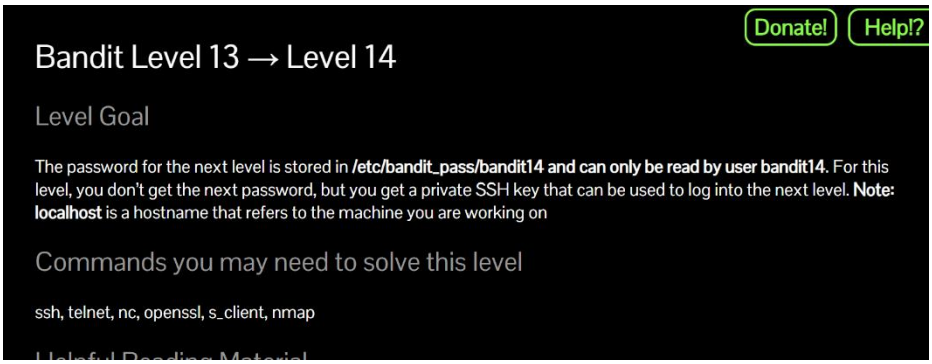
4회차 - 20. 케로로

Bandit 레벨 13 ~ 16 라이트업

정보보호학부 2024111262 조현서

Lv. 13 → 14

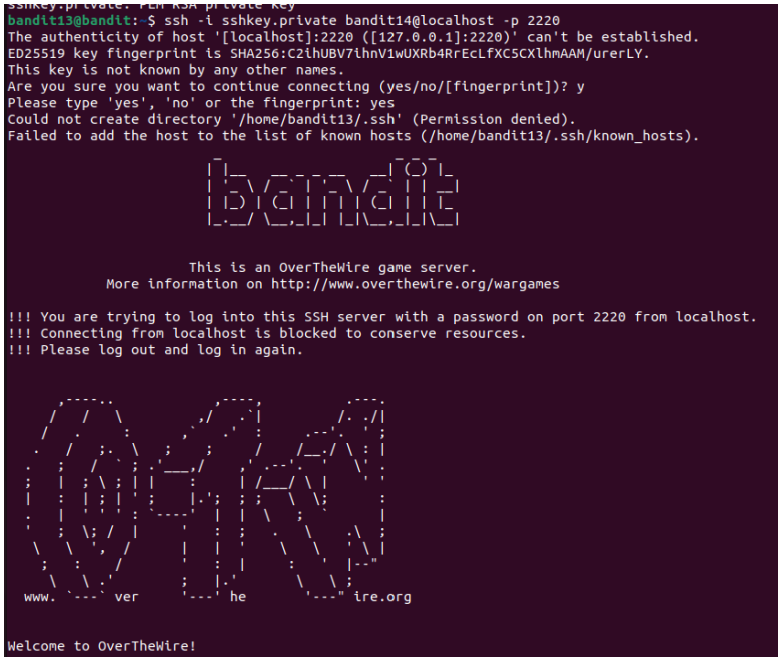


웹 사이트의 문제 설명을 보니, 다음 레벨의 비밀번호는 /etc/bandit_pass/bandit14에 저장되어 있으며, 오직 bandit14 사용자만 읽을 수 있다고 한다. 이 레벨에서는 비밀번호를 직접 얻지 않고, 다음 레벨에 로그인할 수 있는 개인 SSH 키를 얻게 된다고 한다. 참고로, localhost는 현재 작업 중인 기계를 나타내는 호스트 이름이라고 한다.

```
bandit13@bandit:~$ ls -al
total 24
drwxr-xr-x  2 root     root     4096 Sep 19 07:08 .
drwxr-xr-x 70 root     root     4096 Sep 19 07:09 ..
-rw-r--r--  1 root     root      220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root     root     3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root     root      807 Mar 31  2024 .profile
-rw-r-----  1 bandit14 bandit13 1679 Sep 19 07:08 sshkey.private
bandit13@bandit:~$ file sshkey.private
sshkey.private: PEM RSA private key
bandit13@bandit:~$
```

ls -al을 통해, 현재 모든 파일들의 목록을 확인해보니, 누가봐도 ssh 키와 관련되어 보이는 sshkey.private 파일을 발견할 수 있었다. File 명령어를 통해 해당 파일을 살펴보니 PEM RSA private key라고 한다. 이를 어떻게 다룰지 감이 안 와서 인터넷에 검색해보니, ssh 명령어 옵션 중에 -i 가 있는데 이 명령어는 RSA 인증을 위한 비밀 키를 읽는 아이

