

# System Programming & OS 실습

## 3. SSH, Port Forwarding

정지현, 안석현, 김선재

Dankook University

{wlgjsjames7224, seokhyun, rlatjswo0824}@dankook.ac.kr

# Index

❖ SSH

❖ Port Forwarding

❖ SSH Installation

❖ Putty

❖ Window Terminal

## ❖ SSH (Secure Shell)

- 원격 호스트에 접속하기 위해 사용되는 프로토콜
- 네트워크 상의 다른 컴퓨터에 로그인, 원격 시스템에서 명령을 실행, 다른 시스템으로 파일을 복사할 수 있음
- Client와 Server의 통신이 암호화되어 안전하게 통신

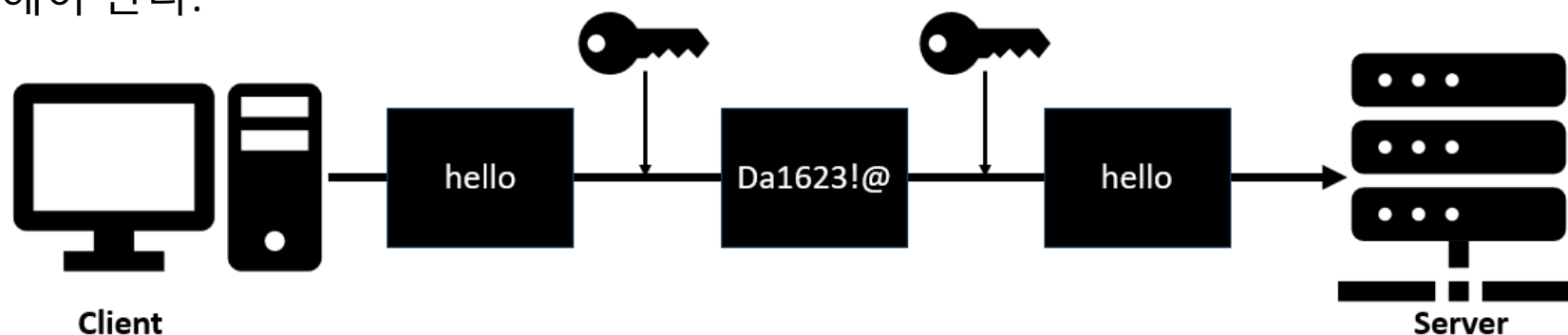


# SSH(Secure Shell)

## ❖ SSH (Secure Shell) 사용 이유

- 사용자 및 자동화 된 프로세스에 원격 접속 시
- 자동화된 파일 전송 시
- 원격 명령 실행 시
- 네트워크 인프라와 중요 시스템 관리 시

=> 안전한 통신을 하기 위해 사용해야 한다.



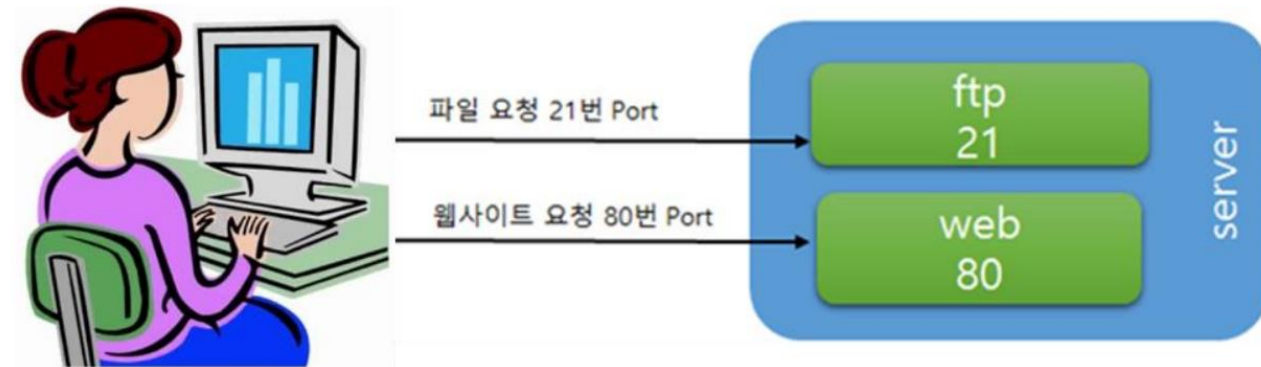
# Port Forwarding

## ❖ Port

- 통신을 필요로 하는 프로그램이 다수일 때, 이를 구별할 수 있는 번호로 “논리적인 접속장소 ” 를 의미
- 각각의 응용 프로그램에 정해진 포트 번호를 이용해 구분

ex) 컴퓨터에 여러 개의 서버가 실행되고 있을 때, 포트 번호를 통해 어느 서버에 접속해야 하는지 컴퓨터에 알려줄 수 있음

- SSH -> 22 / HTTP -> 80 / FTP -> 21, ...



