# 2022년도 지방기능경기대회 채점기준(3과제)

## 1. 채점 시 유의사항

| 직 종 명 | 사이버 보안 |
|---|---|

① 채점은 선수의 Guest OS를 모두 power off 한 상태에서 진행하도록 합니다.

② 채점이 시작되면 심사위원의 지시에 따라 선수는 Guest OS를 켜고 대기합니다.

③ 채점 중 선수의 요청에 의해 모든 장비의 재시작과 서비스 재시작은 총 3회로 제한합니다.

④ 모든 채점은 대 소문자를 구분합니다.

⑤ 부분 점수가 인정되는 항목은 별도로 표시되어 있으므로 점수 계산에 차질이 없도록 합니다.

⑥ 채점 시 주어지지 않은 모든 암호는 "Global43@!" 을 사용하도록 합니다.

⑦ 채점 상에서 **빨간색으로 highlight된 부분은 명령어**이며, **파란색으로 highlight된 부분은 참고표시**입니다.

⑧ 모든 채점은 **빨간색 네모칸에 있는 부분만 채점**하도록 합니다.

⑨ 대회장에서 제공되지 않은 소프트웨어가 설치되어 있을 시 부정행위로 간주합니다.

⑩ 과제에 제시되지 않은 설정에 대한 책임은 선수 본인에게 있습니다.

# 2. 채점기준표

## 1) 주요항목별 배점

| 직종명 | 사이버 보안 |
|---|---|

| 과제 번호 | 일련 번호 | 주 요 항 목 | 배 점 | 채점방법 | | 채점시기 | | 비고 |
|---|---|---|---|---|---|---|---|---|
| | | | | 독립 | 합의 | 경기 진행중 | 경기 종료후 | |
| 제3과제 | 1 | 토폴로지 구성 | 6 | | ○ | | ○ | |
| | 2 | 윈도우 시스템 보안 | 5 | | ○ | | ○ | |
| | 3 | 리눅스 시스템 보안 | 12 | | ○ | | ○ | |
| | 4 | 네트워크 보안 | 5 | | ○ | | ○ | |
| | 5 | 어플리케이션 보안 | 12 | | ○ | | ○ | |
| 합 계 | | | 40 | | | | | |

## 2) 채점방법 및 기준

| 과제 번호 | 일련 번호 | 주 요 항 목 | 배점 번호 | 세 부 항 목(채점방법) | 배점 | 비고 |
|---|---|---|---|---|---|---|
| 제3과제 | 1 | 토폴로지 구성 | 1 | 운영체제 설치 및 호스트 네임 확인 | 3 | |
| | | | 2 | TCP/IP 설정 및 통신 상태 확인 | 3 | |
| | 2 | 윈도우 시스템 보안 | 1 | 시스템 보안 정책 | 1 | |
| | | | 2 | 계정 암호 정책 | 2 | |
| | | | 3 | 감사 정책 | 2 | |
| | 3 | 리눅스 시스템 보안 | 1 | 계정 암호 정책 | 2 | |
| | | | 2 | 싱글 모드 접근 보안 | 2 | |
| | | | 3 | 외부 저장매체 접근 보안 | 2 | |
| | | | 4 | sudo 보안 | 2 | |
| | | | 5 | 취약점 점검 스크립트 작성 | 2 | |
| | | | 6 | 로그 백업 | 2 | |
| | 4 | 네트워크 보안 | 1 | ufw 방화벽 구현 | 3 | |
| | | | 2 | 패킷 덤프 분석 | 2 | |
| | 5 | 어플리케이션 보안 | 1 | SSH 서비스 보안 | 3 | |
| | | | 2 | 데이터베이스 보안 | 6 | |
| | | | 3 | 이메일 서비스 보안 | 3 | |
| 합 계 | | | | | 40 | |

| 번호 | 세부 채점 내용 |
|---|---|
| 1 | **▶토폴로지 구성**<br>**1) 운영체제 설치 및 호스트네임 확인 (3점)**<br>HOST-PC에서 cmd 창을 실행하여 **d:** -> **D:\Cyber-비번\호스트네임 폴더**에 접근 한 뒤, **dir** 명령을 실행하여 **아래의 내용과 같은지 확인합니다. (부분점수 0.5)** |


그리고 Adm-PC에 user 계정으로 로그인하여, **실행** -> **cmd 창**을 실행하여 **hostname** 명령을 수행합니다.
**출력 내용이 아래와 동일해야합니다.**

cmd> **hostname**
**Adm-PC** **(부분점수 0.5)**

이어서, GW-SRV에 administrator(gwinadmin) 계정으로 로그인하고 아래와 같이 동일하게 확인하도록 합니다.

cmd> **hostname**
**GW-SRV** **(부분점수 0.5)**

다음은 GR-SRV tty5 세션에 gruser 계정으로 로그인하여 터미널 창을 실행하여 hostname 명령을 수행합니다.
**출력 내용이 아래와 동일해야합니다.**

gruser@GR-SRV:~# **hostname**
**GR-SRV** **(부분점수 0.5)**

이어서 GL-SRV tty1 세션에 gluser 계정으로 로그인하여 동일하게 진행합니다.

gluser@GL-SRV:~# **hostname**
**GL-SRV** **(부분점수 0.5)**

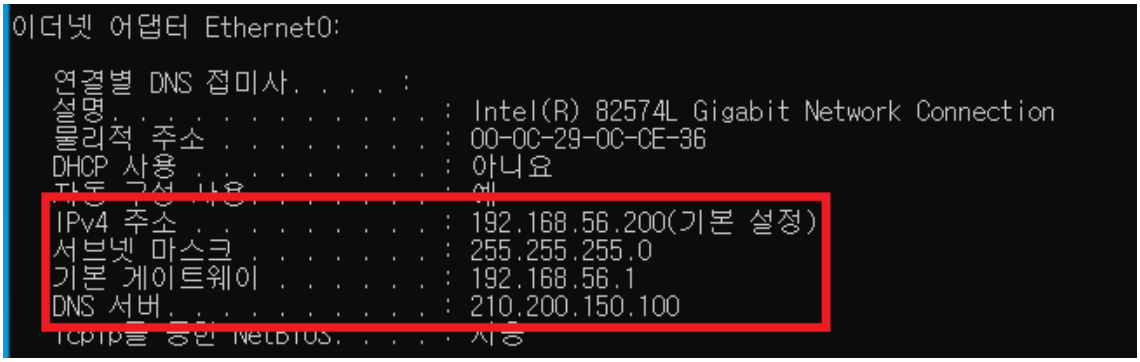
마지막으로 Ext-SRV에 tty5 세션에 user 계정으로 로그인하여 동일하게 진행합니다.

user@Ext-SRV:~# **hostname**
**Ext-SRV** **(부분점수 0.5)**

2) TCP/IP 설정 확인 (1.5점)

Adm-PC에 user 계정으로 로그인하여 cmd 창을 실행하고, 아래와 같이 진행합니다.

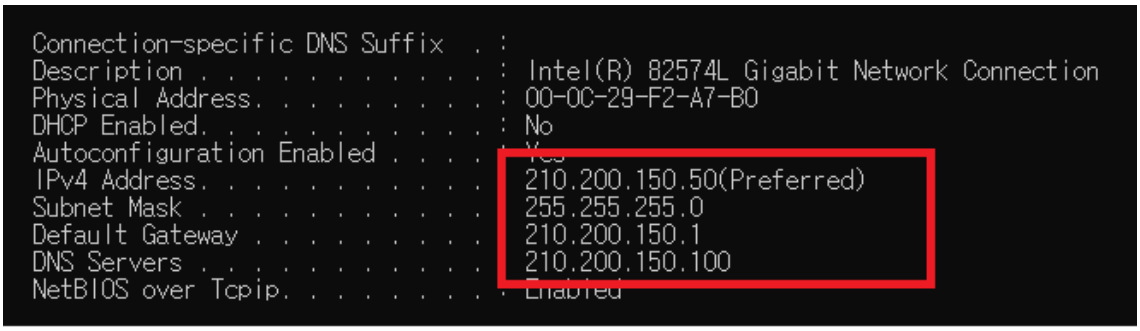
> ipconfig /all




출력 결과가 위와 같아야합니다. (부분점수 0.3)

GW-SRV에 administrator(gwinadmin) 계정으로 로그인하여 cmd 창을 실행하고, 아래와 같이 진행합니다.