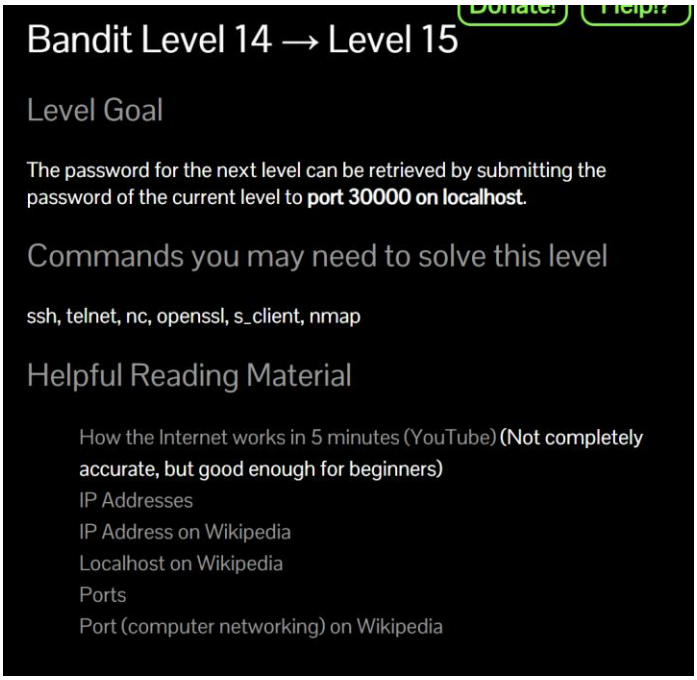
덴티티 파일을 선택할 수 있다고 한다. 이를 활용하여, 풀이를 진행해보려고 한다.



ssh -i sshkey.private bandit14@localhost -p 2220 명령어를 입력해보니, 자동으로 bandit14 계정으로 로그인되어 있었다!

Lv.13 → 14해결

Lv. 14 → 15



Bandit Level 14 → Level 15

Level Goal

The password for the next level can be retrieved by submitting the password of the current level to **port 30000 on localhost**.

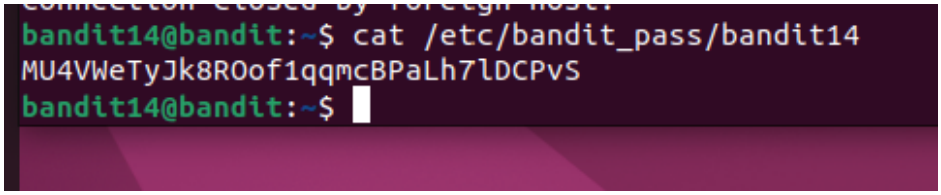
Commands you may need to solve this level

ssh, telnet, nc, openssl, s_client, nmap

Helpful Reading Material

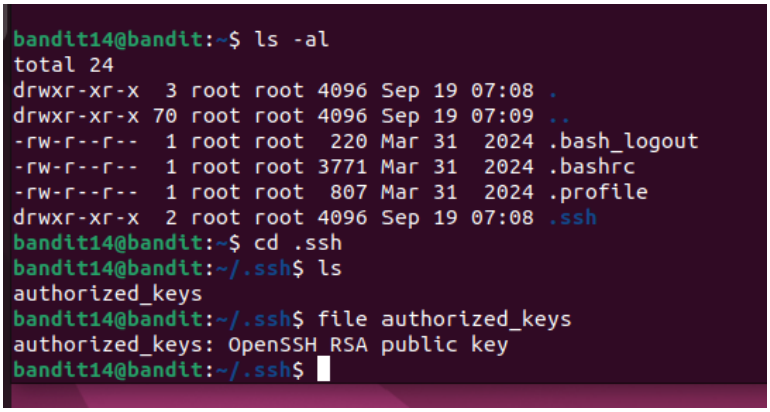
How the Internet works in 5 minutes (YouTube) **(Not completely accurate, but good enough for beginners)**
IP Addresses
IP Address on Wikipedia
Localhost on Wikipedia
Ports
Port (computer networking) on Wikipedia