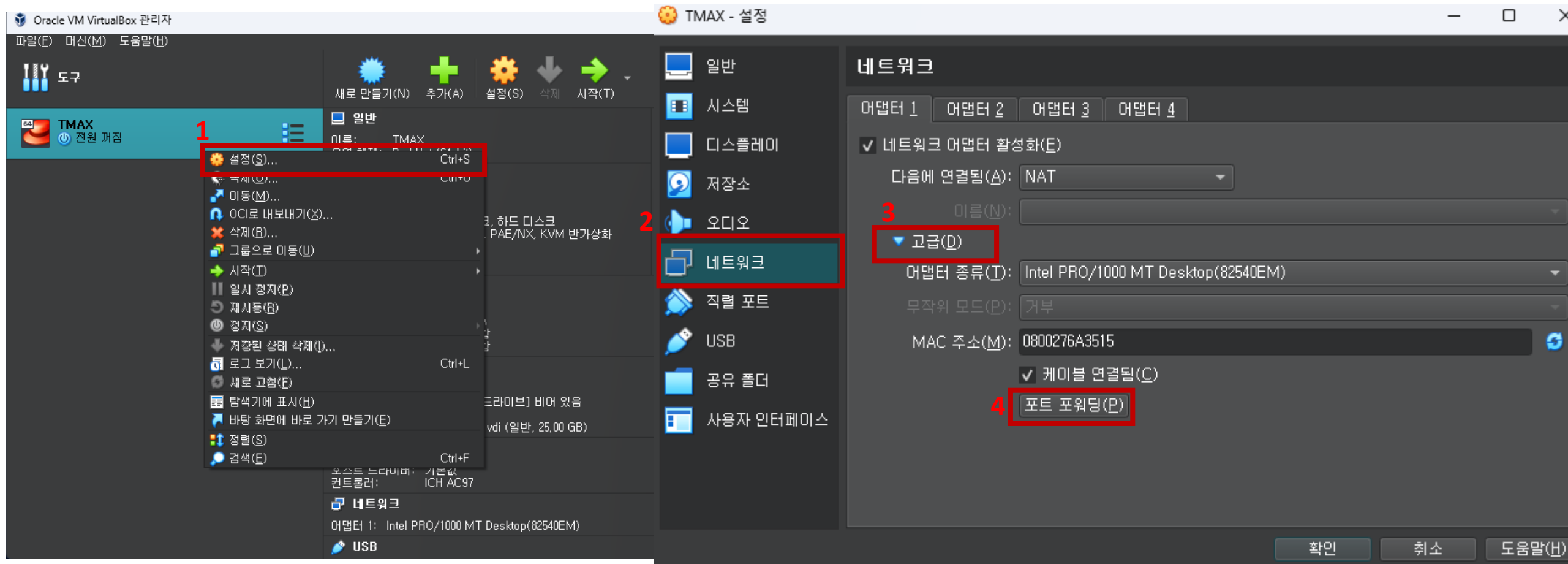
# Port Forwarding

## ❖ Port Forwarding

- 특정한 포트로 들어오는 데이터 패킷을 다른 포트로 바꿔서 다시 전송해주는 포트 전달
  - 외부에서 공유기에 연결된 PC에 통신을 요청할 때, 공유기에 이정표를 달아주는 작업
- ex) 21번 포트로 요청이 오면 공유기는 이정표를 참조해 192.168.0.20번 PC로 전달 가능

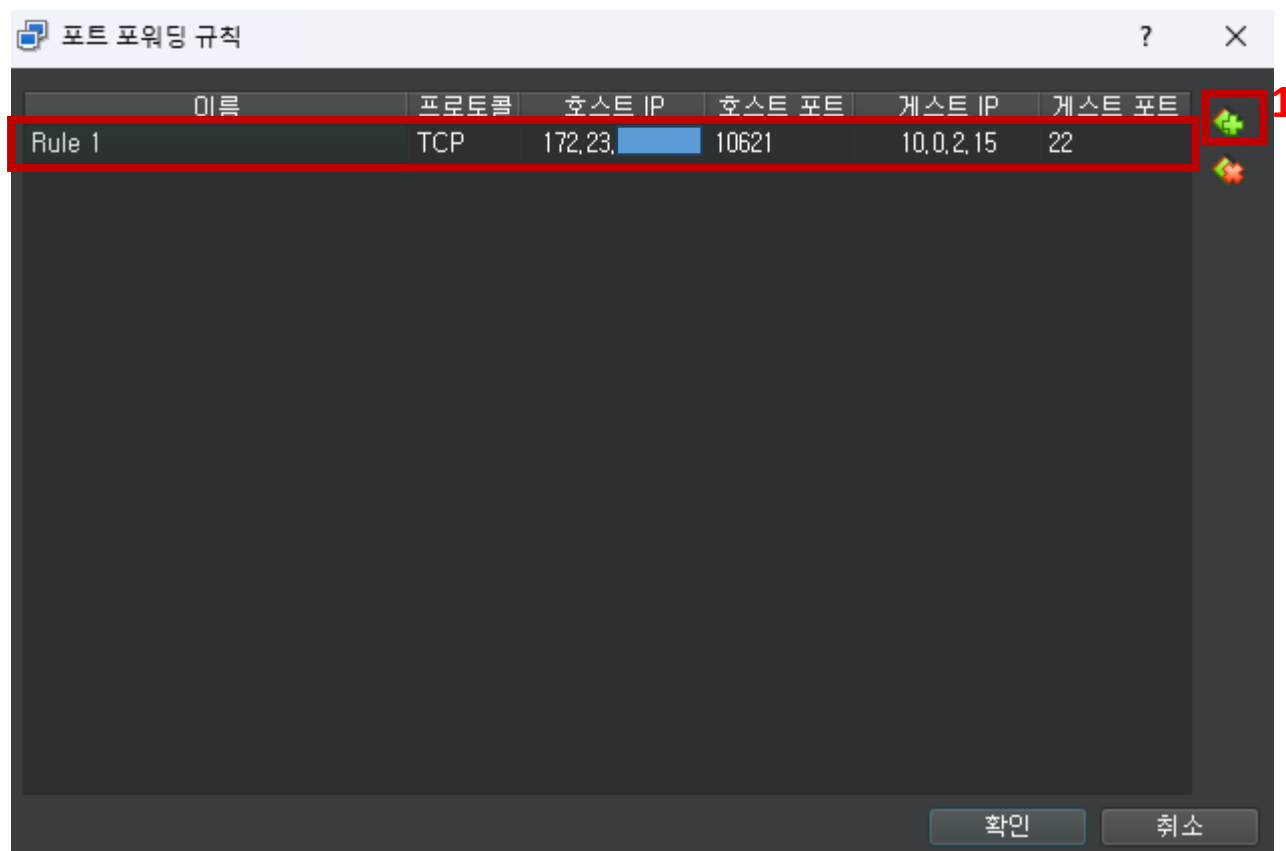


# Virtual Box Port Forwarding



# Virtual Box Port Forwarding

1



- 호스트 IP
  - 172.23.XXX.XXX
- 호스트 Port
  - 10621 (임의)
- 게스트 IP
  - 10.0.2.15
- 게스트 Port
  - 22



# Virtual Box SSH Installation

1

```
[seokhyun@localhost ~]$ sudo yum install openssh-server
```

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for seokhyun:
```

```
CentOS Stream 9 - BaseOS                12 kB/s | 6.4 kB    00:00
CentOS Stream 9 - AppStream              11 kB/s | 6.5 kB    00:00
CentOS Stream 9 - Extras packages        27 kB/s | 6.5 kB    00:00
Package openssh-server-8.7p1-43.el9.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[seokhyun@localhost ~]$
```

- yum 명령어를 통한 ssh 설치
- sudo yum install openssh-server

```
[seokhyun@localhost ~]$ sudo yum -y install openssh-server openssh-clients openssh-askpass
```

```
Last metadata expiration check: 0:04:52 ago on Fri 09 Aug 2024 03:30:34 AM KST.
Package openssh-server-8.7p1-43.el9.x86_64 is already installed.
Package openssh-clients-8.7p1-43.el9.x86_64 is already installed.
Dependencies resolved.
```

- 1번 명령어로 설치가 안될 시
  - sudo yum -y install openssh-server openssh-clients openssh-askpass

# Virtual Box SSH Installation

```
[seokhyun@localhost ~]$ yum list installed | grep ssh
libssh.x86_64                                0.10.4-13.el9                                @anaconda
libssh-config.noarch                        0.10.4-13.el9                                @anaconda
openssh.x86_64                              8.7p1-43.el9                                @anaconda
openssh-askpass.x86_64                     8.7p1-43.el9                                @appstream
openssh-clients.x86_64                     8.7p1-43.el9                                @anaconda
openssh-server.x86_64                      8.7p1-43.el9                                @anaconda
```

- grep을 통해 ssh 설치 확인
- yum list installed | grep ssh

