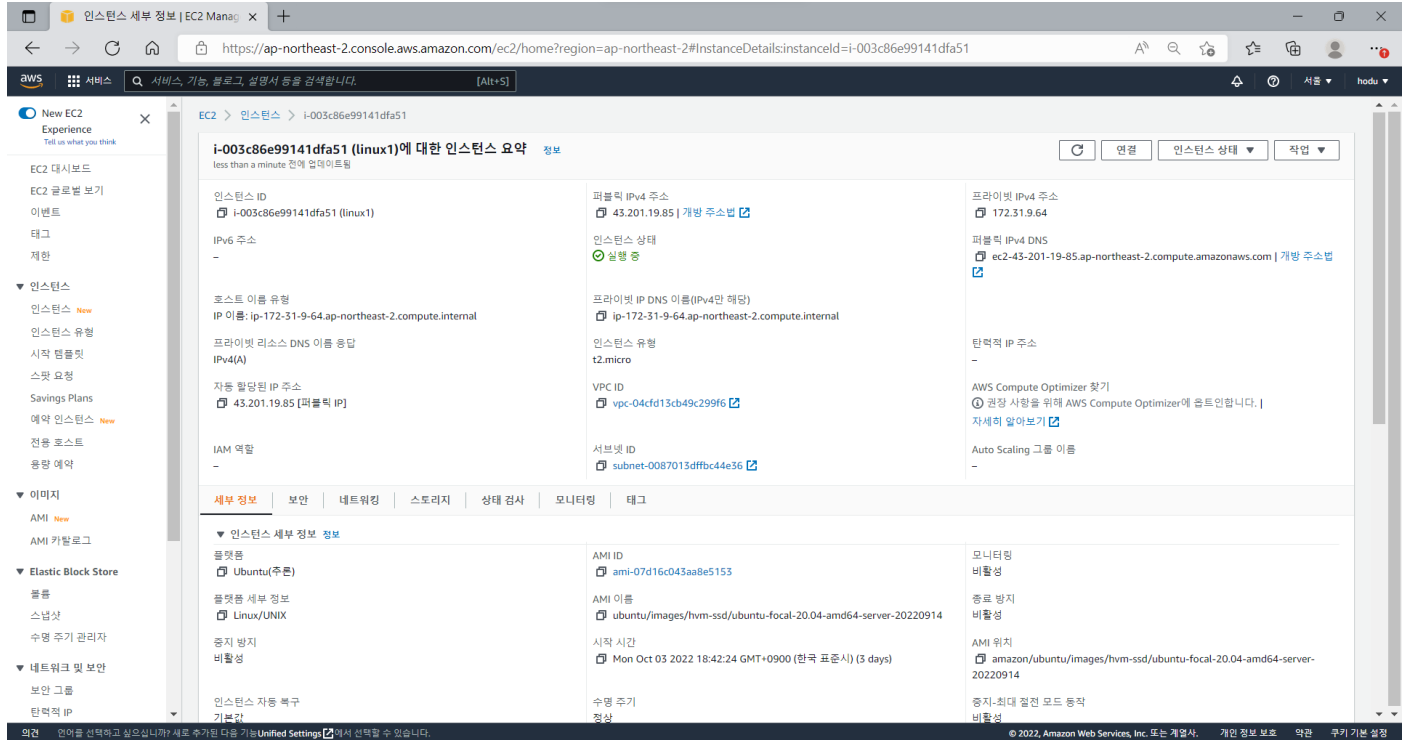