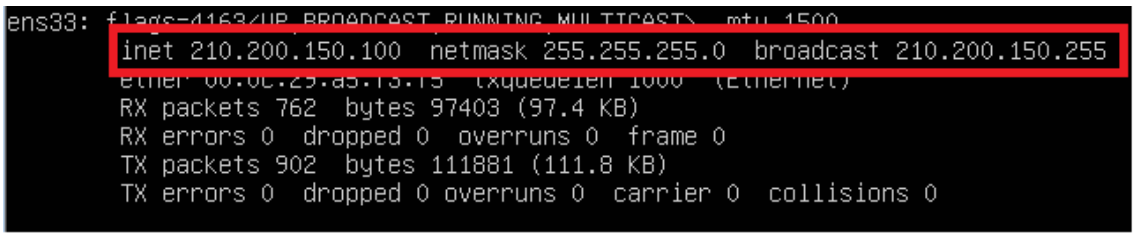
> ipconfig /all



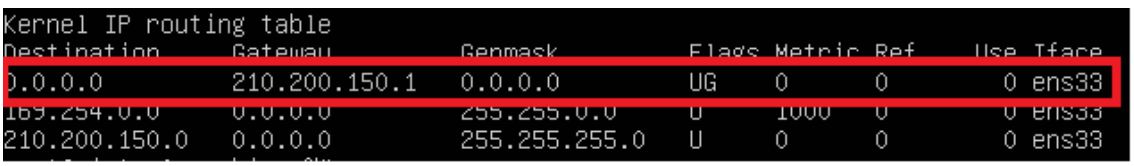

출력 결과가 위와 같아야합니다. (부분점수 0.3)

이어서 GL-SRV tty1 세션에 gluser 계정으로 로그인하여 아래와 같이 진행합니다.

gluser@GL-SRV:~# ifconfig




gluser@GL-SRV:~# route -n




출력 결과가 위와 같아야합니다. (부분점수 0.3)

이어서 GR-SRV tty5 세션에 gruser 계정으로 로그인 한 뒤, 아래와 같이 진행합니다.

gruser@GR-SRV:~# **ifconfig**

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.1  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::20c:29ff:fee8:df2c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:df:2c  txqueuelen 1000  (Ethernet)
        RX packets 363  bytes 29486 (29.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 446  bytes 44525 (44.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 210.200.150.1  netmask 255.255.255.0  broadcast 210.200.150.255
        inet6 fe80::20c:29ff:fee8:df36  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:df:36  txqueuelen 1000  (Ethernet)
        RX packets 448  bytes 50739 (50.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 491  bytes 41728 (41.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens39: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 30.30.30.1  netmask 255.255.255.0  broadcast 30.30.30.255
        inet6 fe80::20c:29ff:fee8:df40  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:df:40  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 146  bytes 14283 (14.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

**출력 결과가 위와 같아야합니다. (부분점수 0.3)**

마지막으로 Ext-SRV tty5 세션에 user 계정으로 로그인 한 뒤, 아래와 같이 진행합니다.

user@Ext-SRV:~# **ifconfig**

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 30.30.30.100  netmask 255.255.255.0  broadcast 30.30.30.255
        inet6 fe80::5bba:7fcc:571a:4456  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:da:92:34  txqueuelen 1000  (Ethernet)
        RX packets 47619  bytes 67404689 (67.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19267  bytes 1310387 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

user@Ext-SRV:~# **route -n**

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         30.30.30.1      0.0.0.0         UG    0      0        0 ens33
30.30.30.0      0.0.0.0         255.255.255.0   U     0      0        0 ens33
30.30.30.0      0.0.0.0         255.255.255.0   U     100    0        0 ens33
```

**출력 결과가 위와 같아야합니다. (부분점수 0.3)**

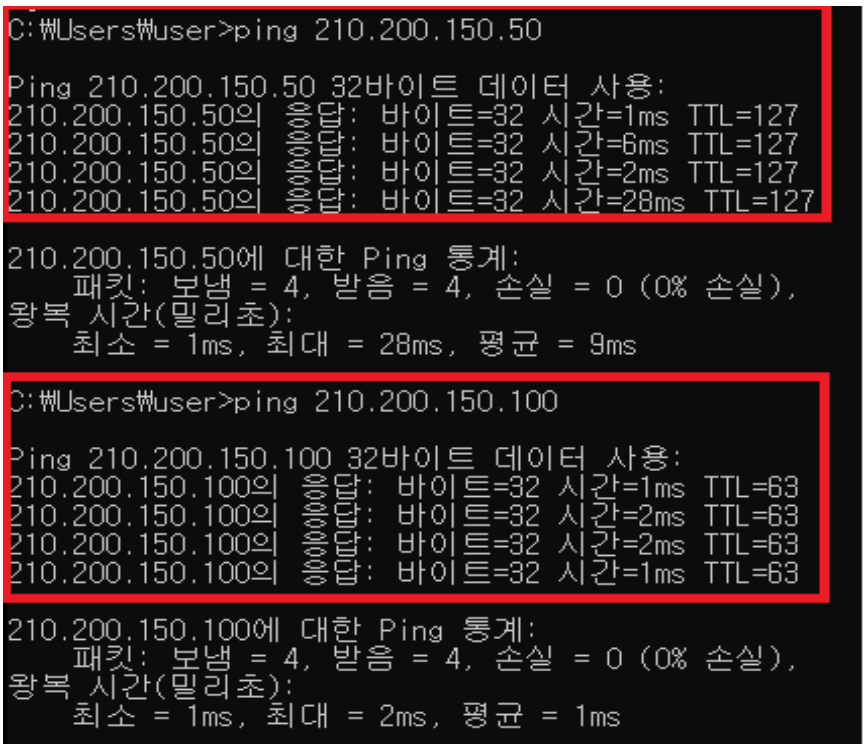
3) 통신 상태 확인 (1.5점)

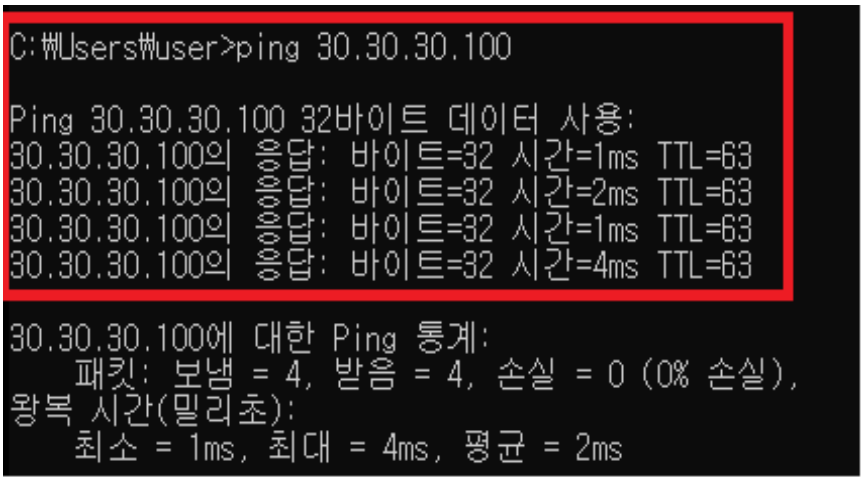
[Adm-PC]

현재 상태에서 Adm-PC로 돌아와 cmd 창을 실행하여 아래의 목적지 주소로 ping 테스트를 진행합니다.

**Destination**: GW-SRV(210.200.150.50), GL-SRV(210.200.150.100), Ext-SRV(30.30.30.100)

<u>아래와 같이 통신이 모두 성공해야합니다.</u>



[GL-SRV]

GL-SRV tty1 세션에 gluser로 로그인하여 터미널 창을 실행하고, 아래의 목적지 주소로 ping 테스트를 진행합니다.

**Destination** : GW-SRV(210.200.150.50), Ext-SRV(30.30.30.100)

**아래와 같이 통신이 모두 성공해야합니다.**

