가상 네트워크 보안 인프라 구축

지도교수님 - 이병천

팀장 홍성찬

김효성

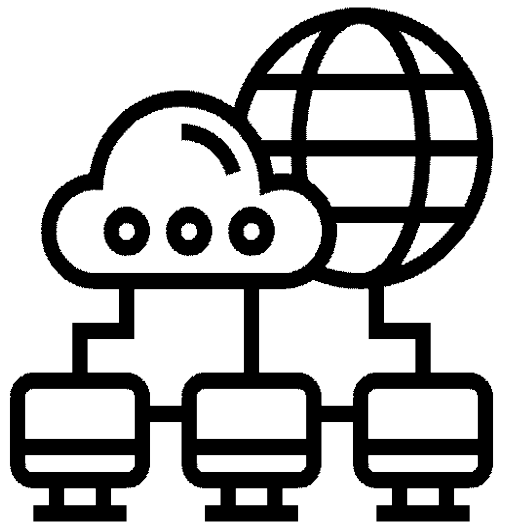
연호준

목차

1.주제 설명

가상의 회사를 기준으로 네트워크 보안 인프라를 구축하고 모의 해킹 및 그에 따른 보안 솔루션을 진행했다.

이때 패킷을 주고 받는 척하는 시뮬레이터인 시스코 패킷 트레이서와 달리 실제 장비의 CPU처리의 결과를 보여주는 GNS3 에뮬레이터를 사용해서 현장과 똑같은 결과를 만들어 볼 수 있다.