```
[seokhyun@localhost ~]$ sudo cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- cat을 통해 설정 파일 확인
- sudo cat /etc/ssh/sshd\_config

# Virtual Box SSH Installation

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
```

Port 22

```
[seokhyun@localhost ~]: cat /etc/ssh/sshd_config
cat: /etc/ssh/sshd_config: Permission denied
[seokhyun@localhost ~]$ sudo cat /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# To modify the system-wide sshd configuration, create a *.conf file under
# /etc/ssh/sshd_config.d/ which will be automatically included below
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

- `sudo vim /etc/ssh/sshd_config`
- `#port 22 -> port 22` (주석제거)
- `cat /etc/ssh/sshd_config`

# Virtual Box SSH Installation

```
[seokhyun@localhost ~]$ service sshd start
Redirecting to /bin/systemctl start sshd.service
[seokhyun@localhost ~]$ service sshd status
Redirecting to /bin/systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-08-09 03:35:26 KST; 15min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 877 (sshd)
    Tasks: 1 (limit: 23008)
   Memory: 2.8M
      CPU: 28ms
   CGroup: /system.slice/sshd.service
           └─877 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 09 03:35:26 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Aug 09 03:35:26 localhost.localdomain sshd[877]: Server listening on 0.0.0.0 port 22.
Aug 09 03:35:26 localhost.localdomain sshd[877]: Server listening on :: port 22.
Aug 09 03:35:26 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
```

- service sshd start
- service sshd status

# SSH Installation Trouble Shooting

```
[seokhyun@localhost ~]$ service sshd start
Redirecting to /bin/systemctl start sshd.service
Job for sshd.service failed because the control process exited with error code.
See "systemctl status sshd.service" and "journalctl -xeu sshd.service" for details.
```

```
[seokhyun@localhost ~]$ journalctl -xeu sshd.service
A start job for unit sshd.service has finished with a failure.

The job identifier is 5224 and the job result is failed.
Aug 11 19:15:41 localhost.localdomain systemd[1]: Stopped OpenSSH server daemon.
Subject: A stop job for unit sshd.service has finished
Defined-By: systemd
Support: https://access.redhat.com/support

A stop job for unit sshd.service has finished.

The job identifier is 5330 and the job result is done.
Aug 11 19:18:04 localhost.localdomain systemd[1]: Starting OpenSSH server daemon...
Subject: A start job for unit sshd.service has begun execution
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit sshd.service has begun execution.

The job identifier is 6046.
Aug 11 19:18:04 localhost.localdomain sshd[3787]: Server listening on 0.0.0.0 port 22.
Aug 11 19:18:04 localhost.localdomain sshd[3787]: Server listening on :: port 22.
Aug 11 19:18:04 localhost.localdomain systemd[1]: Started OpenSSH server daemon.
Subject: A start job for unit sshd.service has finished successfully
Defined-By: systemd
Support: https://access.redhat.com/support

A start job for unit sshd.service has finished successfully.

The job identifier is 6046.
```

- service sshd start
- 에러가 발생할 수 있음
  
- journalctl -xeu ssh.service
  - 시스템 로그 조회 가능
  - -x : 로그 메시지에 대한 설명 출력
  - -e : 가장 최근 로그 출력
  - -u [system unit name] : 특정 서비스 로그만 출력

# SSH Installation Trouble Shooting

```
[seokhyun@localhost ~]$ firewall-cmd --permanent --zone=public --add-port=22/tcp
Warning: ALREADY_ENABLED: 22:tcp
success
```

```
[seokhyun@localhost ~]$ firewall-cmd --reload
success
[seokhyun@localhost ~]$ systemctl restart sshd.service
```

```
[seokhyun@localhost ~]$ netstat -tulpn |grep LISTEN
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:22                0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.1:631            0.0.0.0:*        LISTEN     -
tcp6       0      0 :::22                   :::*             LISTEN     -
tcp6       0      0 :::1:631                 :::*             LISTEN     -
```

```
[seokhyun@localhost ~]$ sudo semanage port -l | grep ssh
ssh_port_t                tcp                22
```

- 방화벽에 port number 허용
  - firewall-cmd --permanent --zone=public --add-port=[port number]/tcp
- 방화벽 재시작
  - firewall-cmd --reload
- Port number 허용 확인
  - Netstat -tulpn |grep LISTEN
  - sudo semanage port -l |grep ssh

# SSH Installation Trouble Shooting

```
[seokhyun@localhost ~]$ cat /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#   enforcing - SELinux security policy is enforced.
#   permissive - SELinux prints warnings instead of enforcing.
#   disabled - No SELinux policy is loaded.
# See also:
# https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/changing-selinux-states-
-selinux#changing-selinux-modes-at-boot-time_changing-selinux-states-and-modes
#
# NOTE: Up to RHEL 8 release included, SELINUX=disabled would also
# fully disable SELinux during boot. If you need a system with SELinux
# fully disabled instead of SELinux running with no policy loaded, you
# need to pass selinux=0 to the kernel command line. You can use grubby
# to persistently set the bootloader to boot with selinux=0:
#
#   grubby --update-kernel ALL --args selinux=0
#
# To revert back to SELinux enabled:
#
#   grubby --update-kernel ALL --remove-args selinux
#
SELINUX=disabled
# SELINUX= can take one of these three values:
```

- /etc/selinux/config 확인
- 보안정책 비활성화
- SELINUX = enforcing  
-> SELINUX = disabled

```
[seokhyun@localhost ~]$ ssh seokhyun@172.23. [REDACTED] -p 10621
seokhyun@172.23.[REDACTED]'s password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Aug  9 03:57:38 2024 from [REDACTED]
[seokhyun@localhost ~]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

[seokhyun@localhost ~]$ exit
logout
Connection to 172.23.14.241 closed.
```

- `ssh userID@접속IP -p 포트번호`

Ex) `ssh seokhyun@172.23.xxx.xxx -p 10621`



# SSH Port Number

```
[seokhyun@localhost ~]$ sudo semanage port -l | grep ssh
ssh_port_t                tcp                22
[seokhyun@localhost ~]$ sudo semanage port -a -t ssh_port_t -p tcp 8080
Port tcp/8080 already defined, modifying instead
[seokhyun@localhost ~]$ sudo semanage port -l | grep ssh
ssh_port_t                tcp                8080, 22
```

- ssh가 사용하고 있는 port 확인
  - `sudo semanage port -l | grep ssh`

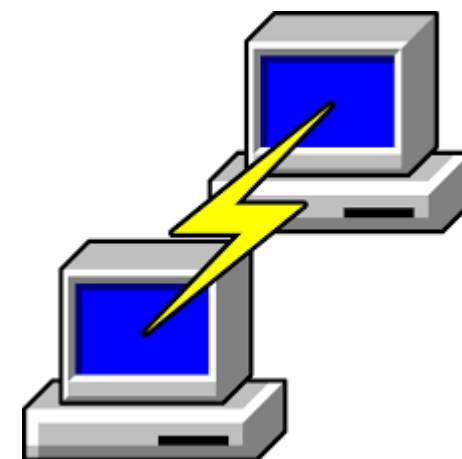
- ssh에 port number 추가하기
  - `sudo semanage port -a -t ssh_port_t -p tcp [port number]`

```
[seokhyun@localhost ~]$ sudo semanage port -d -t 8080 -p tcp 8080
[seokhyun@localhost ~]$ sudo semanage port -l | grep ssh
ssh_port_t                tcp                22
```