```
gluser@GL-SRV:~$ ping 210.200.150.50
PING 210.200.150.50 (210.200.150.50) 56(84) bytes of data.
64 bytes from 210.200.150.50: icmp_seq=1 ttl=128 time=1.07 ms
64 bytes from 210.200.150.50: icmp_seq=2 ttl=128 time=12.3 ms
64 bytes from 210.200.150.50: icmp_seq=3 ttl=128 time=0.854 ms
64 bytes from 210.200.150.50: icmp_seq=4 ttl=128 time=0.873 ms
64 bytes from 210.200.150.50: icmp_seq=5 ttl=128 time=1.04 ms
^C
--- 210.200.150.50 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4587ms
rtt min/avg/max/mdev = 0.854/3.232/12.316/4.542 ms
gluser@GL-SRV:~$ ping 30.30.30.100
PING 30.30.30.100 (30.30.30.100) 56(84) bytes of data.
64 bytes from 30.30.30.100: icmp_seq=1 ttl=63 time=1.43 ms
64 bytes from 30.30.30.100: icmp_seq=2 ttl=63 time=1.86 ms
64 bytes from 30.30.30.100: icmp_seq=3 ttl=63 time=1.24 ms
64 bytes from 30.30.30.100: icmp_seq=4 ttl=63 time=1.96 ms
64 bytes from 30.30.30.100: icmp_seq=5 ttl=63 time=1.03 ms
^C
--- 30.30.30.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 1.032/1.507/1.966/0.356 ms
```

Terminal

[Ext-SRV]

GL-SRV tty5 세션에 user로 로그인하여 아래의 목적지 주소로 ping 테스트를 진행합니다.

**Destination** : GL-Win(210.200.150.50), GL-Lin(210.200.150.100)

**아래와 같이 통신이 모두 성공해야합니다.**

```
root@Ext-SRV:~# ping 210.200.150.50
PING 210.200.150.50 (210.200.150.50) 56(84) bytes of data.
64 bytes from 210.200.150.50: icmp_seq=1 ttl=127 time=1.47 ms
64 bytes from 210.200.150.50: icmp_seq=2 ttl=127 time=6.55 ms
64 bytes from 210.200.150.50: icmp_seq=3 ttl=127 time=15.9 ms
64 bytes from 210.200.150.50: icmp_seq=4 ttl=127 time=2.81 ms
64 bytes from 210.200.150.50: icmp_seq=5 ttl=127 time=1.65 ms
^C
--- 210.200.150.50 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 1.478/5.697/15.999/5.466 ms
root@Ext-SRV:~# ping 210.200.150.100
PING 210.200.150.100 (210.200.150.100) 56(84) bytes of data.
64 bytes from 210.200.150.100: icmp_seq=1 ttl=63 time=1.02 ms
64 bytes from 210.200.150.100: icmp_seq=2 ttl=63 time=1.37 ms
64 bytes from 210.200.150.100: icmp_seq=3 ttl=63 time=1.03 ms
64 bytes from 210.200.150.100: icmp_seq=4 ttl=63 time=1.28 ms
64 bytes from 210.200.150.100: icmp_seq=5 ttl=63 time=1.34 ms
^C
--- 210.200.150.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.022/1.212/1.379/0.153 ms
root@Ext-SRV:~#
```

2

## ▶윈도우 시스템 보안

### 1) 시스템 보안 정책 (1점)

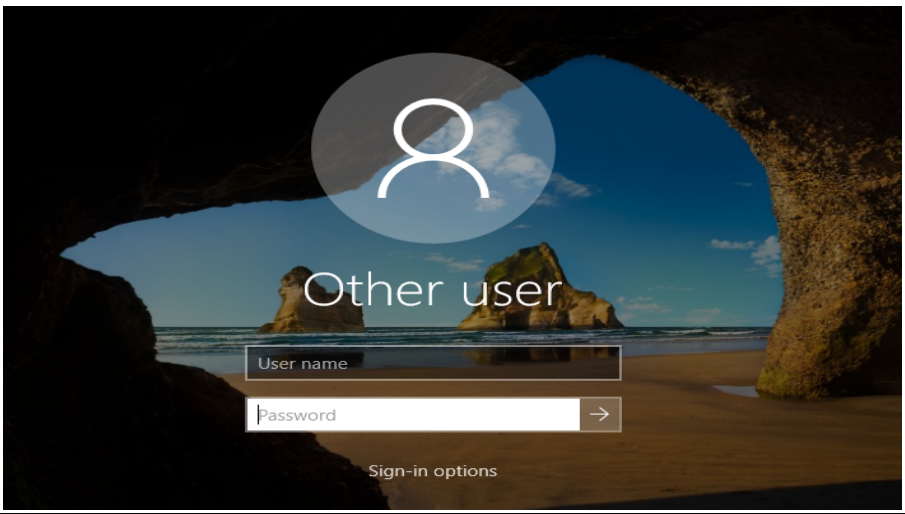
GW-SRV 서버에 administrator(gwinadmin)으로 접속하여 powershell을 실행한 뒤 아래의 명령을 수행합니다.

> net user

```
\\WIN-BNGP7E3GTD9에 대한 사용자 계정

-------------------------------------------------------------------------------
DefaultAccount           Guest                    gwinadmin
gwuser                   WDAGUtilityAccount
명령을 잘 실행했습니다.
```

**출력 결과에 위와 같이 gwinadmin 계정 외 administrator 계정이 존재하지 않아야 합니다.**

그리고 로그아웃을 수행한 뒤, 아래와 같이 마지막 로그인 한 계정의 기록이 존재하지 않는지 확인합니다.




### 2) 계정 암호 정책 (2점)

이어서 powershell을 실행한 뒤 아래의 명령을 수행합니다.

**(Active Directory가 설치되어 있어야만 채점이 가능합니다.)**

> Get-ADDefaultDomainPasswordPolicy

```
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy

ComplexityEnabled           : True
DistinguishedName           : DC=global,DC=com
LockoutDuration             : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold            : 0
MaxPasswordAge              : 60.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 8
objectClass                 : {domainDNS}
objectGuid                  : 4d732994-677d-4784-919d-ca054b968c27
PasswordHistoryCount        : 4
ReversibleEncryptionEnabled : False
```

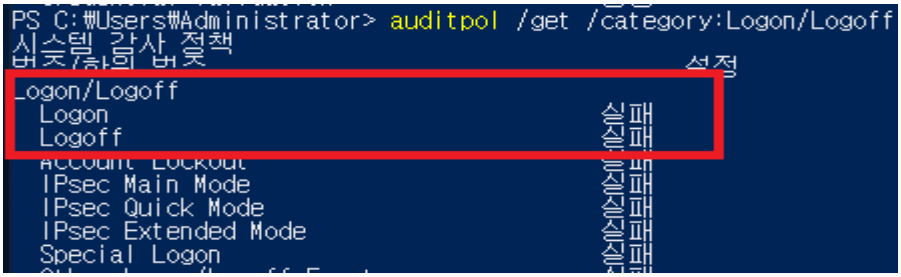
**출력 결과가 빨간색 네모 부분과 같아야합니다.**

### 3) 감사 정책 (2점)

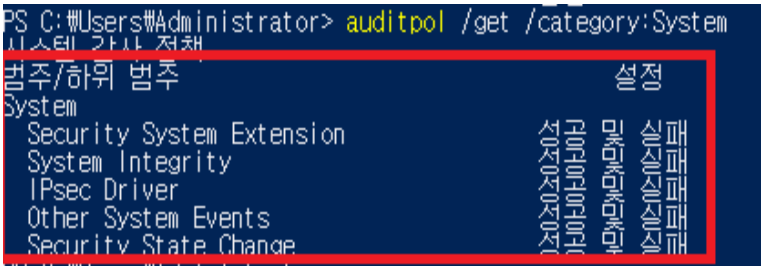
powershell에서 아래의 명령들을 이어서 수행합니다.

(Active Directory가 설치되어 있어야만 채점이 가능합니다.)

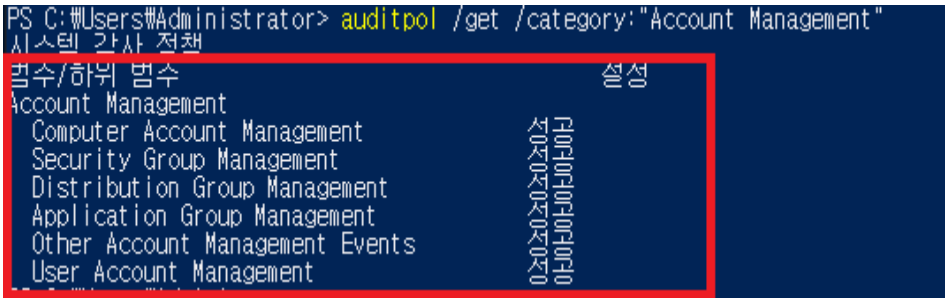
> auditpol /get /category:로그온/로그오프




> auditpol /get /category:시스템




> auditpol /get /category:"계정 관리"




위 3개의 결과 값과 모두 동일해야 정답으로 인정합니다.

## ▶리눅스 시스템 보안

### 1) 계정 암호 정책 (2점)

GL-SRV tty5 세션에 test01 계정으로 로그인하여 터미널 창을 실행합니다.

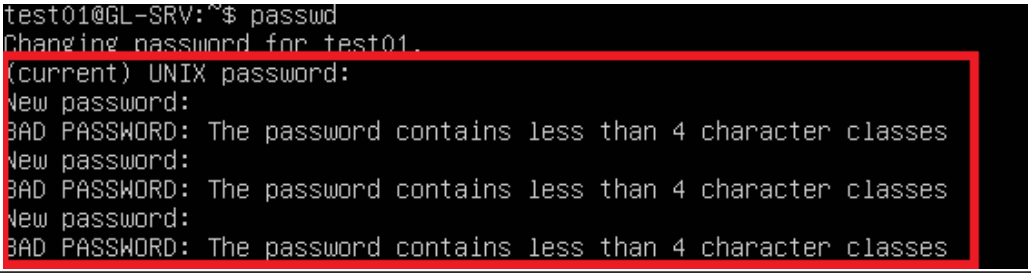
그리고 주어진 패스워드로 순서대로 총 3회의 변경을 시도합니다.

1) cyber123$ 2) Cyber1234 3) Cyber!@#$

3

test01@GL-SRV:~# passwd (부분점수 1점)

아래와 같이 3회 모두 경고 메시지를 출력해야합니다.(출력되는 메시지는 상이할 수 있습니다.)



다시 passwd 명령을 실행한 뒤 Test0112#$로 변경을 시도하여 아래와 같이 출력되는지 확인합니다. (부분점수 0.5점)