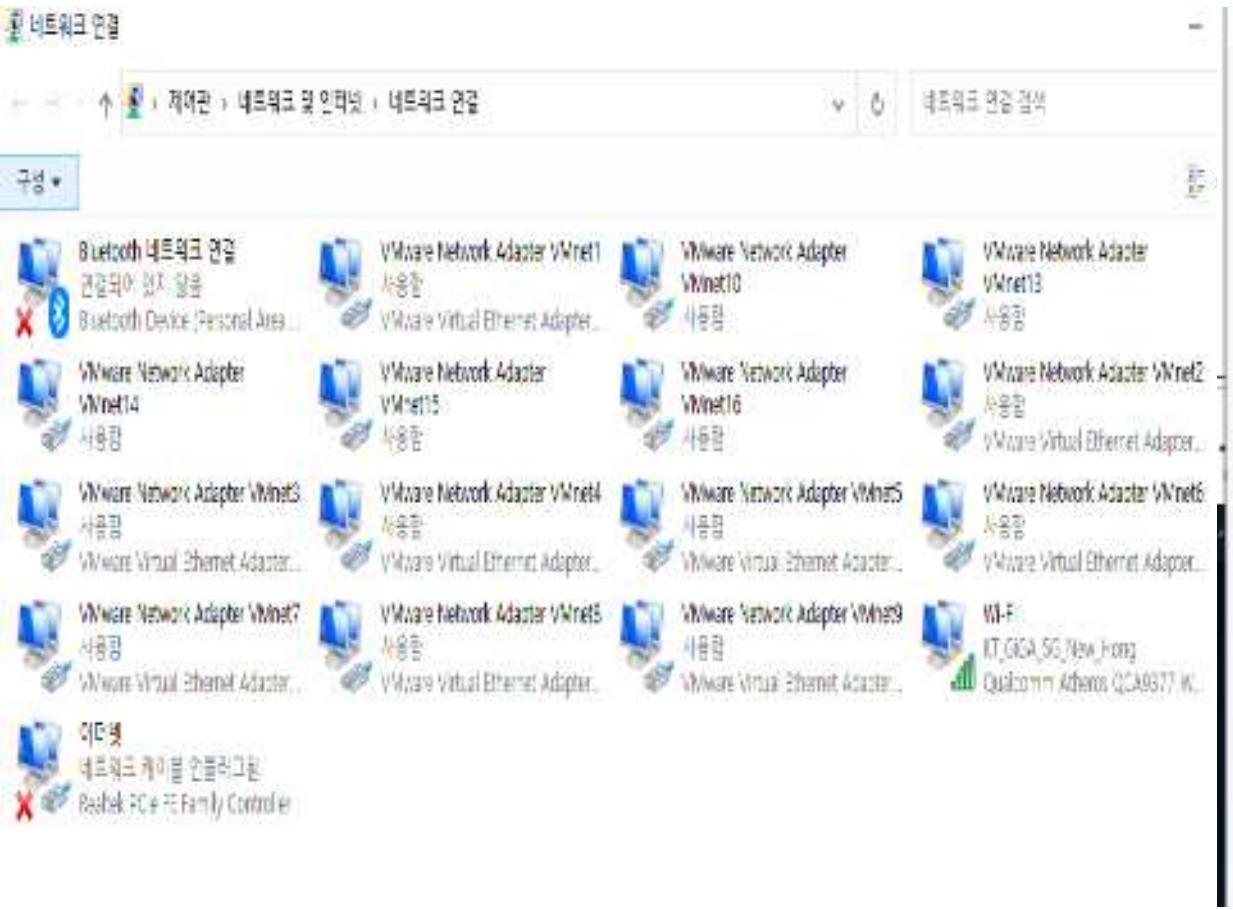


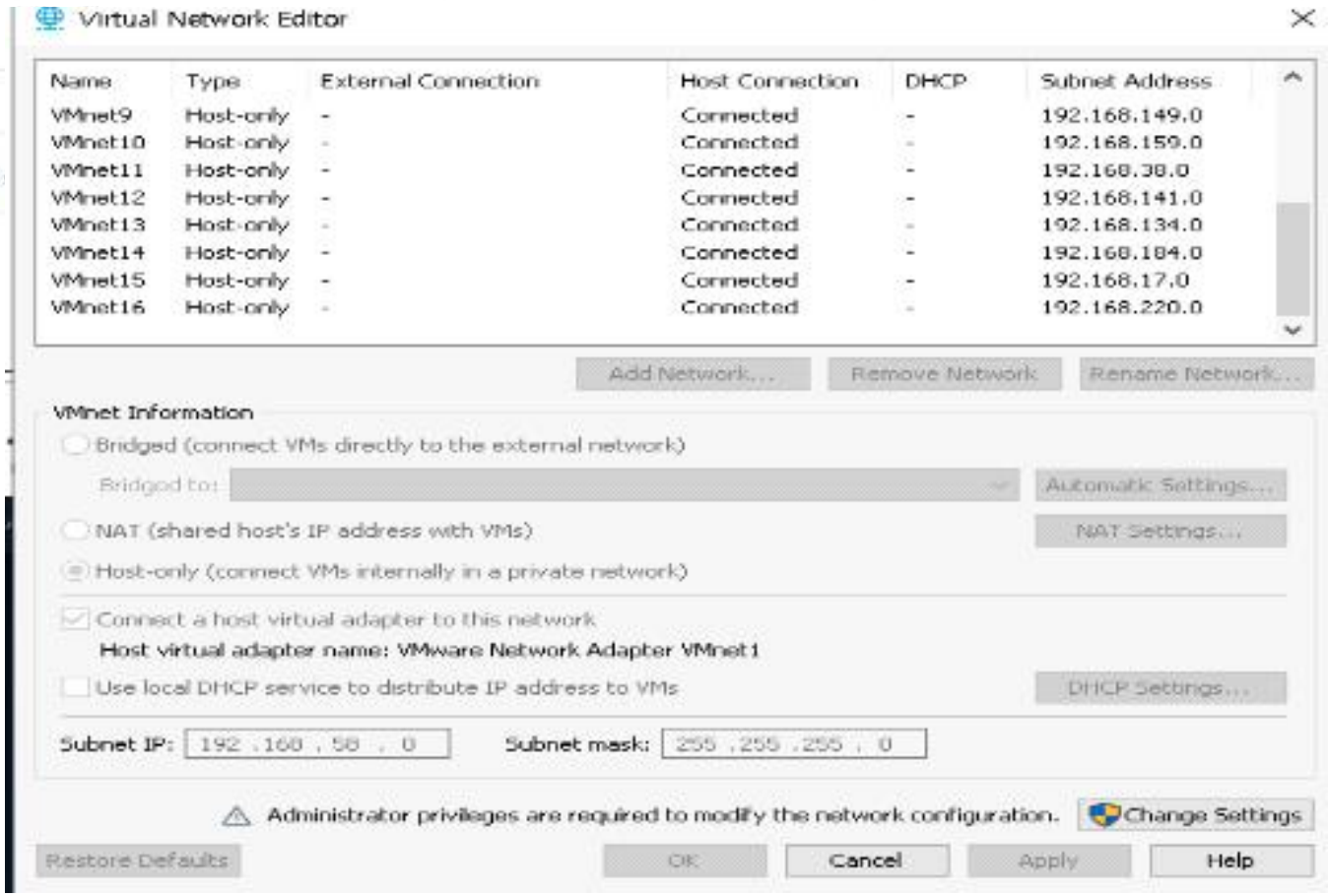
2.1 개발 환경 세팅

GNS3

패킷을 주고 받는 척하는 시뮬레이터인 시스코 패킷 트레이서와 달리 실제 장비의 CPU처리의 결과를 보여주는 GNS3 에뮬레이터를 사용해서 현장과 똑같은 결과를 만들 수 있다.