- ssh가 사용하는 port 삭제
  - `sudo semanage port -d -t [port number] -p tcp [port number]`

## ❖ Putty

- SSH, Telnet, TCP 접속을 위한 클라이언트
- 윈도우 환경에서 리눅스 서버나 다른 원격 시스템에 접속이 가능
- 오픈 소스이며 사용이 간편하여 많이 사용되는 SSH 클라이언트 중 하나
- <https://www.putty.org/>



## Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm)

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

### putty.exe (the SSH and Telnet client itself)

64-bit x86:	<a href="#">putty.exe</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">putty.exe</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">putty.exe</a>	<a href="#">(signature)</a>

### pscp.exe (an SCP client, i.e. command-line secure file copy)

64-bit x86:	<a href="#">pscp.exe</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">pscp.exe</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">pscp.exe</a>	<a href="#">(signature)</a>

### psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)

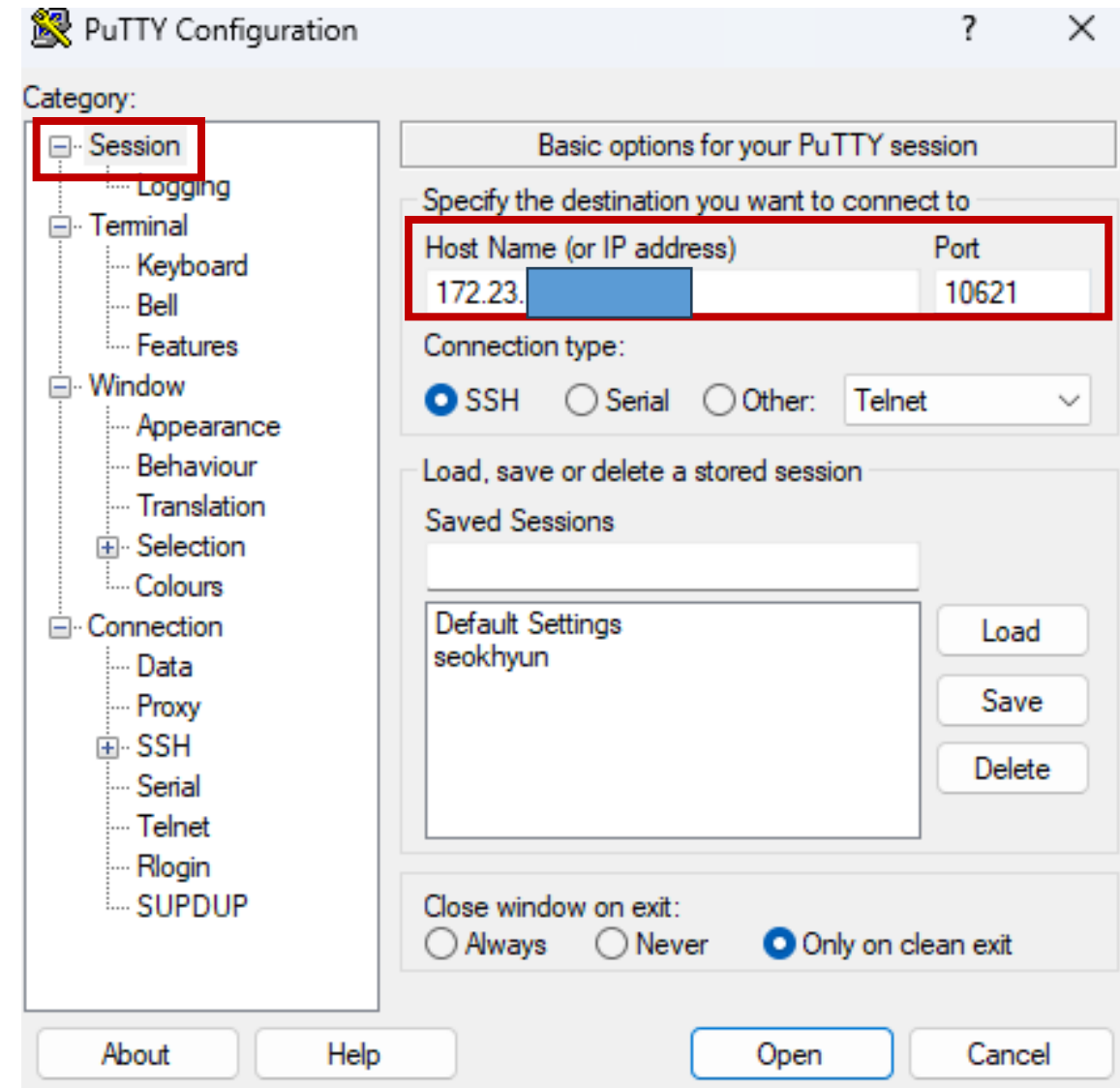
64-bit x86:	<a href="#">psftp.exe</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">psftp.exe</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">psftp.exe</a>	<a href="#">(signature)</a>

