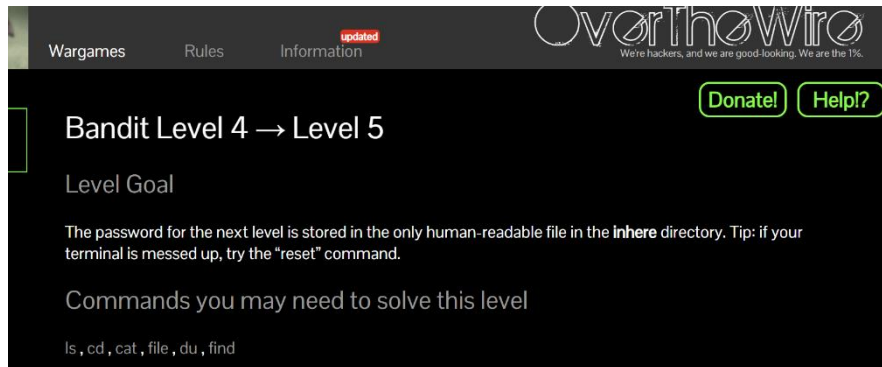
00404
www. ver he ire.org

Welcome to OverTheWire!
```

그 후, "cat ...Hiding-From-You" 을 입력해보니, 비밀번호가 "2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ" 로 출력되었다. 로그아웃하고, 다음 레벨로 이동할 수 있었다.

Lv.3 → 4 해결

Lv. 4 → 5



다음 레벨의 비밀번호는 inhere 디렉토리에 있는 사람이 읽을 수 있는 파일에 저장되어 있다고 한다. 만약, 도중에 터미널이 이상해졌다면, "reset" 명령어를 시도해 보라고 한다.

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -l
total 40
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file00
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file01
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file02
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file03
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file04
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file05
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file06
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file07
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file08
-rw-r----- 1 bandit5 bandit4 33 Jul 17 15:57 -file09
```

앞 풀이와 유사하게, "ls"로 inhere 디렉토리를 찾고, "cd" 명령어로 inhere 디렉토리로 이동하였다. 그 후, "ls -l" 명령어를 통해, 해당 디렉토리의 목록을 상세하게 출력하게끔 하였는데, 여러 파일들이 존재하고 있는 것을 확인할 수 있다.

```
bandit4@bandit:~/inhere$ cat ./-file00
**.,*****Yq*FfL***j**0*****x*4Fbandit4@bandit:~/inhere$ file ./
./: directory
bandit4@bandit:~/inhere$ file ./*
./-file00: data
./-file01: data
./-file02: data
./-file03: data
./-file04: data
./-file05: data
./-file06: data
./-file07: ASCII text
./-file08: data
./-file09: data
bandit4@bandit:~/inhere$ cat ./-file07
4oQYVPkxZ00E00SpTW81FB8j8lxXGUQw
bandit4@bandit:~/inhere$
```

그 중, 아무 파일이나 출력해보니까, 알 수 없는 문자들이 있었다. "file ./*" 명령어를 사용하여, 해당 디렉토리에 위치한 파일들의 종류를 출력하게끔 하였다. 나머지는 다 data 타입인데, "-file07"만 사람이 읽을 수 있는 아스키 코드 형식이었다. 이를 "cat" 명령어로

출력하니, 비밀번호는 “4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw” 인 것을 알 수 있었다.

```
ubuntu@ubuntu-virtual-machine:~$ ssh bandit5@bandit.labs.overthewire.org -p2220
bandit5@bandit.labs.overthewire.org:~$

[O] [V] [E] [R] [I] [E]
[ ] [ ] [ ] [ ] [ ] [ ]

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

bandit5@bandit.labs.overthewire.org's password:

[O] [V] [E] [R] [I] [E]
[ ] [ ] [ ] [ ] [ ] [ ]

www. ver he ire.org

Welcome to OverTheWire!
```

Lv.4 → 5 해결