2.1 개발 환경 세팅





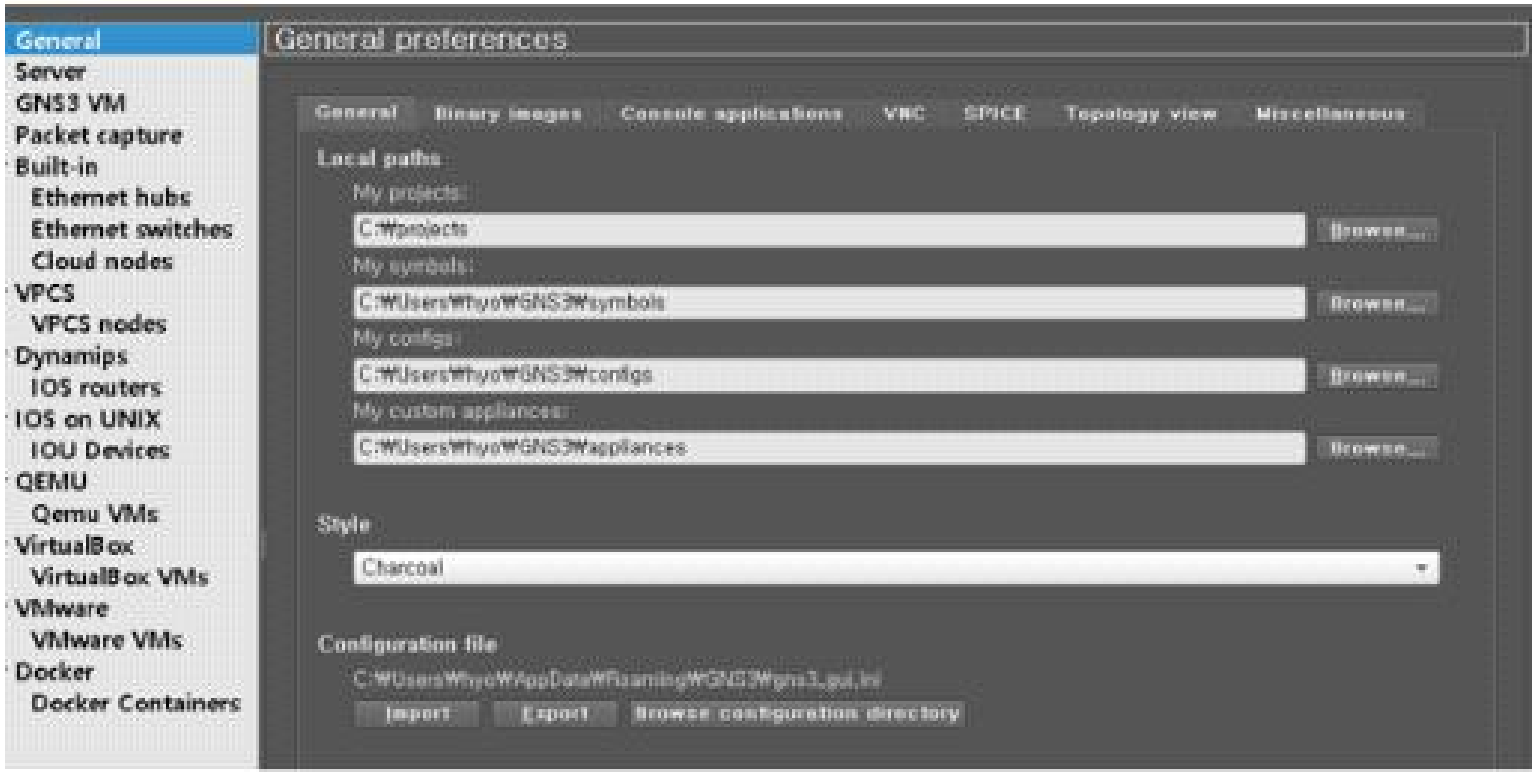
가상 네트워크를 추가하기 위해서 각 PC에 vmnet추가

2.1 개발 환경 세팅

VMWARE 환경에서 가상 네트워크 추가WINXP, CENTOS 사용

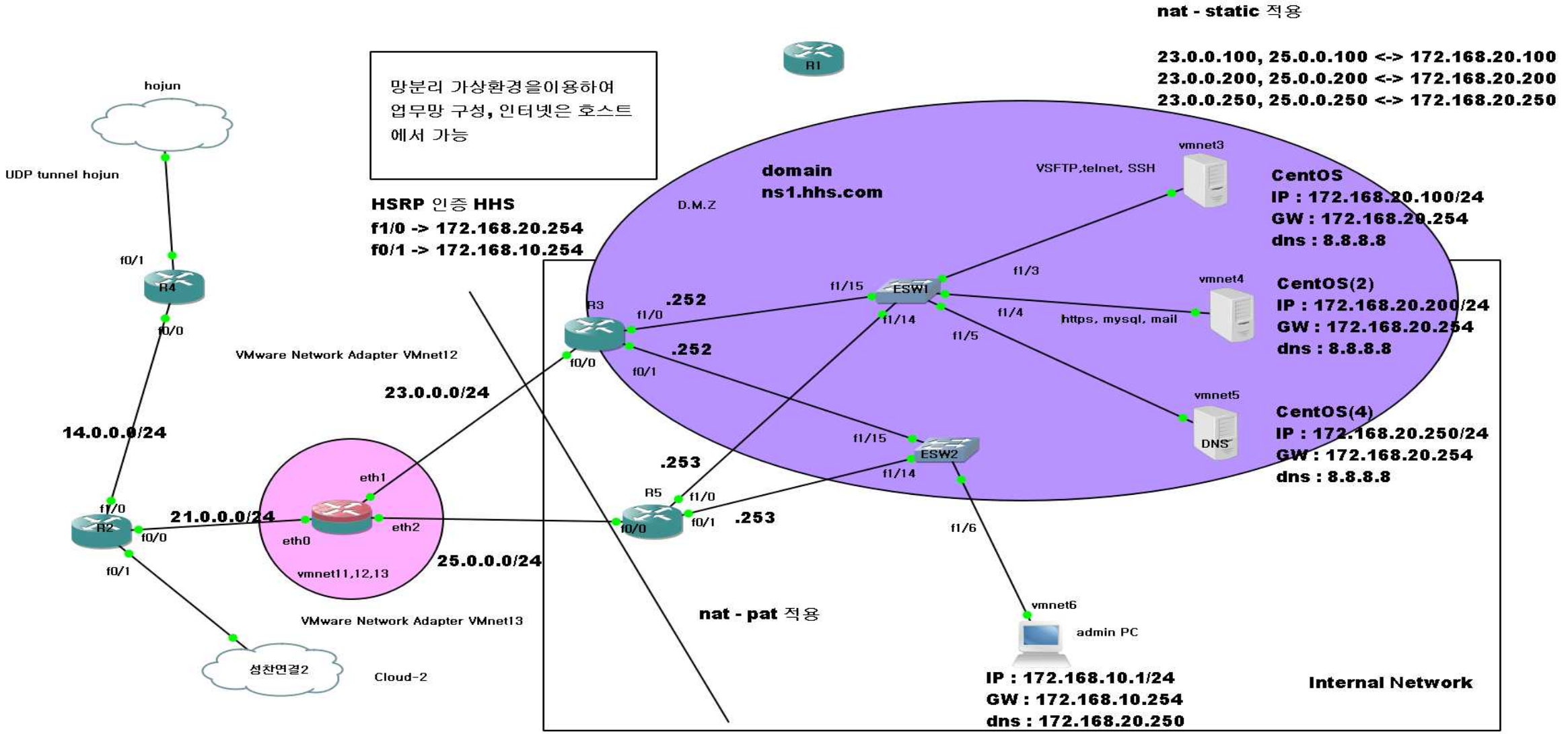
2.1 개발 환경 세팅

이미지 파일을 받아서 라우터랑 스위치를 구성

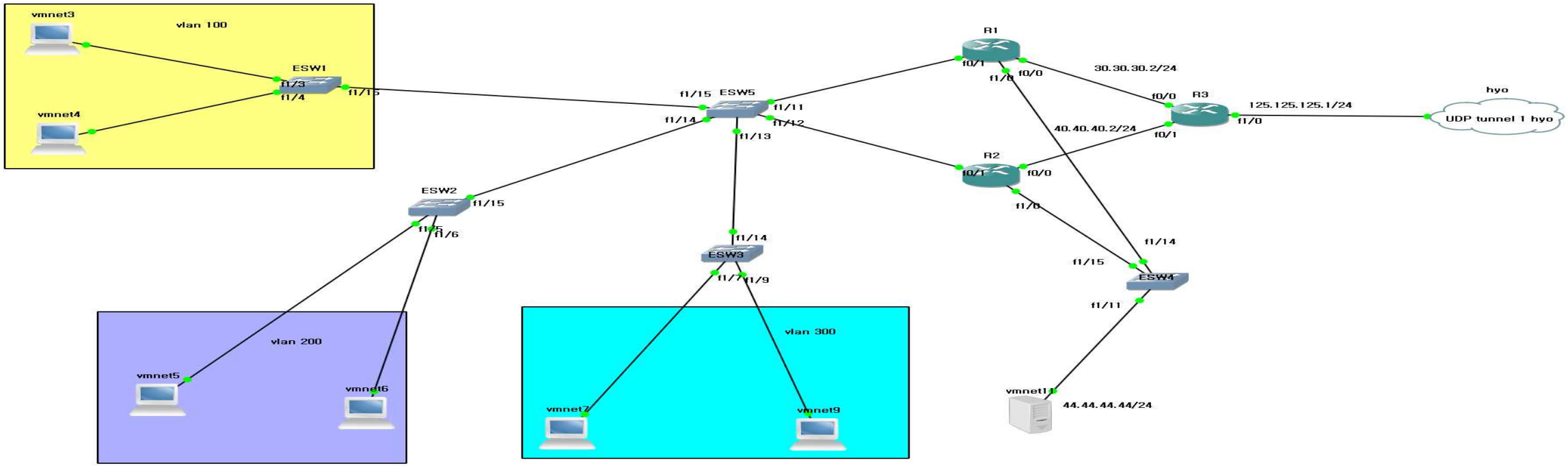


GNS3에 Bin 파일을 삽입해서 라우터랑 스위치 사용

2.2 개발 내용 및 실습

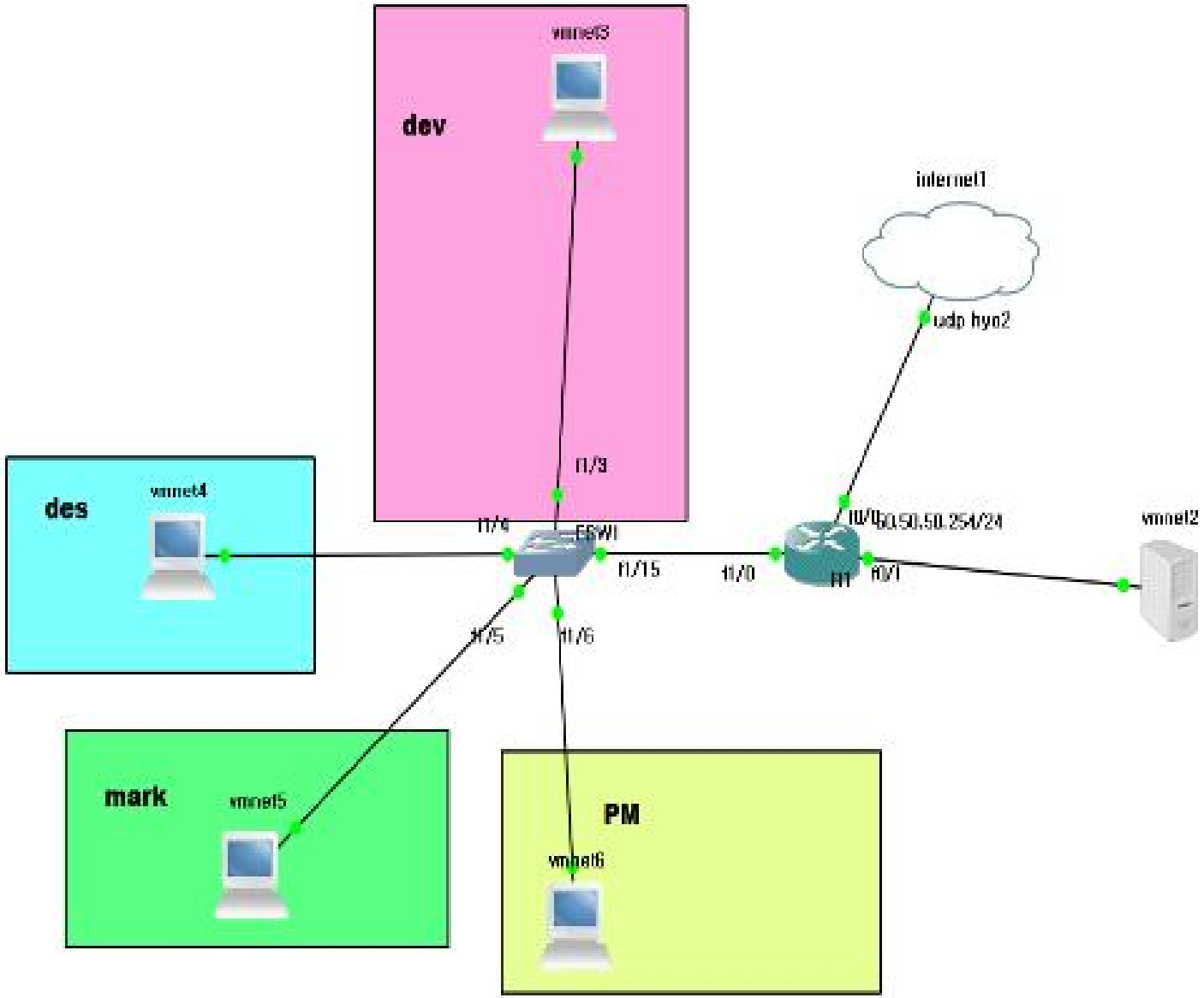

nat - static 적용
23.0.0.100, 25.0.0.100 <-> 172.168.20.100