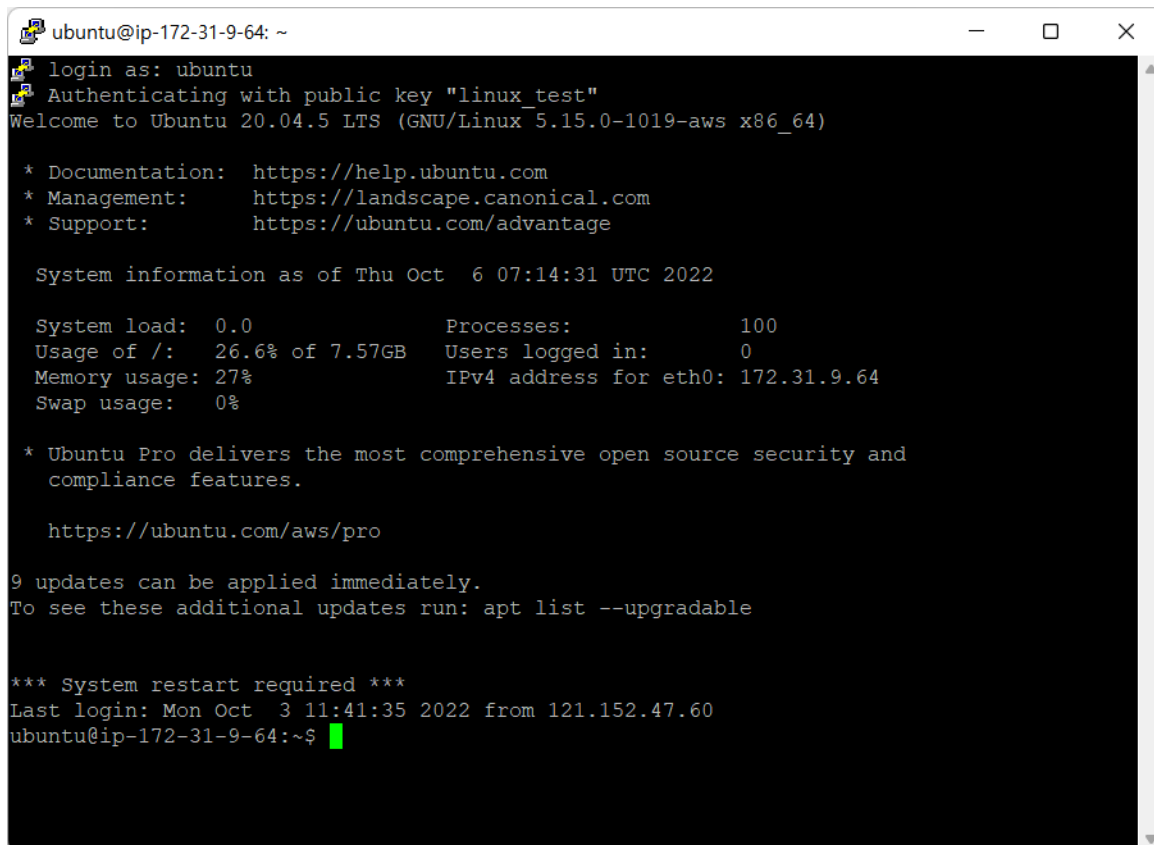