```
test01@GL-SRV:~$ passwd
Changing password for test01.
(current) UNIX password:
New password:
BAD PASSWORD: The password contains the user name in some form
```

이어서 su - 명령을 통해 루트 계정으로 접근한 뒤, chage -l test01 명령을 수행하여 **출력 결과가 아래와 동일한지 확인합니다.**

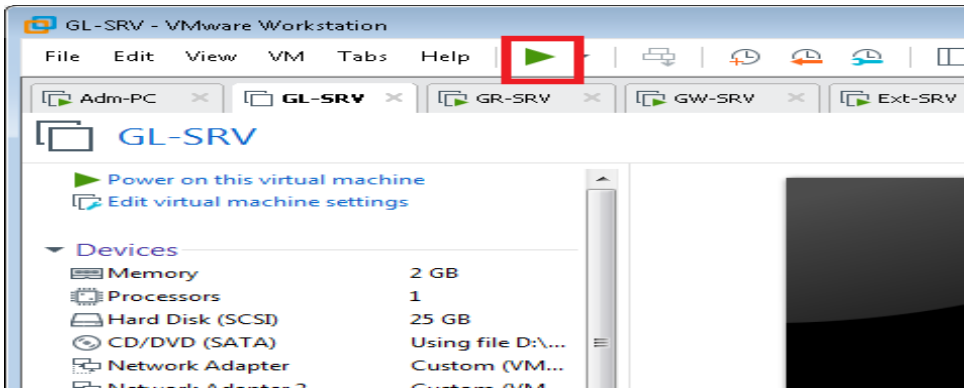
root@GL-SRV:~# chage -l test01 (부분점수 0.5점)

```
Last password change                                    :  5월  16, 2021
Password expires                                        :  7월  15, 2021
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 1
Maximum number of days between password change          : 60
Number of days of warning before password expires       : 7
```

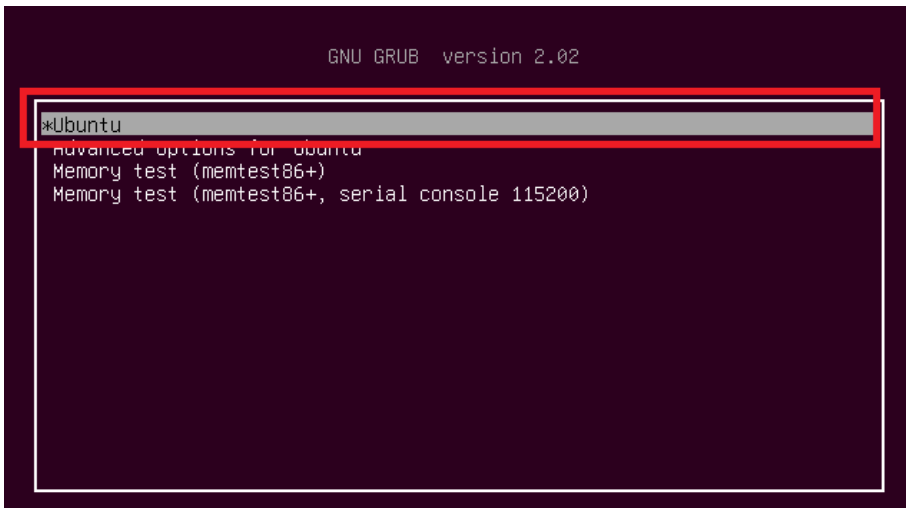
## 2) 싱글 모드 접근 보안 (2점)

root 계정으로 poweroff 명령을 수행하여 GL-SRV를 완전히 종료합니다.

종료된 머신을 다시 시작하면서 L-SHIFT 버튼을 계속 클릭합니다.

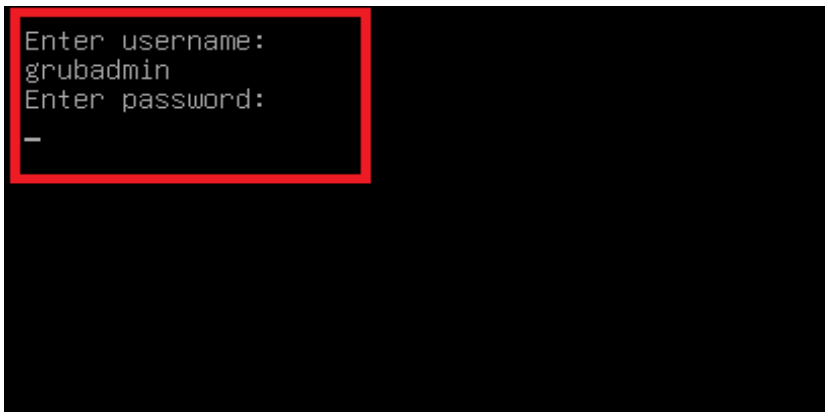



아래와 같이 GRUB 부트 메뉴 화면이 나타나면, **e키를 입력하여 편집 모드로 진입합니다.**




(부트 메뉴 화면이 나타나기전에 프롬프트가 출력되는 경우 오답으로 처리)

Enter username: 프롬프트가 출력되는지 확인하며, grubadmin/Global43@!로 인증을 수행합니다.

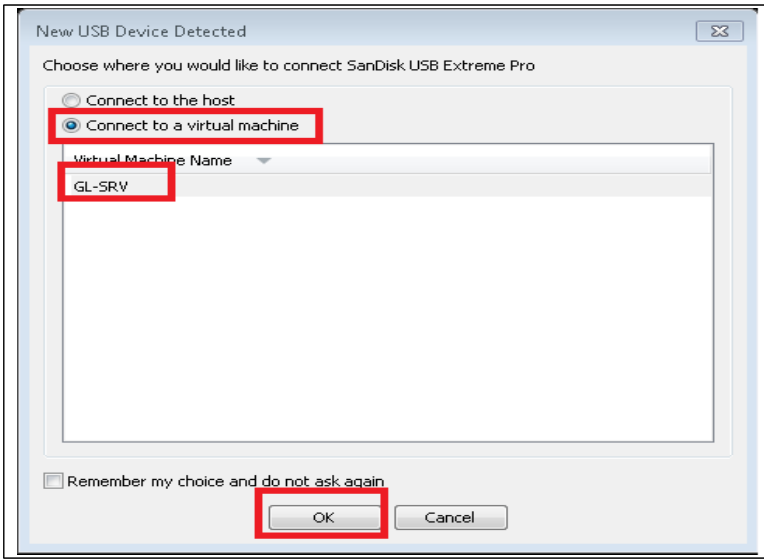



인증이 정상적으로 수행되었다면, 아래와 같이 정상적으로 GRUB 편집 모드에 진입이 가능해야 합니다.


채점이 끝났다면, 다음 채점을 위해 ctrl + x를 입력하여 부팅을 진행하도록 합니다.

### 3) 외부 저장매체 접근 보안 (2점)

각 선수에게 지급된 USB를 PC USB 단자에 연결한 뒤, Connect to a virtual machine을 클릭하여 GL-SRV 서버에 연결시키도록 합니다.



그리고 tty5 root 계정으로 로그인하여 fdisk -l 명령을 수행합니다.