다음 레벨의 비밀번호는 localhost의 30000번 포트로 출력하게끔 해서 얻을 수 있다고 한다.



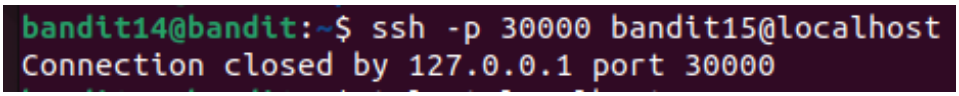
```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$
```

Cat /etc/bandit_pass/bandit14 명령어를 입력하니, bandit14의 비밀번호가 출력되었다! 레벨 14 비밀번호는 "**MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS**"이다.

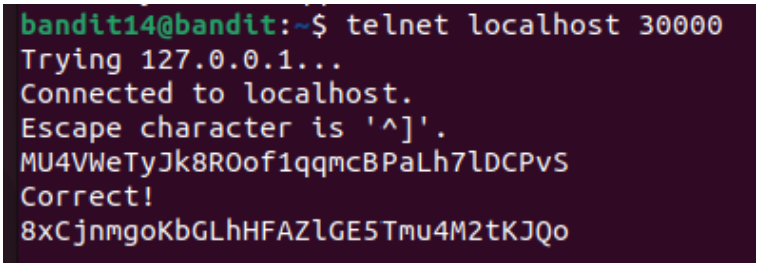


```
bandit14@bandit:~$ ls -al
total 24
drwxr-xr-x  3 root root 4096 Sep 19 07:08 .
drwxr-xr-x 70 root root 4096 Sep 19 07:09 ..
-rw-r--r--  1 root root  220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root root 3771 Mar 31  2024 .bashrc
-rw-r--r--  1 root root  807 Mar 31  2024 .profile
drwxr-xr-x  2 root root 4096 Sep 19 07:08 .ssh
bandit14@bandit:~$ cd .ssh
bandit14@bandit:~/.ssh$ ls
authorized_keys
bandit14@bandit:~/.ssh$ file authorized_keys
authorized_keys: OpenSSH RSA public key
bandit14@bandit:~/.ssh$
```

그 후, ls -al을 통해, 현재 모든 파일들의 목록을 확인해보니, 숨겨진 ssh 디렉토리를 발견할 수 있었다. 그리고 그 디렉토리 안에는 authorized_keys라는 파일이 존재하였다. 해당 파일을 file 명령어를 사용하여 살펴보니, OpenSSH RSA public key라고 한다. 뭔가 전 단계와 비슷해 보인다. 아까와 유사하게 30000번 포트를 통해 비밀번호를 얻어내려고 해보았는데,



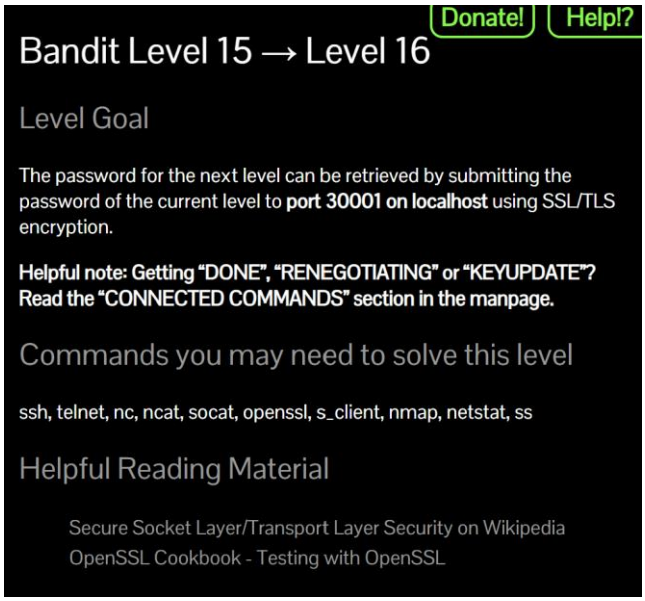
연결이 진행되지 않는데, 그래서 비슷한 명령어인 telnet을 사용해보기로 하였다.



