

과제 12/5

2315028 김성현

1. ssh서버에 로그인과정없이 바로 접속

공개키를 삭제함!

```
rocky@localhost:~  
ssh-rsa AAAAC3NzaC1lZDI1NTE5AAAAIO7YfchUriaJmZr6YMY80M4jmFh  
HPEY9aH5ct2QeXb/  
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCYNbtOrw2YrsqYcZS6/VxcIguA  
eAP1CE50VwzeY30No0oTBq1lUNMKoK+M3F0HrYT2ki4mdZIdx2U0IPKZ/GsZEkoU+Anl+7Cn/PTx6kXv  
8P9NpTvn0+L0UQLTSxzVP2D0nvc88IdtecYS++hxc9AznHNN0I0Czf1DggyH6PAkzstkV6W0Rpy0HRRG  
Lxe4GadEH3nLQuNIIdzrxhlkz1XoIv0Bb1uHxq3EL9mUvdaDz/9A5zF1D09NKglZ1X8a0vPq3QcfWWcsi  
Q2FmHZSJNRIEhdpfSqK68zg72C3MFYZrORKTFXcwhoLk3sVr21WBBRUPmjGdJ8UG+NW6P7boZoRG8t5  
nxQEsng2tULMMWboxGSwlx1+QCsVZDWjEULGgWZjM30J/PA2AiIq/R7oNSH/nCaTfhn0rZ7ZtNzH+2Gm  
SVX0LAR9ChDmBuL1xHGgIW57ulrVkr3ZwgljtJzvKSp06800sTYXank25jdj3RxgsH4UBo84+GY3NWgj  
vhDAvr0=  
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy  
NTYAAABBBH4g1o3nWML7rm/4JHRiX8BaTii7tzQHDc6m6zIn4G21/JbgE69FCyHhuSkZdUraBznBCv+l  
Q4eIZkFgiR6wRzY=  
~  
~
```

srv-adm-sec.net에 로그인 없이 바로 접속!!

```
[rocky@localhost ~]$ vi ~/.ssh/known_hosts  
[rocky@localhost ~]$ ssh kh15028@srv-adm-sec.net  
The authenticity of host 'srv-adm-sec.net (59.6.51.163)' can't be established.  
ED25519 key fingerprint is SHA256:kWsOnSmF2VTD/N40/S+OH0ME/2NDbb6agHqD5fVHIGI.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'srv-adm-sec.net' (ED25519) to the list of known host  
s.  
kh15028@srv-adm-sec.net's password:  
서버 운영 및 보안 (2024-Fall) 실습용 원격 서버입니다.  
Last login: Tue Nov 26 13:20:01 2024 from 1.209.144.250  
[kh15028@srv-adm-sec ~]$
```

공개키를 authorized_keys에 넣음!


```

(base) → ~ git:(main) * nmap -T5 -sn 192.168.111.1-254
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-05 12:23 KST
Nmap scan report for 192.168.111.1
Host is up (0.00074s latency).
Nmap scan report for 192.168.111.128
Host is up (0.0011s latency).
Nmap done: 254 IP addresses (2 hosts up) scanned in 21.35 seconds
(base) → ~ git:(main) * nmap -T5 -sV 192.168.111.129
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-05 12:24 KST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.79 seconds

```

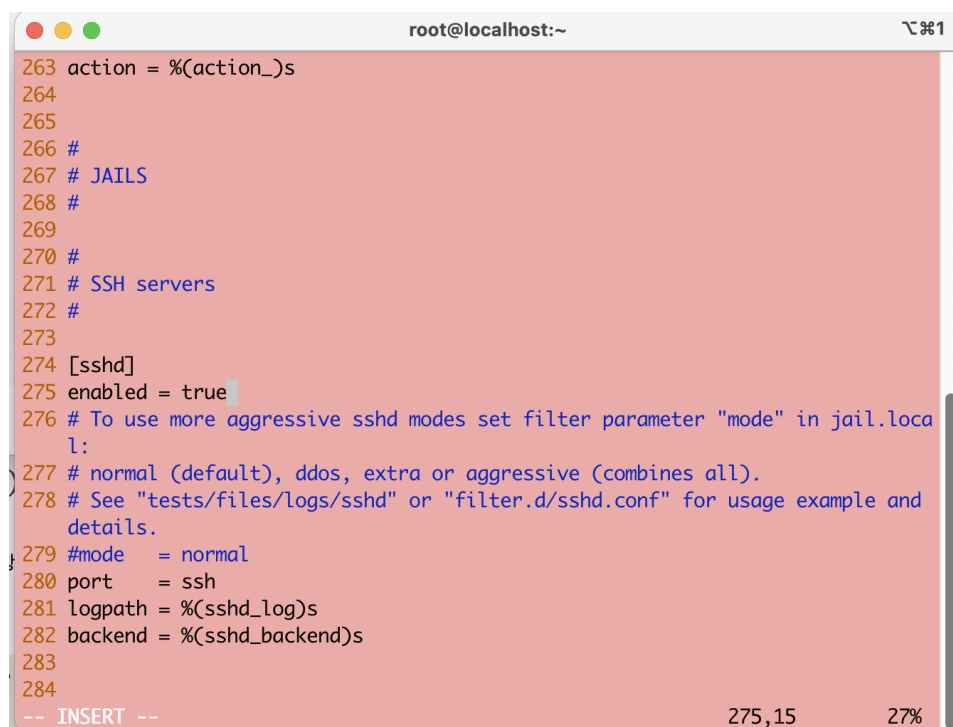
3. 로그인 시도(fail2ban 실행)

```

[root@localhost ~]# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
[root@localhost ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.
[root@localhost ~]# systemctl start fail2ban

```

vi편집기로 /etc/fail2ban/jail.local 파일을 열어 수정함



```

root@localhost:~
263 action = %(action_)s
264
265
266 #
267 # JAILS
268 #
269
270 #
271 # SSH servers
272 #
273
274 [sshd]
275 enabled = true
276 # To use more aggressive sshd modes set filter parameter "mode" in jail.local:
277 # normal (default), ddos, extra or aggressive (combines all).
278 # See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
279 #mode = normal
280 port = ssh
281 logpath = %(sshd_log)s
282 backend = %(sshd_backend)s
283
284
-- INSERT --
275,15 27%

```

```
(base) → ~ git:(main) ✕ ssh wis-hyun@192.168.111.128
wis-hyun@192.168.111.128's password:
Permission denied, please try again.
wis-hyun@192.168.111.128's password:
Permission denied, please try again.
wis-hyun@192.168.111.128's password:
wis-hyun@192.168.111.128: Permission denied (publickey,gssapi-keyex,gssapi-with-
mic,password).
(base) → ~ git:(main) ✕ ssh wis-hyun@192.168.111.128
wis-hyun@192.168.111.128's password:
Permission denied, please try again.
wis-hyun@192.168.111.128's password:
Permission denied, please try again.
wis-hyun@192.168.111.128's password:
```