```
Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 29999103 29997056 14.3G 83 Linux
/dev/sda2       29999104 39999487 10000384  4.8G 83 Linux
/dev/sda3       40001534 47998975  7997442  3.8G  5 Extended
/dev/sda5       40001536 43999231  3997696  1.9G 83 Linux
/dev/sda6       44001280 47998975  3997696  1.9G 82 Linux swap / Solaris


Disk /dev/loop8: 65.1 MiB, 68259840 bytes, 133320 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop9: 55.5 MiB, 58142720 bytes, 113560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop10: 2.2 MiB, 2273280 bytes, 4440 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/loop11: 29.9 MiB, 31334400 bytes, 61200 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

위와 같이 /dev/sdb, /dev/sdc.. 등의 블록 장치가 보이지 않아야합니다.

## 4) sudo 보안 (2점)

GL-SRV tty1 세션에 gluser로 로그인하여 커맨드 창을 실행한 뒤, **sudo echo "this is sudo test"** 명령을 수행합니다.

```
gluser@GL-SRV:~$ sudo echo "this is sudo test"
this is sudo test
```

위와 같이 아무런 패스워드 입력 없이, 명령어의 결과가 출력되는 경우는 오답처리 합니다.

logout을 수행하고, **test01 계정**으로 로그인하여 동일한 명령어를 입력했을 때, 아래와 같이 패스워드 입력 후 실행되는지 확인합니다.

```
test01@GL-SRV:~$ sudo echo "this is sudo test"
[sudo] password for test01:
this is sudo test
```

결과가 동일하다면, 다시 **sudo systemctl status bind9** 명령을 입력합니다.

**(대회장에서 명령어는 과제에 제시된 범위내에서 심사위원 재량으로 변경될 수 있습니다.)**

```
test01@GL-SRV:~$ sudo systemctl status bind9
Sorry, user test01 is not allowed to execute '/bin/systemctl status bind9' as root on GL-SRV.
```

위와 같이 실행이 거부되어야 합니다.

## 5) 취약점 점검 스크립트 작성 (2점)

tty1 세션에 gluser로 로그인 된 상태에서 su - 명령을 통해 root로 접근합니다.

그리고 아래의 절차대로 진행합니다.

1) /root/check.sh

```
**********************************************************
            시스템 취약점 점검을 실시합니다.
**********************************************************
시작시간 : 2022. 03. 25. (금) 17:07:29 KST

01. /etc/passwd 파일 권한 점검
  ===> [양호] 현재 권한 : -rw-r--r--

02. 라우팅 기능 활성화 여부 점검
  ===> [양호] 라우팅 기능이 비활성화 되어 있습니다.

03. SetUID, SetGID, Sticky bit 파일을 검색하여 저장합니다. 저장 위치는 /root/fi
les.txt 입니다.
```

위와 같이 실행 결과의 1, 2 항목이 모두 [양호]로 표시되어야 하며, 3번 항목의 경우 문구가 동일해야합니다.(단, 내용은 동일하나 단순 오타의 경우 정답으로 인정합니다.)
출력이 정상적으로 확인되었다면, 이번엔 시스템의 일부 값을 변경하고 스크립트를 실행하도록 합니다.

2) rm /etc/rootkit /root/flist.txt
3) chmod 645 /etc/passwd
4) echo "1" > /proc/sys/net/ipv4/ip_forward
5) touch /etc/rootkit ; chmod 4777 /etc/rootkit
6) /root/check.sh

```
**********************************************************
            시스템 취약점 점검을 실시합니다.
**********************************************************
시작시간 : 2022. 03. 25. (금) 17:28:08 KST

01. /etc/passwd 파일 권한 점검
  ===> [취약] 현재 권한 : -rw-r--r-x

02. 라우팅 기능 활성화 여부 점검
 ===> [취약] 라우팅 기능이 활성화되어 있습니다.

03. SetUID, SetGID, Sticky bit 파일을 검색하여 저장합니다. 저장 위치는 /root/fi
les.txt 입니다.
```

위와 같이 실행 결과의 1, 2 항목이 모두 [취약]으로 표시되어야 합니다.

7) cat /root/flist.txt | grep rootkit

```
root@GL-SRV:~# cat /root/flist.txt | grep rootkit
/etc/rootkit
```

위와 같이 rootkit 파일이 검출 되는지 확인합니다.

### 6) 로그 백업 (2점)

tty1 세션에 gluser로 로그인 된 상태에서 su - 명령을 통해 root로 접근합니다.

그리고 아래의 절차대로 진행합니다.

1) /root/backup.sh => full backup 진행
2) ls /backup => backup이 정상적으로 수행되었는지 확인

```
root@GL-SRV:~# ls /backup/
2021-05-04-16:51:40-log.tar.gz  list
```

3) touch /var/log/new1.log /var/log/new2.log
4) /root/backup.sh => Incremental backup 진행
5) ls /backup

```
root@GL-SRV:~# ls /backup/
2021-05-04-16:51:40-log.tar.gz  2021-05-04-16:53:23-log.tar.gz  list
```

6) gzip -dc /backup/2021-05-04-16:53:23-log.tar.gz | tar -tvf - | grep new*
(파일명은 상이할 수 있으며, 마지막에 생성된 파일의 이름으로 지정합니다.)

```
root@GL-SRV:~# gzip -dc /backup/2021-05-04-16:53:23-log.tar.gz | tar -tvf - | g
rep new*
-rw-r--r-- root/root         0 2021-05-04 16:53 var/log/new1.log
-rw-r--r-- root/root         0 2021-05-04 16:53 var/log/new2.log
```

7) gzip -dc /backup/2021-05-04-16:53:23-log.tar.gz | tar -tvf - | grep lastlog
아무런 출력도 없어야합니다.

## ▶네트워크 보안

### 1) ufw 방화벽 구현 (3점)

GR-SRV 서버 tty5에 root 계정으로 로그인하여 아래의 명령을 수행합니다.

root@GR-SRV:~# ufw status

```
root@GR-SRV:~# ufw status
Status: active
```

4 위와 같이 ufw가 활성화 된 경우에만 계속해서 채점을 진행합니다.

아래와 같은 절차대로 방화벽 테스트를 진행합니다.

1) Private -> ServerFarm (부분점수 1.5점)
Adm-PC에 user 계정으로 로그인하여 cmd창을 실행한 뒤, 아래와 같이 nslookup 명령을 수행합니다.
> nslookup global.com

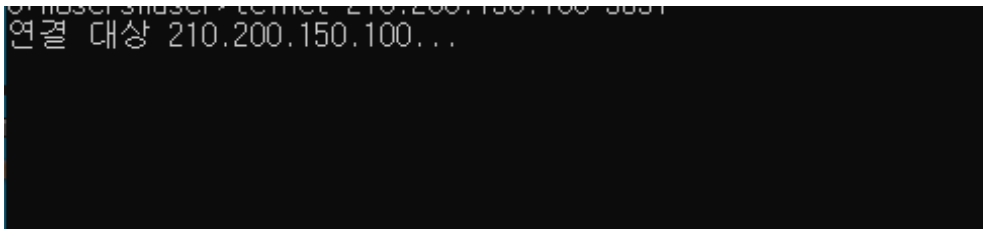
```
C:₩Users₩user>nslookup
기본 서버:  GL-SRV.global.com
Address:  210.200.150.100

> global.com
서버:    GL-SRV.global.com
Address:  210.200.150.100

이름:    global.com
Address:  210.200.150.100

> _
```

위와 같이 정상적으로 질의가 가능해야합니다.