23.0.0.200, 25.0.0.200 <-> 172.168.20.200
23.0.0.250, 25.0.0.250 <-> 172.168.20.250
망분리 가상환경을이용하여
업무망 구성, 인터넷은 호스트
에서 가능
HSRP 인증 HHS
f1/0 -> 172.168.20.254
f0/1 -> 172.168.10.254
hojun
UDP tunnel hojun
R1
R4
f0/1
f0/0
R3
f1/0
.252
.252
f0/0
f0/1
VMware Network Adapter VMnet12
23.0.0.0/24
14.0.0.0/24
R2
f1/0
f0/0
f0/1
21.0.0.0/24
eth1
eth0
eth2
vmnet11,12,13
25.0.0.0/24
VMware Network Adapter VMnet13
성찬연결2
Cloud-2
domain
ns1.hhs.com
D.M.Z
VSFTP,telnet, SSH
vmnet3
CentOS
IP : 172.168.20.100/24
GW : 172.168.20.254
dns : 8.8.8.8
f1/15
ESW1
f1/3
f1/4
f1/5
f1/14
vmnet4
https, mysql, mail
CentOS(2)
IP : 172.168.20.200/24
GW : 172.168.20.254
dns : 8.8.8.8
vmnet5
DNS
CentOS(4)
IP : 172.168.20.250/24
GW : 172.168.20.254
dns : 8.8.8.8
f1/15
ESW2
f1/14
.253
R5
f1/0
f0/0
f0/1
.253
f1/6
nat - pat 적용
vmnet6
admin PC
IP : 172.168.10.1/24
GW : 172.168.10.254
dns : 172.168.20.250
Internal Network