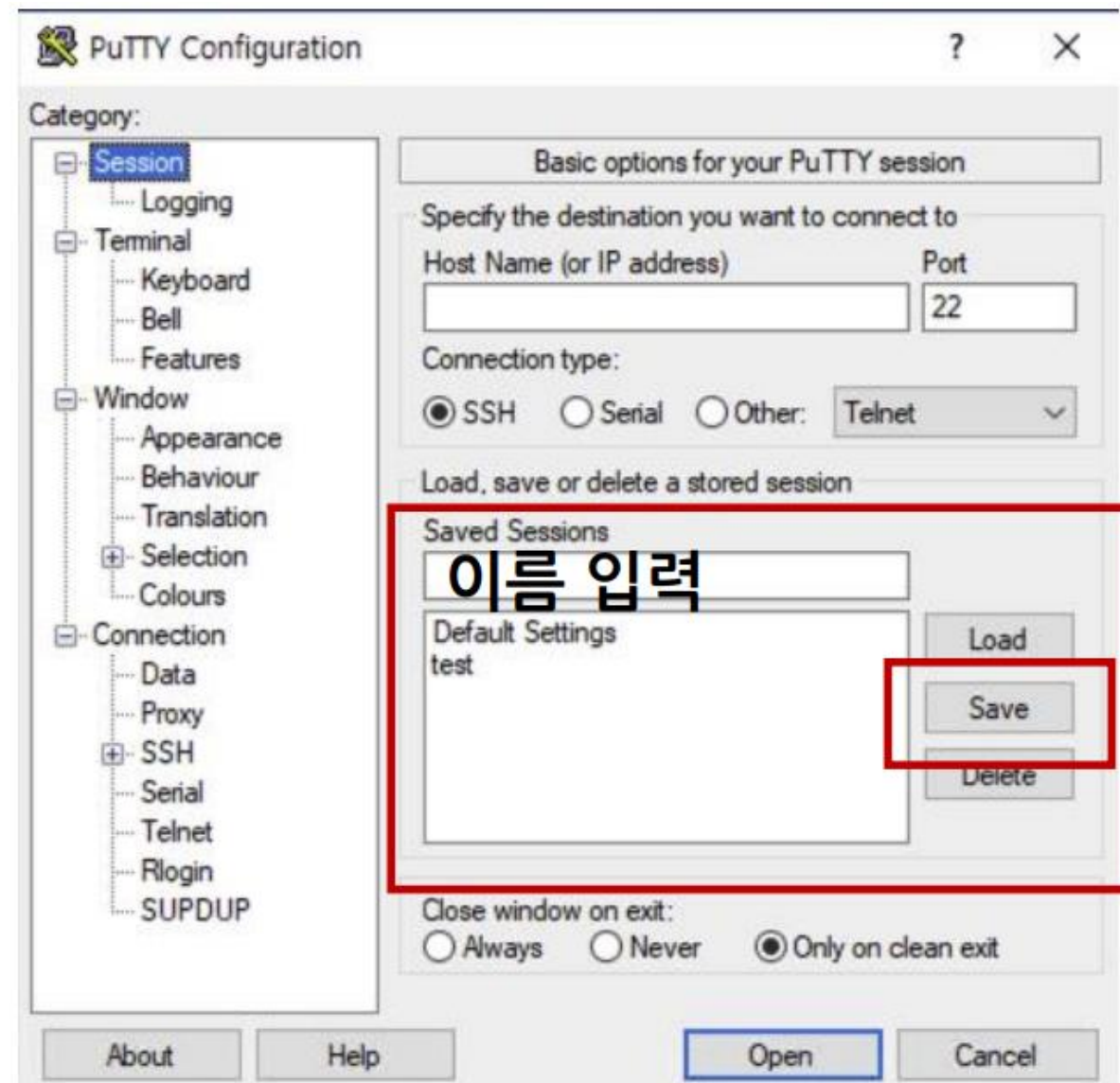
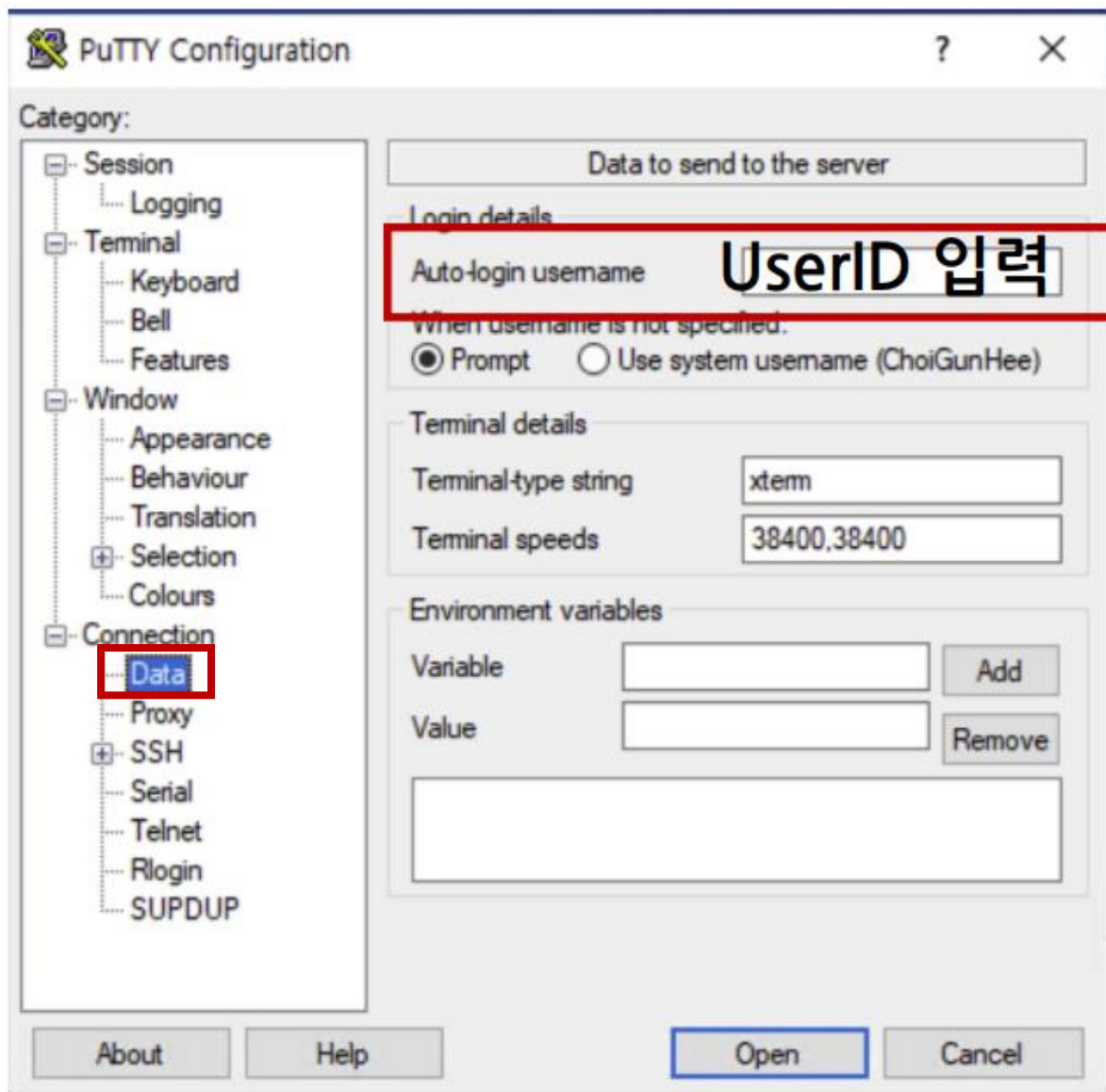
### puttytel.exe (a Telnet-only client)

64-bit x86:	<a href="#">puttytel.exe</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">puttytel.exe</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">puttytel.exe</a>	<a href="#">(signature)</a>