과제 1. 리눅스 보안

1-1. 리눅스 시스템 구성하기



1-2. putty로 리눅스 연결



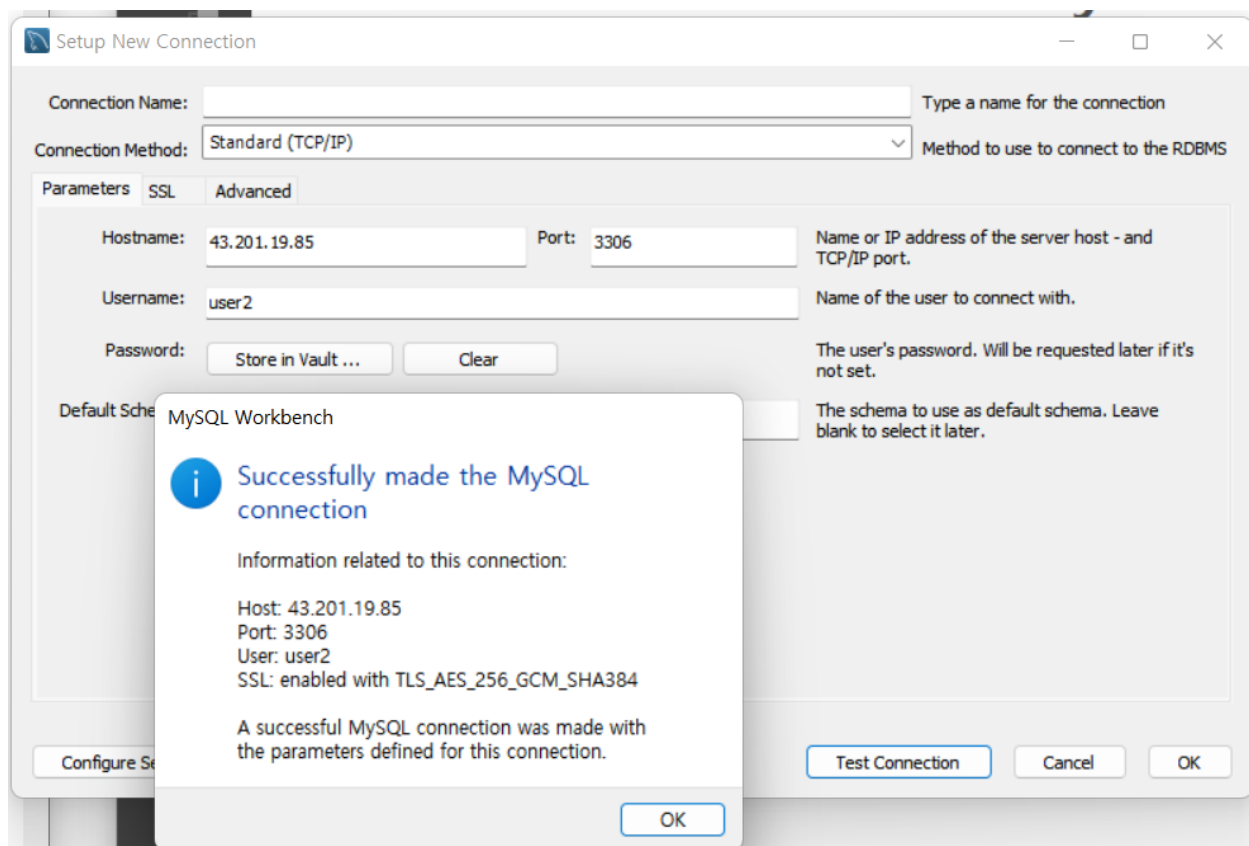
2. 계정 생성

```
user1@ip-172-31-9-64: /home/ubuntu
user1@ip-172-31-9-64:/home/ubuntu$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:112:./run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:./nonexistent:/usr/sbin/nologin
sshd:x:109:65534:./run/sshd:/usr/sbin/nologin
landscape:x:110:115:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1:./var/cache/pollinate:/bin/false
ec2-instance-connect:x:112:65534:./nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:./usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100:./var/snap/lxd/common/lxd:/bin/false
user1:x:1001:1001:,,,:/home/user1:/bin/bash
mysql:x:113:119:MySQL Server,,,:/nonexistent:/bin/false
user1@ip-172-31-9-64:/home/ubuntu$
```