2.2 개발 내용 및 실습



VMware Network Adapter VMnet3
VMware Network Adapter VMnet6
VMware Network Adapter VMnet4
VMware Network Adapter VMnet9
VMware Network Adapter VMnet11

2.2 개발 내용 및 실습



encapsulation dot1Q 10
ip address 10.10.50.254 255.255.255.0
ip helper-address 50.50.50.50

interface FastEthernet1/0.20 intervlan
encapsulation dot1Q 20
ip address 10.10.60.254 255.255.255.0
ip helper-address 50.50.50.50

(ip helper :목적지 **IP**주소가 **broadcast IP**주소일 때 폐기하지 않고 지정된 목적지로 전달하는 기능**)**

2.2 개발 내용 및 실습

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
DEVICE=eth1:100
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
IPADDR=21.0.0.100
NETMASK=255.255.255.0
~
~
~
~
~
~
~
```

ETH1-100(nat-static 적용을 위한 가상망)

```
[root@localhost ~]# iptables -t nat -nL
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       all  --  0.0.0.0/0            21.0.0.100          to:172.168.20.100
DNAT       all  --  0.0.0.0/0            21.0.0.200          to:172.168.20.200
DNAT       all  --  0.0.0.0/0            21.0.0.250          to:172.168.20.250

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  172.168.10.1         0.0.0.0/0
```

nat 사용

2.2 개발 내용 및 실습

```
mysql> select user, password, host from mysql.user;
+-------------+-------------------------------------------+-----------------------
----------------------------+
| user        | password                                  | host
                           |
+-------------+-------------------------------------------+-----------------------
----------------------------+
| root        | *8232A1298A49F710DBEE0B330C42EEC825D4190A | localhost
                           |
| root        | *8232A1298A49F710DBEE0B330C42EEC825D4190A | a23-0-0-10.deploy.sta
tic.akamaitechnologies.com |
| root        | *8232A1298A49F710DBEE0B330C42EEC825D4190A | 127.0.0.1
                           |
|             |                                           | localhost
                           |
|             |                                           | a23-0-0-10.deploy.sta
tic.akamaitechnologies.com |
| remoteroot  | *8232A1298A49F710DBEE0B330C42EEC825D4190A | 172.16.0.20
                           |
| remoteUser  | *8232A1298A49F710DBEE0B330C42EEC825D4190A | 20.20.20.20
                           |
| root        | *8232A1298A49F710DBEE0B330C42EEC825D4190A | 172.168.10.1
                           |
+-------------+-------------------------------------------+-----------------------
----------------------------+
```

관리자 PC에서 FTP를 사용해서 자동으로 WAS 서버에 업로드 하기 위하여 DB 권한을 추가한다.

2.2 개발 내용 및 실습

```
[root@localhost html]# ls
board.php            download.php          login_proc.php
board_del.php        edit_member.php       logout.php
board_insert.php     edit_member_proc.php  style.css
board_search.php     index.php             upload.php
board_view.php       inmember.html         upload_proc.php
change_nick.php      inmember_proc.php     uploaded_search_proc.php
change_nick_proc.php login.html            uploadfiles
```

웹서버 파일
원격지의 관리자 PC에서 sql 워크벤치를 사용해 DB를 연결하고,
vscode의 sftp 응용프로그램을 사용하여 port 번호와 DB를 알맞게 설정하여 웹프로그래밍 한 파일들을 자동으로 was에 업로드

2.2 개발 내용 및 실습

```
; Maximum size of POST data that PHP will accept.
; http://www.php.net/manual/en/ini.core.php#ini.post-max-size
post_max_size = 8M

; Magic quotes are a preprocessing feature of PHP where PHP will attempt to
; escape any character sequences in GET, POST, COOKIE and ENV data which might
; otherwise corrupt data being placed in resources such as databases before
; making that data available to you. Because of character encoding issues and
; non-standard SQL implementations across many databases, it's not currently
; possible for this feature to be 100% accurate. PHP's default behavior is to
; enable the feature. We strongly recommend you use the escaping mechanisms
; designed specifically for the database your using instead of relying on this
; feature. Also note, this feature has been deprecated as of PHP 5.3.0 and is
; scheduled for removal in PHP 6.
; Default Value: On
; Development Value: Off
; Production Value: Off
; http://www.php.net/manual/en/info.configuration.php#ini.magic-quotes-gpc
magic_quotes_gpc = On

; Magic quotes for runtime-generated data, e.g. data from SQL, from exec(), etc.
; http://www.php.net/manual/en/info.configuration.php#ini.magic-quotes-runtime
magic_quotes_runtime = Off