telnet localhost 30000을 입력하니, escape character을 입력하라길래, 레벨 14의 비밀번호를 입력하니 correct!이라면서 레벨 15의 비밀번호가 출력되었다. 레벨 15 비밀번호는 "**8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo**"이다.

Lv.14→ 15해결

Lv. 15 → 16



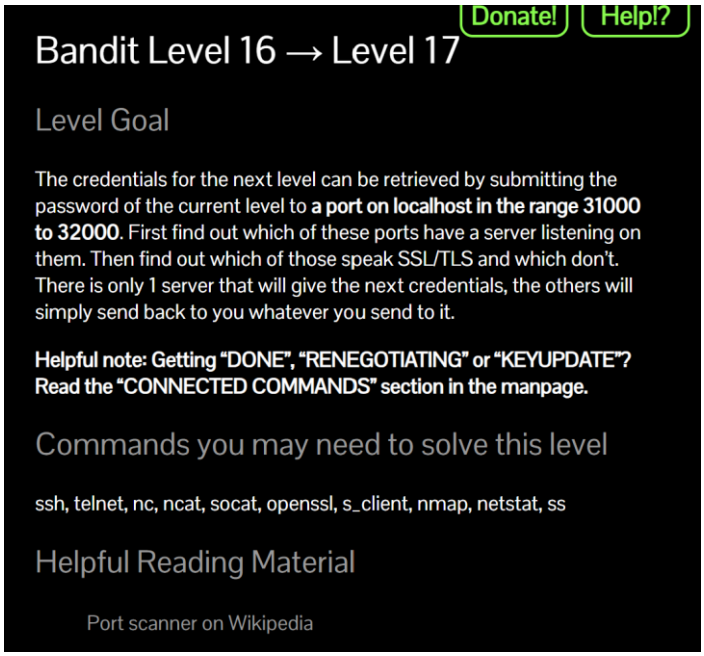
다음 레벨의 비밀번호는 현재 레벨의 비밀번호를 localhost의 포트 30001로 전송함으로써 얻을 수 있다.

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
```

이는 지난번과 유사하지만 SSL/TLS 암호화 방식이 사용된다는 점에서 차이점이 있다. Openssl 명령어를 사용해서 연결한 후, 현재 레벨의 비밀번호를 전송해보려고 한다. "openssl s_client -connect localhost:30001" 를 입력하니,
다음 단계의 비밀번호는 "**kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx**"이다.

Lv.15 → 16 해결

Lv. 16 → 17



다음 레벨의 비밀번호는 현재 레벨의 비밀번호를 localhost의 포트 31000에서 32000 사이로 전송해야 한다 이 포트들 중 어떤 포트에서 서버가 대기하고 있는지 확인한 후, SSL/TLS 를 사용하는 포트와 사용하지 않는 포트를 구분해야 할 것으로 보인다.

```
bandit16@bandit:~$ nmap -sV localhost -p 31000-32000
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-18 14:54 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE     VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
```

Nmap 명령어를 사용해서 우리에게 필요한 포트가 뭔지 탐색해보았다. 다른건 exho로 뜨는데 31790 포트에서만 이상하게 unknown이 뜨는게 수상해보인다.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----
```

그래서 이전에 풀었던 방식과 같이, openssl s_client -connect localhost:31790 을 입력하니, 개인 키가 출력되었다. 이를 somefile,private에 복사한 후, bandit17에 연결하면 될 것으로 보인다.

다음 단계 비밀번호는 "**FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn**"이다

Lv.12 → 13 해결