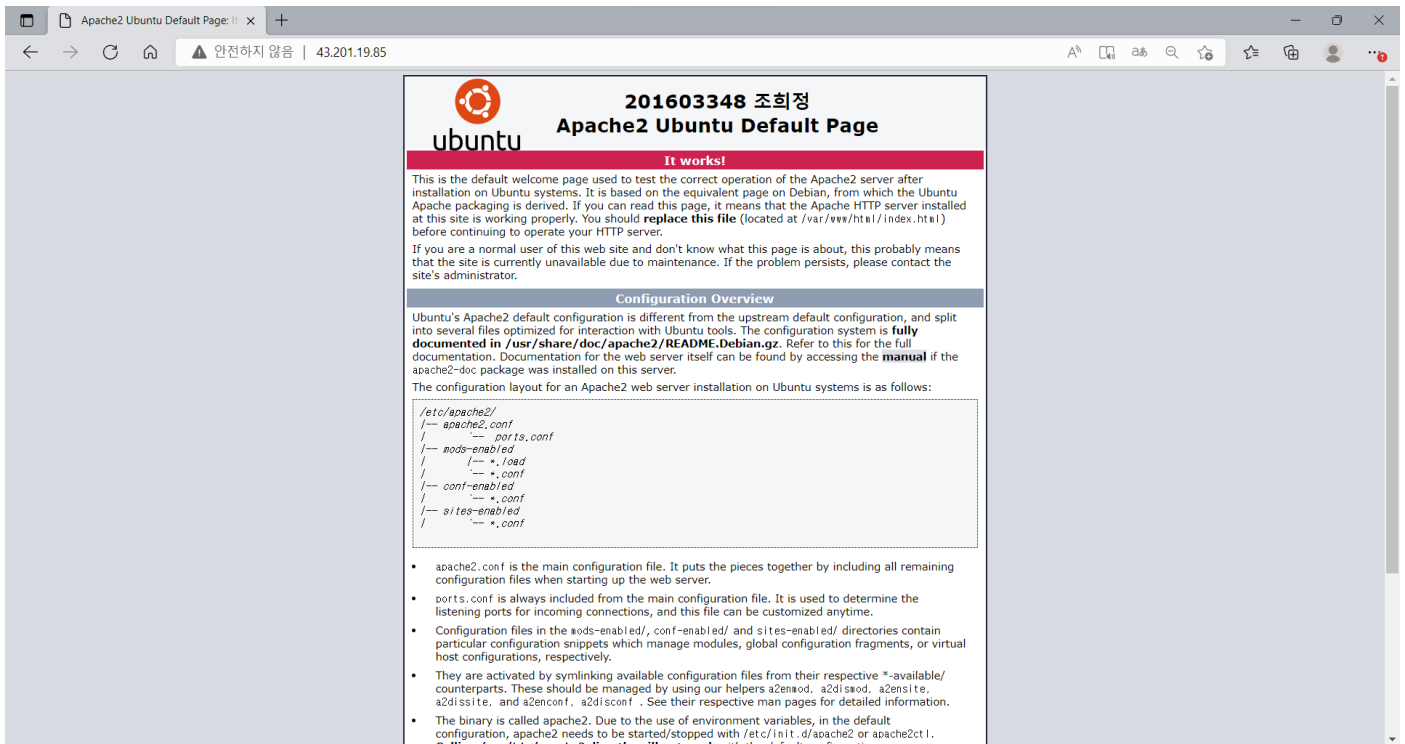
3-1. mysql 설치 및 구동

```
ubuntu@ip-172-31-9-64: ~  
ubuntu@ip-172-31-9-64:~$ sudo mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 10  
Server version: 8.0.30-0ubuntu0.20.04.2 (Ubuntu)  
  
Copyright (c) 2000, 2022, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> select host, user from mysql.user;  
+-----+-----+  
| host      | user                |  
+-----+-----+  
| %         | user2               |  
| localhost | debian-sys-maint    |  
| localhost | mysql.infoschema    |  
| localhost | mysql.session       |  
| localhost | mysql.sys           |  
| localhost | root                |  
+-----+-----+  
6 rows in set (0.00 sec)  
  
mysql>
```