### plink.exe (a command-line interface to the PuTTY back ends)

64-bit x86:	<a href="#">plink.exe</a>	<a href="#">(signature)</a>
64-bit Arm:	<a href="#">plink.exe</a>	<a href="#">(signature)</a>
32-bit x86:	<a href="#">plink.exe</a>	<a href="#">(signature)</a>





```

seokhyun@localhost:~
Using username "seokhyun".
seokhyun@172.23.█'s password:
Activate the web console with: systemctl enable --now cockpit.socket

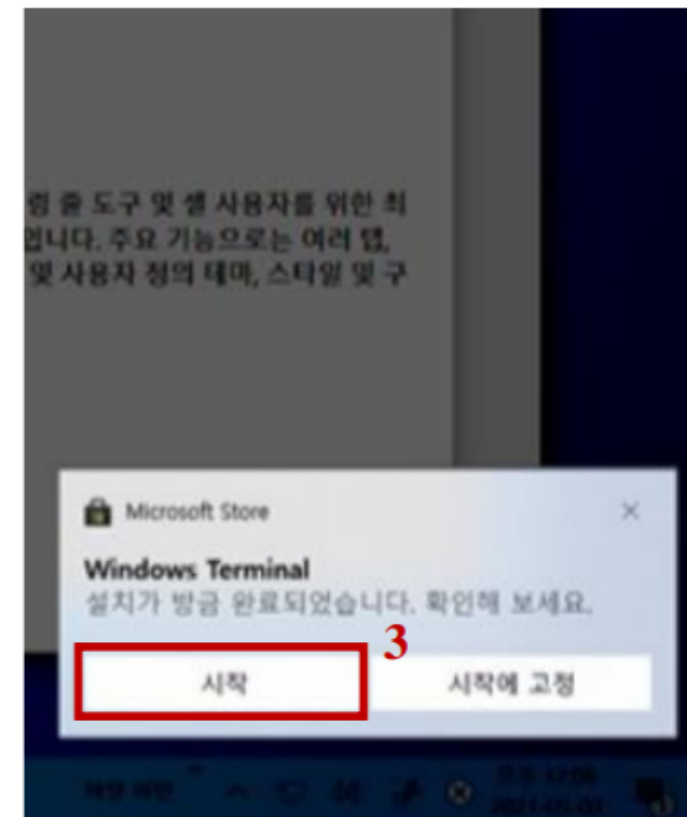
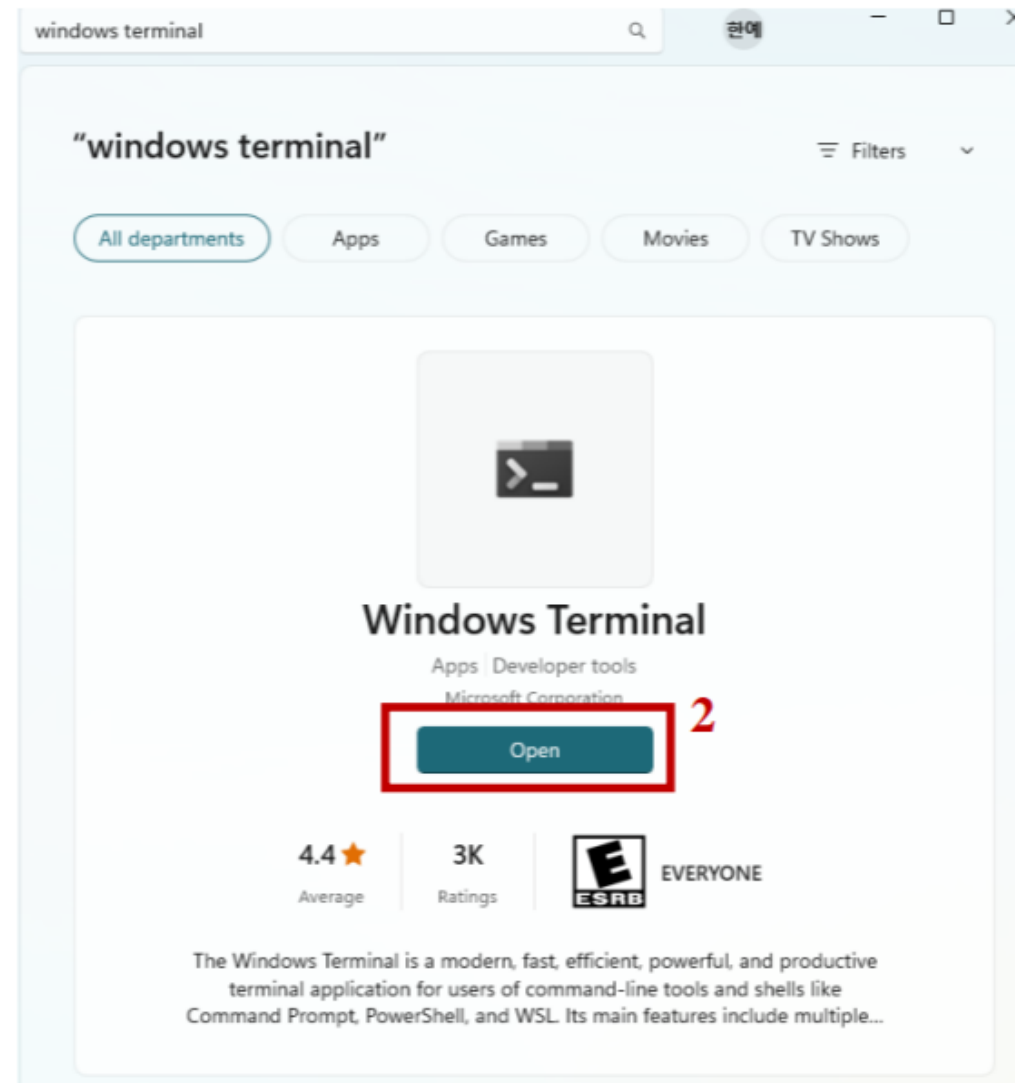
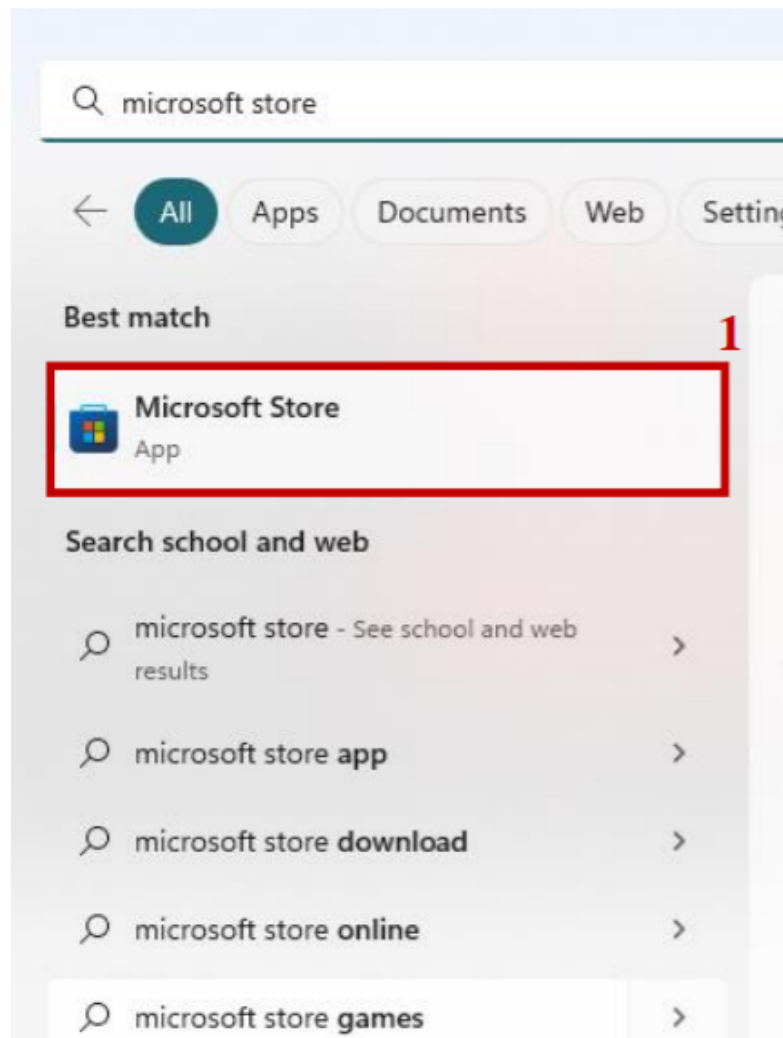
Last login: Sun Aug 11 23:05:28 2024 from 10.0.2.2
[seokhyun@localhost ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe6a:3515  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:6a:35:15  txqueuelen 1000  (Ethernet)
    RX packets 1411  bytes 636200 (621.2 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 1045  bytes 104290 (101.8 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 30  bytes 2880 (2.8 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 30  bytes 2880 (2.8 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
    
```