이후 telnet 명령을 통해 Adm-PC -> GL-SRV으로 tcp 22(SSH), tcp 80(HTTP), tcp 143(IMAP), tcp 1106(PostgreSQL) 접속이 모두 성공해야합니다.

> telnet 210.200.150.100 80
> telnet 210.200.150.100 22
> telnet 210.200.150.100 143
> telnet 210.200.150.100 11106
> telnet 210.200.150.50 389


**(접속 성공시의 화면)** 위 화면에서 아무키나 누르고 엔터를 입력하여 빠져나오도록 합니다.




**(접속 실패시의 화면)**

반면 아래의 접속은 모두 실패해야합니다.

> telnet 210.200.150.100 631
> telnet 210.200.150.50 445

```
C:₩Users₩user>telnet 210.200.150.100 631
연결 대상 210.200.150.100...호스트에 연결할 수 없습니다. 포트 631: 연결하지 못했습니다.

C:₩Users₩user>
C:₩Users₩user>telnet 210.200.150.50 445
연결 대상 210.200.150.50...호스트에 연결할 수 없습니다. 포트 445: 연결하지 못했습니다.
```

2) Ext-SRV -> Private, ServerFarm **(부분점수 0.5점)**

Ext-SRV tty5 세션에 root로 로그인한 뒤 아래와 같이 nc 명령을 수행합니다.

> nc -zv 210.200.150.100 53

> nc -zv 210.200.150.100 22

> nc -zv 210.200.150.100 80

**3개의 명령 모두 아래와 같이 아무런 출력 메시지가 보이지 않아야합니다.**

```
root@Ext-SRV:~# nc -zv 210.200.150.100 53
```

**(5초이내에 응답이 없으면 ctrl + c로 빠져나와 다음 커맨드를 입력합니다.)**

3) ServerFarm-> Private **(부분점수 1점)**

GL-SRV tty5 세션에 root로 로그인한 뒤 아래와 같이 nc 명령을 수행합니다.

> nc -zv 192.168.56.200 135

> nc -zv 192.168.56.200 445

**2개의 명령 모두 아래와 같이 아무런 출력 메시지가 보이지 않아야합니다.**

```
root@GL-SRV:~# nc -zv 192.168.56.200 135
```

> nc -zv 192.168.56.200 5040

```
root@GL-SRV:~# nc -zv 192.168.56.200 5040
Connection to 192.168.56.200 5040 port [tcp/*] succeeded!
```

**well-known port 범위가 아닌 5040 포트는 위와 같이 접속이 성공해야합니다.**

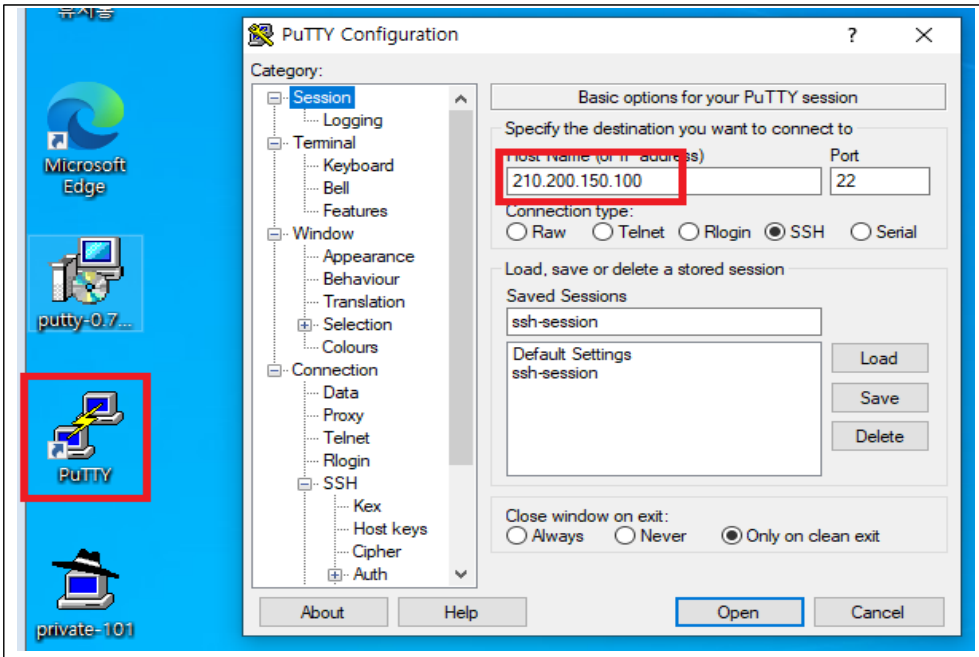
## 2) 패킷 덤프 분석 (2점)

채점기준표 공개로 답이 공개될 수 있는 항목이므로 비공개

## ▶어플리케이션 보안

### 1) SSH 서비스 보안 (3점)

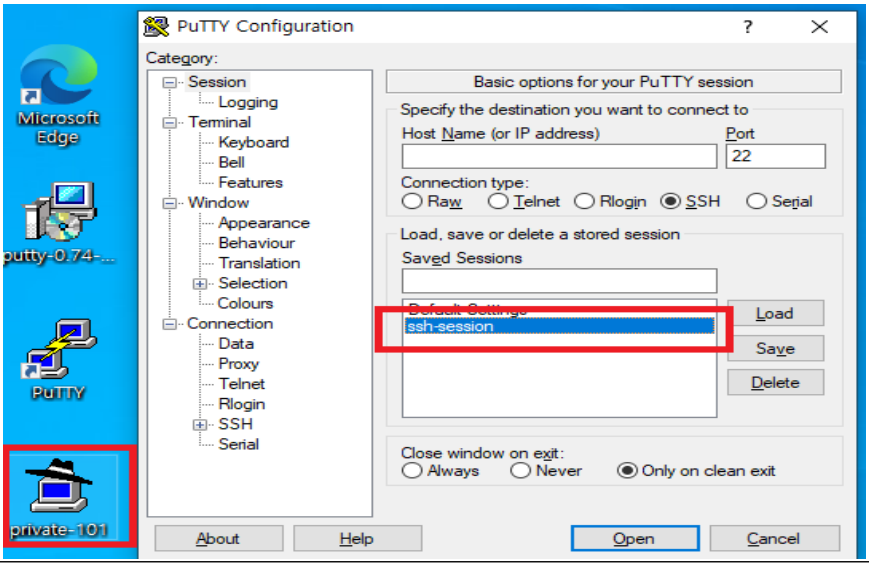
Adm-PC에 user계정으로 접속하여 Putty 프로그램을 실행하고, GL-SRV(210.200.150.100)에 SSH로 접속합니다.



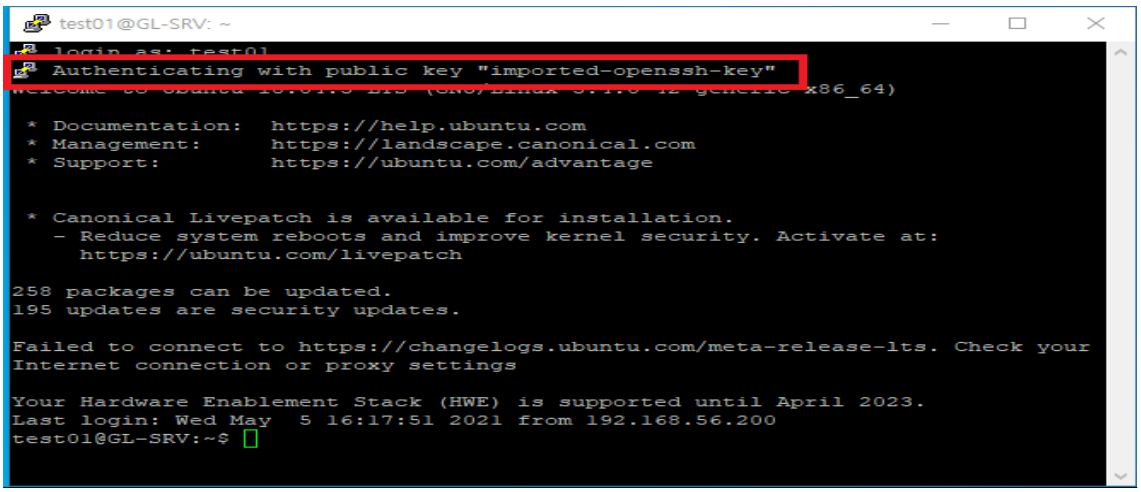

1) **root 계정**을 통해 로그인을 시도합니다.