; Use Sybase-style magic quotes (escape ' with '' instead of \').
; http://www.php.net/manual/en/sybase.configuration.php#ini.magic-quotes-sybase
magic_quotes_sybase = Off

; Automatically add files before PHP document.
; http://www.php.net/manual/en/ini.core.php#ini.auto-prepend-file
auto_prepend_file =
```

방지기능 PHP_ini)
waf 기능도 수행할 수 있게 php.ini httpd.conf를 수정
그 외 다른 업무망에서 dhcp 서비스를 사용하므로, 로컬 POOL을 구성하고 네트워크에 맞게 POOL 구성한것을 각각 windows XP에다가 할당 scope 만큼,또한 스니핑을 방지하기 위해서 arp -s 를 이용해 정적으로 mac주소를 할당

2.2 개발 내용 및 실습

```
[root@localhost ~]# iptables -nL --line
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  0.0.0.0/0            25.0.0.200          multiport dports 80,443 STRING match "admin" ALGO name kmp TO 65535
2    DROP       tcp  --  0.0.0.0/0            23.0.0.200          multiport dports 80,443 STRING match "admin" ALGO name kmp TO 65535
3    ACCEPT     tcp  --  0.0.0.0/0            23.0.0.100          tcp dpts:20:22
4    ACCEPT     tcp  --  0.0.0.0/0            25.0.0.100          tcp dpts:20:22
5    DROP       all  --  0.0.0.0/0            23.0.0.100
6    DROP       all  --  0.0.0.0/0            25.0.0.100
7    ACCEPT     tcp  --  0.0.0.0/0            23.0.0.200          multiport dports 80,443,25,110,143
8    ACCEPT     tcp  --  0.0.0.0/0            25.0.0.200          multiport dports 80,443,25,110,143
9    DROP       all  --  0.0.0.0/0            23.0.0.200
10   DROP       all  --  0.0.0.0/0            25.0.0.200
11   ACCEPT     udp  --  0.0.0.0/0            23.0.0.250          udp dpt:53
12   ACCEPT     udp  --  0.0.0.0/0            25.0.0.250          udp dpt:53
13   DROP       all  --  0.0.0.0/0            23.0.0.250
14   DROP       all  --  0.0.0.0/0            25.0.0.250
15   DROP       all  --  0.0.0.0/0            23.0.0.0/24
16   DROP       all  --  0.0.0.0/0            25.0.0.0/24

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

firewall 보안강화 (방화벽 역할도하면서 정보도 전송)

2.2 개발 내용 및 실습

```
# Authentication:
# 로그인 대기시간 2분 루트 로그인 금지, 인증 시도 5회, 최대 연결 수 10
LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
MaxAuthTries 5
MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
-- 끼워넣기 --
```

서비스 할 서비스들을 yum install sshd, vsftpd 등 설정

2.2 개발 내용 및 실습

```
root@localhost security]# cat /etc/pam.d/sshd
%PAM-1.0
ccount    required     pam_time.so
uth       required     pam_listfile.so item=user sense=allow file=/etc/ssh/sshlist onerr=succeed
uth       required     pam_sepermit.so
uth       include      password-auth
ccount    required     pam_nologin.so
ccount    include      password-auth
assword   include      password-auth
 pam_selinux.so close should be the first session rule
ession    required     pam_selinux.so close
ession    required     pam_loginuid.so
 pam_selinux.so open should only be followed by sessions to be executed in the user context
ession    required     pam_selinux.so open env_params
ession    optional     pam_keyinit.so force revoke
ession    include      password-auth
root@localhost security]# cat /etc/pam.d/vsftpd
%PAM-1.0
ession    optional     pam_keyinit.so    force revoke
ccount    required     pam_time.so
uth       required     pam_listfile.so item=user sense=deny file=/etc/vsftpd/ftpusers onerr=succeed
uth       required     pam_shells.so
uth       include      password-auth
ccount    include      password-auth
```

PAM 을 이용해서 (sshlist, timeso)를 이용하여 유저 화이트 리스트 작성, 시간 작성

2.2 개발 내용 및 실습

```
[root@localhost ~]# rpm -qa vsftpd
vsftpd-2.2.2-24.el6.x86_64
[root@localhost ~]#
```

(설치 확인) DNS 서비스를 구축하여 이름으로 편리하게 접속이 가능하게 만들어준다.

```
$TTL 1D
@       IN SOA  ns.hhs.com. admin.hhs.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      ns1.hhs.com.
        MX 10   mail.hhs.com.
ns1     A       172.168.20.250
www     A       172.168.20.200
mail    A       172.168.20.200
ssh     A       172.168.20.100
telnet  A       172.168.20.100
ftp     A       172.168.20.100
~
```

회사에서 사용할 HTML,CSS,PHP를 구성한다.