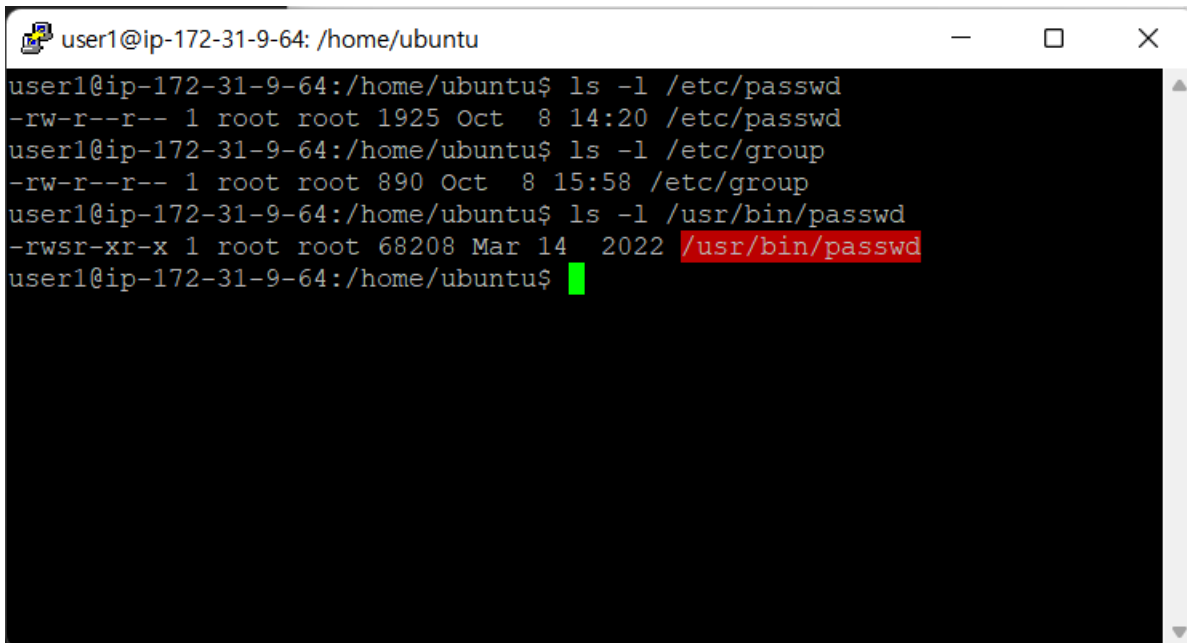
3-2. workbench로 mysql 서버 접속



3-3. apache 설치 및 서버 접속



4. 파일의 접근 권한 확인



5-1. 리눅스 로그 파일 확인

```
ubuntu@ip-172-31-9-64: ~  
ubuntu@ip-172-31-9-64:~$ cat /var/log/auth.log  
Oct 9 00:17:01 ip-172-31-9-64 CRON[45032]: pam_unix(cron:session): session opened for user root by (uid=0)  
Oct 9 00:17:01 ip-172-31-9-64 CRON[45032]: pam_unix(cron:session): session closed for user root  
Oct 9 00:42:19 ip-172-31-9-64 sshd[45065]: Invalid user admin from 60.132.35.157 port 61113  
Oct 9 00:42:20 ip-172-31-9-64 sshd[45065]: error: maximum authentication attempts exceeded for invalid user admin from 60.132.35.157 port 61113 ssh2 [preauth]  
Oct 9 00:42:20 ip-172-31-9-64 sshd[45065]: Disconnecting invalid user admin 60.132.35.157 port 61113: Too many authentication failures [preauth]  
Oct 9 00:42:20 ip-172-31-9-64 sshd[45067]: Connection closed by 60.132.35.157 port 61121 [preauth]  
Oct 9 00:47:01 ip-172-31-9-64 CRON[45076]: pam_unix(cron:session): session opened for user root by (uid=0)  
Oct 9 00:47:01 ip-172-31-9-64 CRON[45076]: pam_unix(cron:session): session closed for user root  
Oct 9 00:53:31 ip-172-31-9-64 sshd[45097]: error: kex_exchange_identification: Connection closed by remote host  
Oct 9 00:56:07 ip-172-31-9-64 sshd[45133]: error: kex_exchange_identification: Connection closed by remote host  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45134]: Invalid user natasha from 104.254.245.83 port 42890  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45139]: Invalid user vion from 104.254.245.83 port 43000  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45138]: Invalid user splunk from 104.254.245.83 port 42928  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45142]: Invalid user vion from 104.254.245.83 port 43070  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45150]: Invalid user es from 104.254.245.83 port 43104  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45134]: Connection closed by invalid user natasha 104.254.245.83 port 42890 [preauth]  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45163]: Invalid user halo from 104.254.245.83 port 43114  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45157]: Invalid user server from 104.254.245.83 port 42920  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45140]: Invalid user jeus from 104.254.245.83 port 42938  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45141]: Invalid user prashant from 104.254.245.83 port 43146  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45155]: Invalid user web from 104.254.245.83 port 43142  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45149]: Invalid user bitrix from 104.254.245.83 port 43002  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45153]: Invalid user admin from 104.254.245.83 port 42948  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45145]: Invalid user hd1ept07 from 104.254.245.83 port 42930  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45152]: Invalid user user from 104.254.245.83 port 43012  