**위와 같이 접근이 거부 되어야합니다. (부분점수 1점)**

2) 다음은 바탕화면에 **private-[비번호].ppk 파일이 존재하는지 확인하고** putty에 미리 저장해놓은 세션을 통해 **test01 계정**으로 로그인을 시도합니다.




아래와 같이 비밀번호 입력 없이 접속이 가능해야합니다. (부분점수 2점)



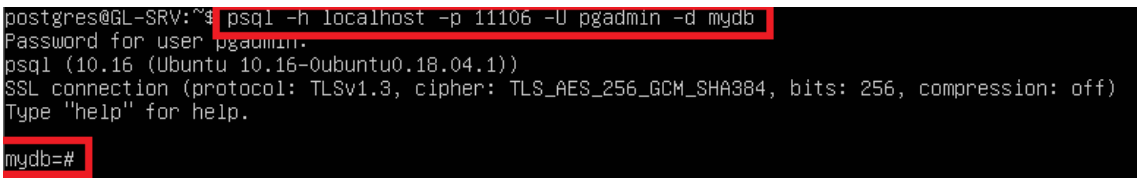

## 2) 데이터베이스 보안 (6점)

GL-SRV tty2에 root 계정으로 접속한 상태에서, 아래의 절차대로 채점을 진행합니다.

1) pgadmin 계정으로 mydb에 접속을 시도합니다.

root@GL-SRV:~# su - postgres

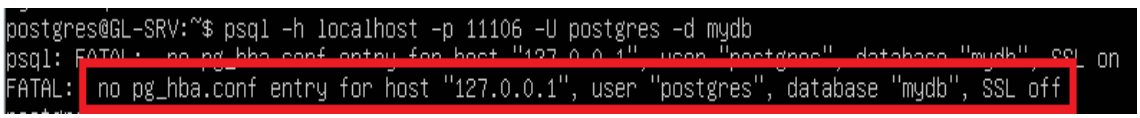
postgres@GL-SRV:~# psql -h localhost -p 11106 -U pgadmin -d mydb




"Global43@!" 패스워드를 입력하면, 위와 같이 정상적으로 DB에 접근이 가능해야합니다. (부분점수 1점)
이후 3)번 채점을 위해 select * from student; 명령을 미리 수행하고, tty2 세션은 그대로 유지합니다.

2) tty3 세션에 root 계정으로 접속 한 뒤, su - postgres 계정으로 다시 전환하여 mydb에 접근을 시도합니다.

postgres@GL-SRV:~# psql -h localhost -p 11106 -U postgres -d mydb




위와 같이 접속이 실패해야합니다.(부분점수 1점)
(접속 실패 메시지는 위 메시지와 조금 상이할 수 있습니다.)

3) postgres 계정으로 로그인된 상태에서, 1)번에서 수행한 SQL 관련 로그 파일이 저장되어 있는지 확인합니다.

postgres@GL-SRV:~# cd /var/lib/postgresql/10/main/my_log

postgres@GL-SRV:~# ls

```
postgres@GL-SRV:~/10/main/my_log$ ls
postgresql-2021-05-05_115621.log  postgresql-2021-05-05_145821.log
postgresql-2021-05-05_125321.log  postgresql-2021-05-05_165821.log
```

(로그 파일의 개수는 채점과 관계 없습니다.)

그리고 이 중 가장 최신 로그 파일을 조회하도록 합니다.

postgres@GL-SRV:~# cat postgresql-2021-05-05_165821.log | grep select

```
postgres@GL-SRV:~/10/main/my_log$ cat postgresql-2021-05-05_165821.log | grep select
2021-05-05 16:58:52.613 KST [4991] pgadmin@mydb LOG:  statement: select * from student;
```

위와 같이 select * from SQL 구문이 존재하는지 확인합니다. (로그 기록시간 확인 필요) (부분점수 2점)

4) tty2 세션으로 돌아와서 \dn+ 명령을 수행합니다.

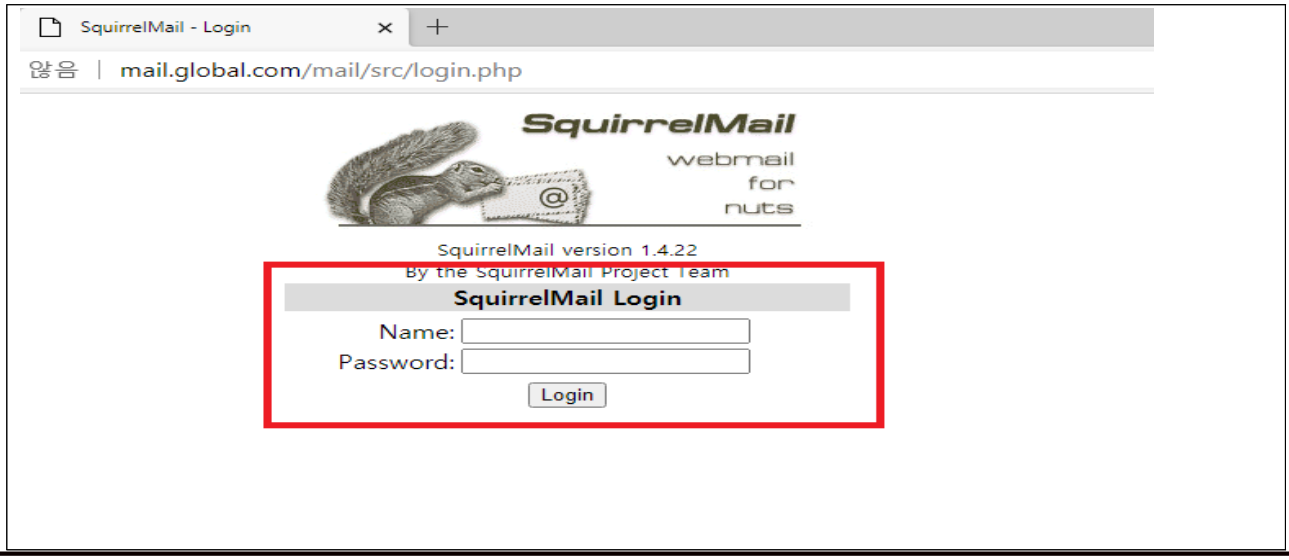
psql> \dn+

```
mydb=# \dn+
                          List of schemas
  Name  |  Owner   |  Access privileges   |      Description
--------+----------+----------------------+------------------------
 public | postgres | postgres=UC/postgres | standard public schema
(1 row)
```

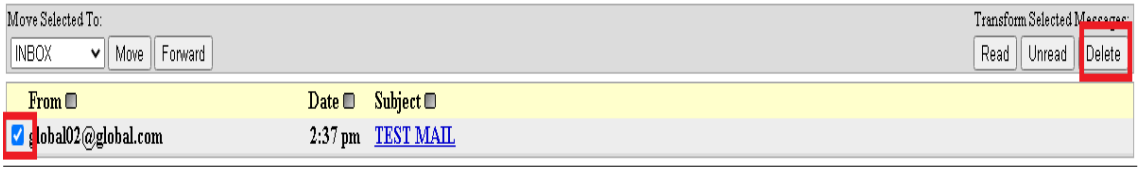
출력 결과가 위와 동일해야합니다. (부분점수 2점)