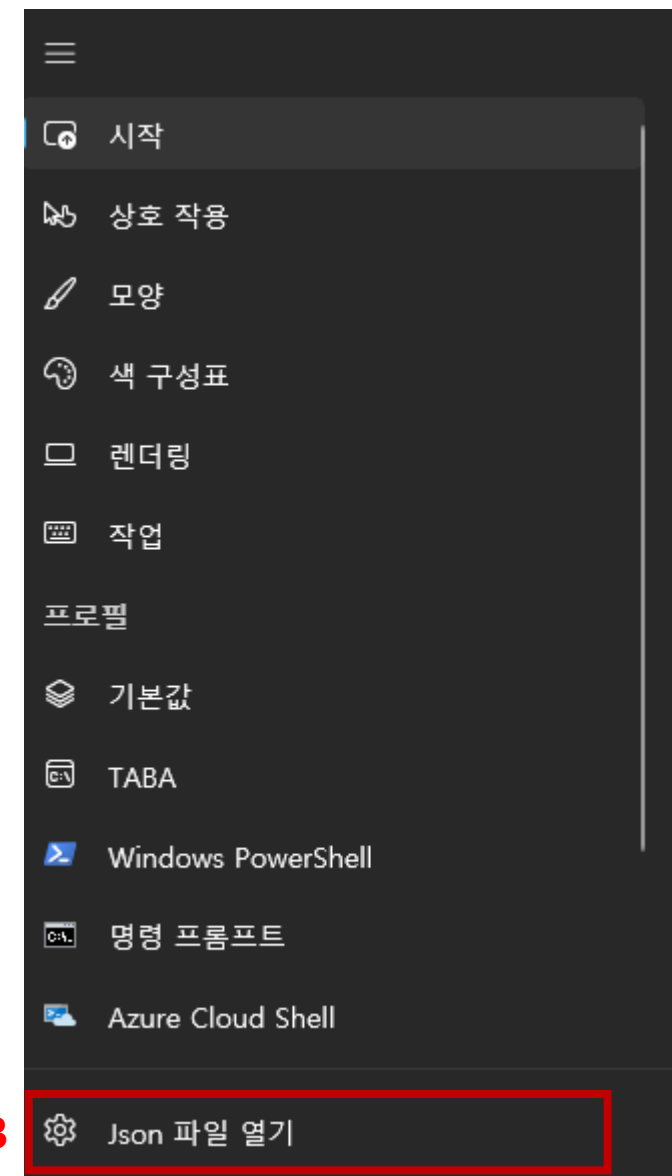
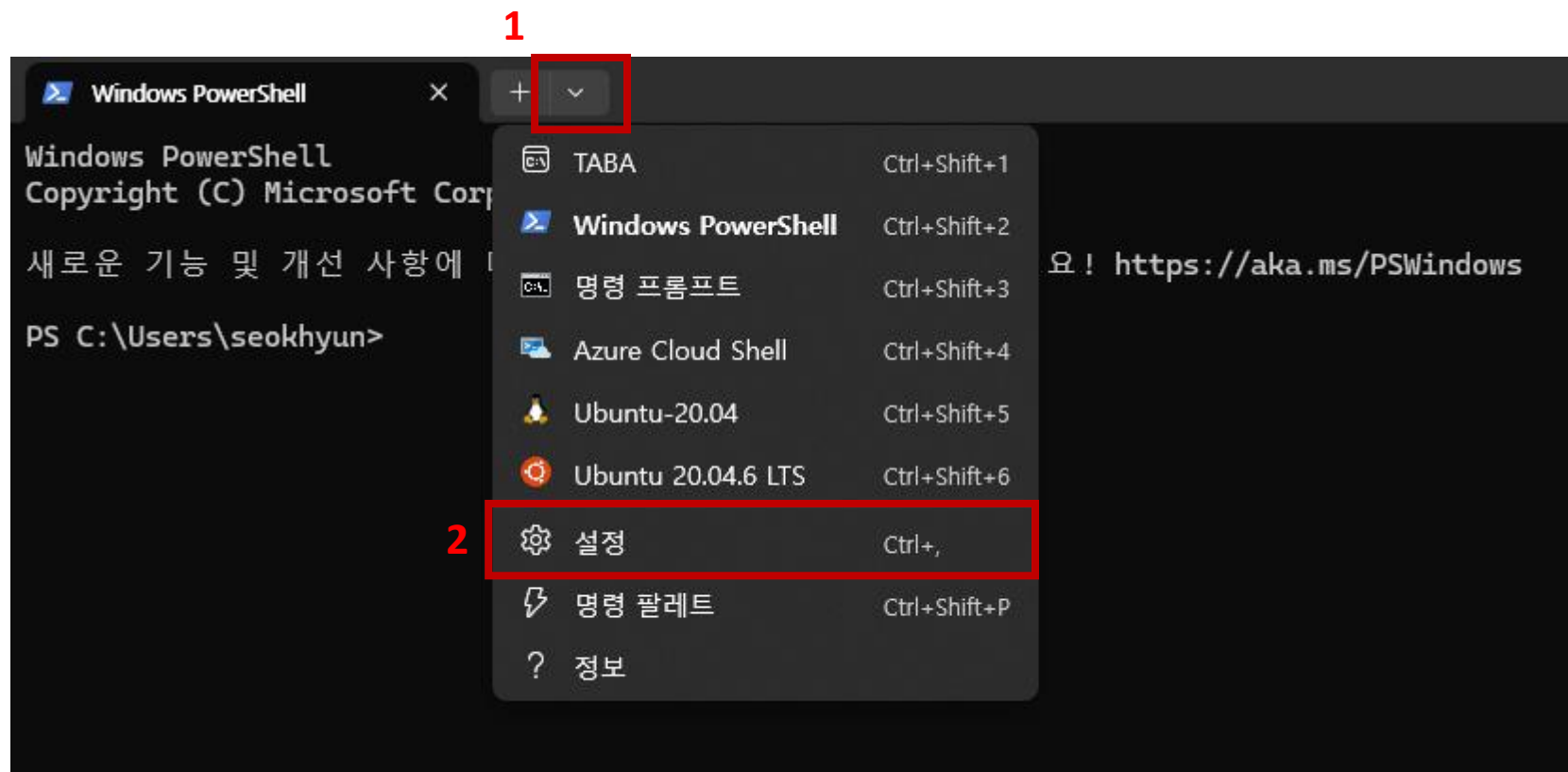
- Password 입력
- 정상적으로 접속이 되었는지 확인을 위해 ip정보 확인