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45162]: Invalid user eng from 104.254.245.83 port 43206  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45139]: Connection closed by invalid user vion 104.254.245.83 port 43000 [preauth]  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45136]: Connection closed by authenticating user root 104.254.245.83 port 42906 [preauth]  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45159]: Invalid user pi from 104.254.245.83 port 43136  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45144]: Connection closed by authenticating user root 104.254.245.83 port 43144 [preauth]  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45161]: Invalid user caspida from 104.254.245.83 port 43122  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45143]: Invalid user vagrant from 104.254.245.83 port 43192  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45138]: Connection closed by invalid user splunk 104.254.245.83 port 42928 [preauth]  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45142]: Connection closed by invalid user vion 104.254.245.83 port 43070 [preauth]  
Oct 9 00:56:09 ip-172-31-9-64 sshd[45150]: Connection closed by invalid user es 104.254.245.83 port 43104 [preauth]
```

5-2. mysql 에러 로그 파일 확인

```
ubuntu@ip-172-31-9-64: ~  
ubuntu@ip-172-31-9-64:~$ cat /var/log/mysql/error.log  
2022-10-10T02:12:43.608264Z 54 [Warning] [MY-010055] [Server] IP address '43.134.92.151' could not be resolved: Name or service not known  
2022-10-10T04:40:28.279341Z 55 [Warning] [MY-010055] [Server] IP address '45.83.64.1' could not be resolved: Name or service not known  
ubuntu@ip-172-31-9-64:~$
```

6. 웹 서버 로그 파일 확인

```
ubuntu@ip-172-31-9-64: ~  
ubuntu@ip-172-31-9-64:~$ tail -f /var/log/apache2/access.log  
210.123.151.135 - - [08/Oct/2022:16:32:40 +0000] "GET / HTTP/1.1" 200 11173 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"  
20.125.137.138 - - [08/Oct/2022:16:45:54 +0000] "GET /.env HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"  
20.125.137.138 - - [08/Oct/2022:16:45:54 +0000] "POST / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36"  
121.152.47.60 - - [08/Oct/2022:16:58:53 +0000] "GET / HTTP/1.1" 200 3519 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33"  
121.152.47.60 - - [08/Oct/2022:16:58:53 +0000] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://43.201.19.85/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33"  
121.152.47.60 - - [08/Oct/2022:16:59:37 +0000] "GET / HTTP/1.1" 200 3516 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33"  
118.235.13.162 - - [08/Oct/2022:16:59:45 +0000] "GET / HTTP/1.1" 200 3516 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 16_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.0 Mobile/15E148 Safari/604.1"  
121.152.47.60 - - [08/Oct/2022:17:00:02 +0000] "GET / HTTP/1.1" 200 3516 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.33"  
121.152.47.60 - - [08/Oct/2022:17:00:54 +0000] "-" 408 0 "-" "-"  
128.14.209.162 - - [08/Oct/2022:17:30:30 +0000] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
```