## 3) 이메일 서비스 보안 (3점)

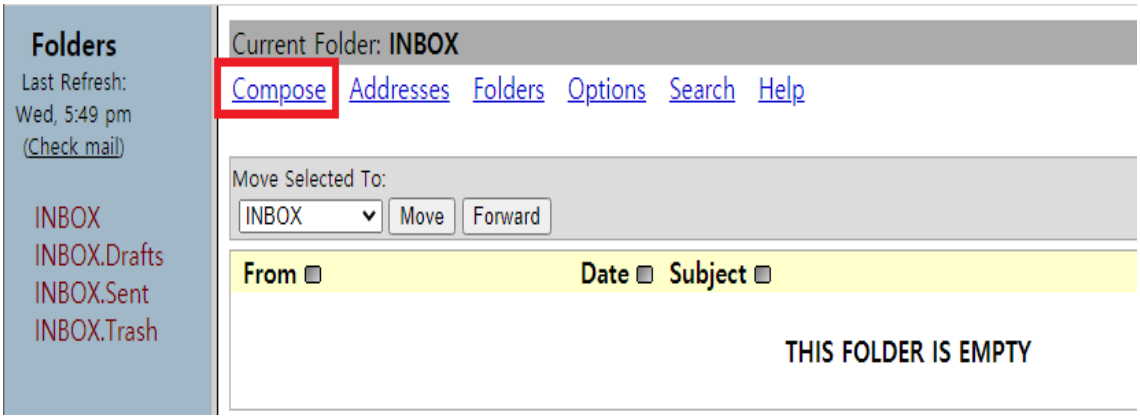
Adm-PC에 user계정으로 접속하여 Microsoft Edge를 실행하여 웹 브라우저를 열고, http://mail.global.com/mail 주소를 입력하여 접속합니다. squirrelmail 화면이 출력되면, **global01 계정으로 로그인합니다.**



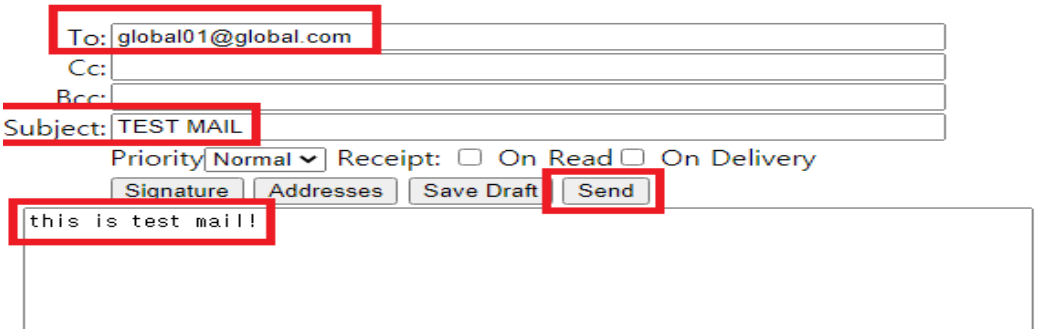
1) **메일함에 있는 모든 메일을 제거하도록 합니다.**



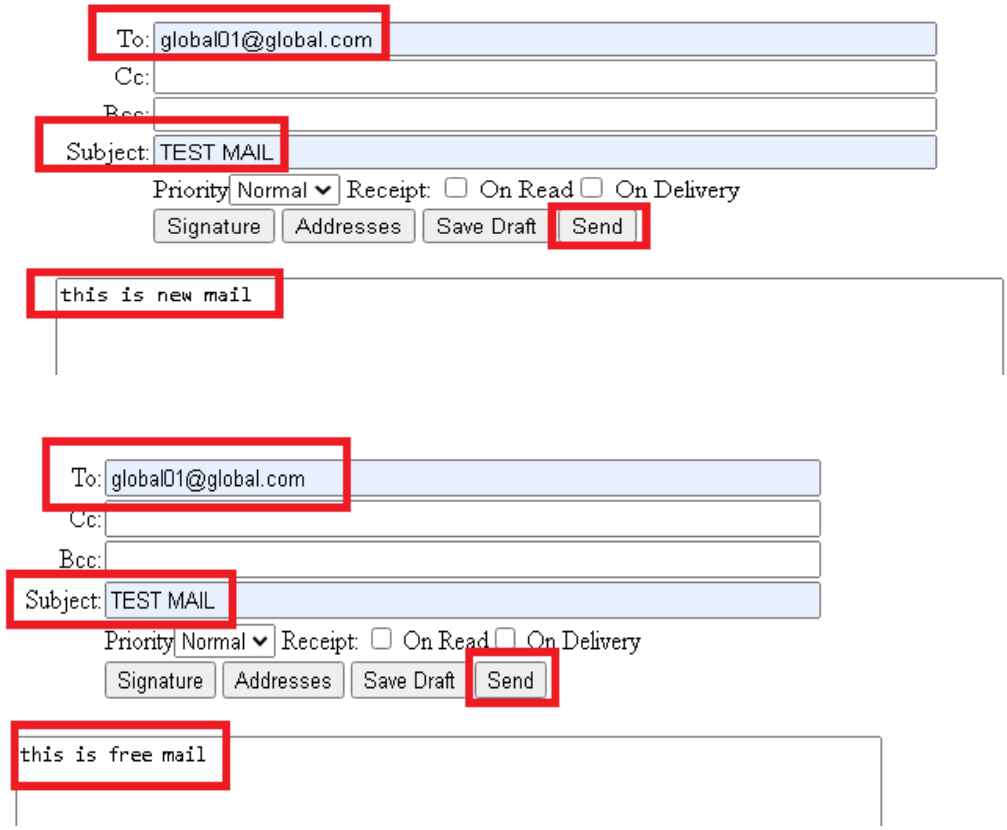

2) 로그아웃 후 global02 계정으로 로그인하여 신규 mail을 작성합니다.



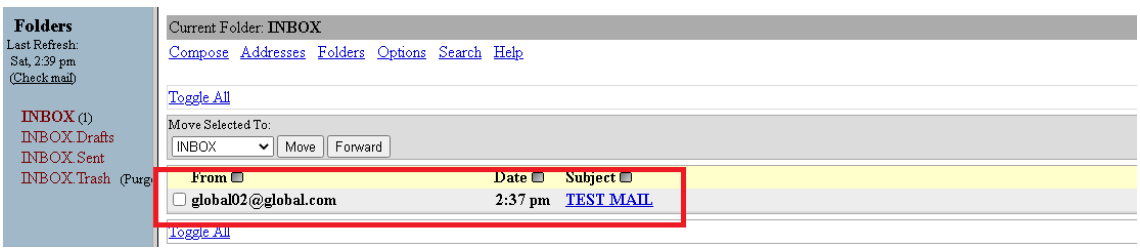

2) 먼저 일반적인 내용의 메일 하나를 작성하여 전송합니다.




3) 다음은 game, new, free의 단어를 포함한 내용의 스팸 메일을 3개를 전송합니다.



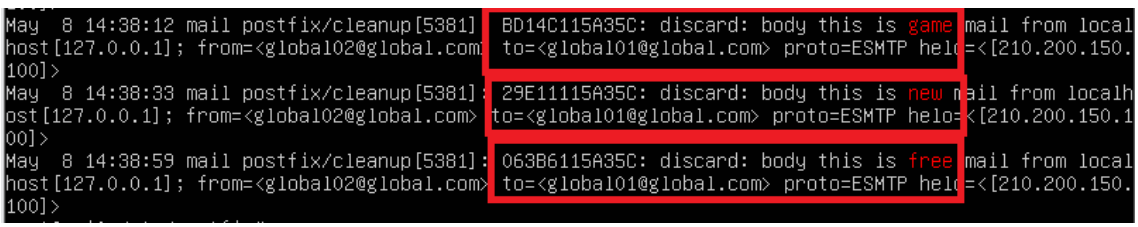

4) 메일을 모두 전송한 뒤, global01 계정으로 다시 로그인하여 수신을 확인합니다.




위와 같이 한 개의 메일만 보여야합니다.

5) GL-SRV tty5 세션에 root 계정으로 로그인 한 뒤 아래의 명령을 수행합니다.

root@GL-SRV:~# cat /var/log/mail.log | grep -E '(game|new|free)'




로그의 내용이 위와 같아야합니다. (단, discard대신 reject로 보여질 수 있음)