# Window Terminal Installation



# Window Terminal 설정



```
PS C:\Users\seokhyun> [guid]::NewGuid()  
  
Guid  
----  
514611bc-8b02-4abc-ade9-[REDACTED]
```

```
"profiles":  
{  
  "defaults": {},  
  "list":  
  [  
    {  
      "guid" : "{514611bc-8b02-4abc-ade9-[REDACTED]}",  
      "hidden" : false,  
      "name" : "TAB A",  
      "suppressApplicationTitle": true,  
      "commandline": "ssh seokhyun@172.23.[REDACTED]",  
      "cursorShape": "filledBox",  
      "colorScheme": "Tango Dark"  
    },  
  ],  
}
```

- Window powershell
  - [guid]::Newguid()
- commandline
  - 프로필에서 사용되는 실행 파일
  - ex) ssh [seokhyun@172.23.xxx.xxx](#)
- Name
  - 메뉴에 표시될 프로필 이름
  - 시작 시 셸에 전달할 제목으로 사용



# Window Terminal로 접속

```
PS C:\Users\seokhyun> ssh seokhyun@172.23. [redacted]
ssh: connect to host 172.23. [redacted] port 22: Connection refused
```

```
PS C:\Users\seokhyun> ssh -p 10621 seokhyun@172.23. [redacted]
seokhyun@172.23. [redacted]'s password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon Aug 12 00:55:23 2024 from [redacted]
[seokhyun@localhost ~]$
```

- Window powershell
  - ssh name@IP address
  - ex) ssh [seokhyun@172.23.xxx.xxx](#)
  - 기본적으로 22번 포트는 사용하지 않기 때문에 접속이 불가
- ssh -p [port number] cmdline
  - ex) ssh -p 10621 [seokhyun@172.23.xxx.xxx](#)
- 윈도우에서도 ssh를 이용해 접속 가능

```
[seokhyun@localhost ~]$ rpm -qa telnet-server  
[seokhyun@localhost ~]$ rpm -qa | grep telnet
```

- `rpm -qa telnet-server`
- `rpm -qa | grep telnet`
- Rpm -qa [검색할 내용]
  - Red Hat 계열에서 사용되는 패키지 관리 명령어
  - 현재 시스템에 설치된 패키지 목록 조회가 가능

```
[seokhyun@localhost ~]$ sudo yum install telnet-server
```

- `Sudo yum install telnet-server`
- `Sudo yum install telnet*`

```
[seokhyun@localhost ~]$ systemctl start telnet.socket
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'telnet.socket'.
Authenticating as: seokhyun
Password:
==== AUTHENTICATION COMPLETE ====

[seokhyun@localhost ~]$ systemctl enable telnet.socket
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ====
Authentication is required to manage system service or unit files.
Authenticating as: seokhyun
Password:
==== AUTHENTICATION COMPLETE ====

==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: seokhyun
Password:
==== AUTHENTICATION COMPLETE ====
```

```
[seokhyun@localhost ~]$ systemctl status telnet.socket
```

```
● telnet.socket - Telnet Server Activation Socket
```

```
Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; preset: disabled)
```

```
Active: active (listening) since Wed 2024-09-04 03:20:33 KST; 5min ago
```

```
Until: Wed 2024-09-04 03:20:33 KST; 5min ago
```

```
Docs: man:telnetd(8)
```

```
Listen: [::]:23 (Stream)
```

```
Accepted: 0; Connected: 0;
```

```
Tasks: 0 (limit: 23008)
```

```
Memory: 4.0K
```

```
CPU: 430us
```

```
CGroup: /system.slice/telnet.socket
```

```
Sep 04 03:20:33 localhost.localdomain systemd[1]: Listening on Telnet Server Activation Socket.
```

# Telnet – 방화벽 설정

1

```
[root@localhost seokhyun]# firewall-cmd --list-ports  
22/tcp
```

```
[root@localhost seokhyun]# firewall-cmd --add-port=23/tcp --zone=public --permanent  
success
```

```
[seokhyun@localhost home]$ sudo firewall-cmd --permanent --add-service=telnet  
success
```

```
[root@localhost seokhyun]# firewall-cmd --reload  
success  
[root@localhost seokhyun]# firewall-cmd --list-ports  
22/tcp 23/tcp
```

```
[seokhyun@localhost ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 22/tcp 23/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

```
[seokhyun@localhost ~]$ sudo firewall-cmd --state
[sudo] password for seokhyun:
running
[seokhyun@localhost ~]$ systemctl enable firewalld
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ====
Authentication is required to manage system service or unit files.
Authenticating as: seokhyun
Password:
==== AUTHENTICATION COMPLETE ====
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: seokhyun
Password:
==== AUTHENTICATION COMPLETE ====
```

```
[seokhyun@localhost ~]$ sudo useradd teluser  
[seokhyun@localhost ~]$ sudo passwd teluser  
Changing password for user teluser.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

```
[seokhyun@localhost home]$ ls  
seokhyun teluser  
[seokhyun@localhost home]$ cd teluser/  
-bash: cd: teluser/: Permission denied  
[seokhyun@localhost home]$ sudo cd teluser/  
[sudo] password for seokhyun:  
[seokhyun@localhost home]$ ls
```



```
[seokhyun@localhost home]$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.

Kernel 5.14.0-480.el9.x86_64 on an x86_64
localhost login: teluser
Password:
[teluser@localhost ~]$ ls
```

xinetd 서비스가 더 이상 사용되지 않음

xinetd 서비스는 더 이상 사용되지 않으며 RHEL 9에서 제거됩니다. 대체 방법으로 systemd 를 사용합니다. 자세한 내용은 [xinetd 서비스를 systemd로 변환하는 방법을](#) 참조하십시오.