2.2 개발 내용 및 실습

de > {..} sftp.json

```
{
    "name": "jbproject",
    "host": "www.hhs.com",
    "protocol": "ftp",
    "port": 21,
    "username": "root",
    "password": "P@ssw0rd",
    "remotePath": "/var/www/html/",
    "uploadOnSave": true,
    "connectTimeout": 1000000
}
```

```
[root@localhost ~]# ls -l /var/www/html/
합계 84
-rw-r--r-- 1 root root 3467 2021-09-12 14:44 board.php
-rw-r--r-- 1 root root 1286 2021-09-11 22:55 board_del.php
-rw-r--r-- 1 root root 1939 2021-10-03 21:58 board_insert.php
-rw-r--r-- 1 root root 1185 2021-09-11 22:54 board_search.php
-rw-r--r-- 1 root root 1018 2021-09-11 22:53 board_view.php
-rw-r--r-- 1 root root 1401 2021-09-11 22:02 change_nick.php
-rw-r--r-- 1 root root 1036 2021-10-03 21:58 change_nick_proc.php
-rw-r--r-- 1 root root  424 2021-09-12 17:07 download.php
-rw-r--r-- 1 root root 2356 2021-09-11 22:57 edit_member.php
-rw-r--r-- 1 root root 1630 2021-09-11 22:39 edit_member_proc.php
-rw-r--r-- 1 root root 2015 2021-09-12 16:37 index.php
-rw-r--r-- 1 root root 3814 2021-09-12 14:43 inmember.html
-rw-r--r-- 1 root root 2374 2021-09-11 22:39 inmember_proc.php
-rw-r--r-- 1 root root 1492 2021-09-12 16:58 login.html
-rw-r--r-- 1 root root 1581 2021-10-03 19:41 login_proc.php
-rw-r--r-- 1 root root  205 2021-09-11 21:58 logout.php
-rw-r--r-- 1 root root  285 2021-09-11 21:43 style.css
-rw-r--r-- 1 root root 1631 2021-09-12 16:49 upload.php
-rw-r--r-- 1 root root 1301 2021-09-12 18:07 upload_proc.php
-rw-r--r-- 1 root root 2233 2021-09-12 17:02 uploaded_search_proc.php
drwxrwxrwx 2 root root 4096 2021-10-03 21:53 uploadfiles
```

회사의 가상 홈페이지 구축

2.2 개발 내용 및 실습

각종 서비스를 할 수 있는 홈페이지 구축완료 후 모의 해킹 등을 실행

2.2 개발 내용 및 실습

```
[root@localhost ~]# iptables -nL --line
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       tcp  --  0.0.0.0/0            25.0.0.200          multiport dports 80,443 STRING match "admin" ALGO name kmp TO 65535
2    DROP       tcp  --  0.0.0.0/0            23.0.0.200          multiport dports 80,443 STRING match "admin" ALGO name kmp TO 65535
3    ACCEPT     tcp  --  0.0.0.0/0            23.0.0.100          tcp dpts:20:22
4    ACCEPT     tcp  --  0.0.0.0/0            25.0.0.100          tcp dpts:20:22
5    DROP       all  --  0.0.0.0/0            23.0.0.100
6    DROP       all  --  0.0.0.0/0            25.0.0.100
7    ACCEPT     tcp  --  0.0.0.0/0            23.0.0.200          multiport dports 80,443,25,110,143
8    ACCEPT     tcp  --  0.0.0.0/0            25.0.0.200          multiport dports 80,443,25,110,143
9    DROP       all  --  0.0.0.0/0            23.0.0.200
10   DROP       all  --  0.0.0.0/0            25.0.0.200
11   ACCEPT     udp  --  0.0.0.0/0            23.0.0.250          udp dpt:53
12   ACCEPT     udp  --  0.0.0.0/0            25.0.0.250          udp dpt:53
13   DROP       all  --  0.0.0.0/0            23.0.0.250
14   DROP       all  --  0.0.0.0/0            25.0.0.250
15   DROP       all  --  0.0.0.0/0            23.0.0.0/24
16   DROP       all  --  0.0.0.0/0            25.0.0.0/24

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

사용하는 서버에서 제공하는 서비스만 사용하기 위한 정책을 작성한다.

2.2 개발 내용 및 실습

나머지 서비스들도 정상동작하는지 확인한다.(mail)

2.2 개발 내용 및 실습

```
root@localhost security]# cat /etc/pam.d/sshd
%PAM-1.0
:count     required      pam_time.so
uth        required      pam_listfile.so item=user sense=allow file=/etc/ssh/sshlist on
uth        required      pam_sepermit.so
uth        include       password-auth
:count     required      pam_nologin.so
:count     include       password-auth
assword    include       password-auth
 pam_selinux.so close should be the first session rule
ession     required      pam_selinux.so close
ession     required      pam_loginuid.so
 pam_selinux.so open should only be followed by sessions to be executed in the user c
ession     required      pam_selinux.so open env_params
ession     optional      pam_keyinit.so force revoke
ession     include       password-auth
root@localhost security]# cat /etc/pam.d/vsftpd
%PAM-1.0
ession     optional      pam_keyinit.so    force revoke
:count     required      pam_time.so
uth        required      pam_listfile.so item=user sense=deny file=/etc/vsftpd/ftpusers
uth        required      pam_shells.so
uth        include       password-auth
:count     include       password-auth
```

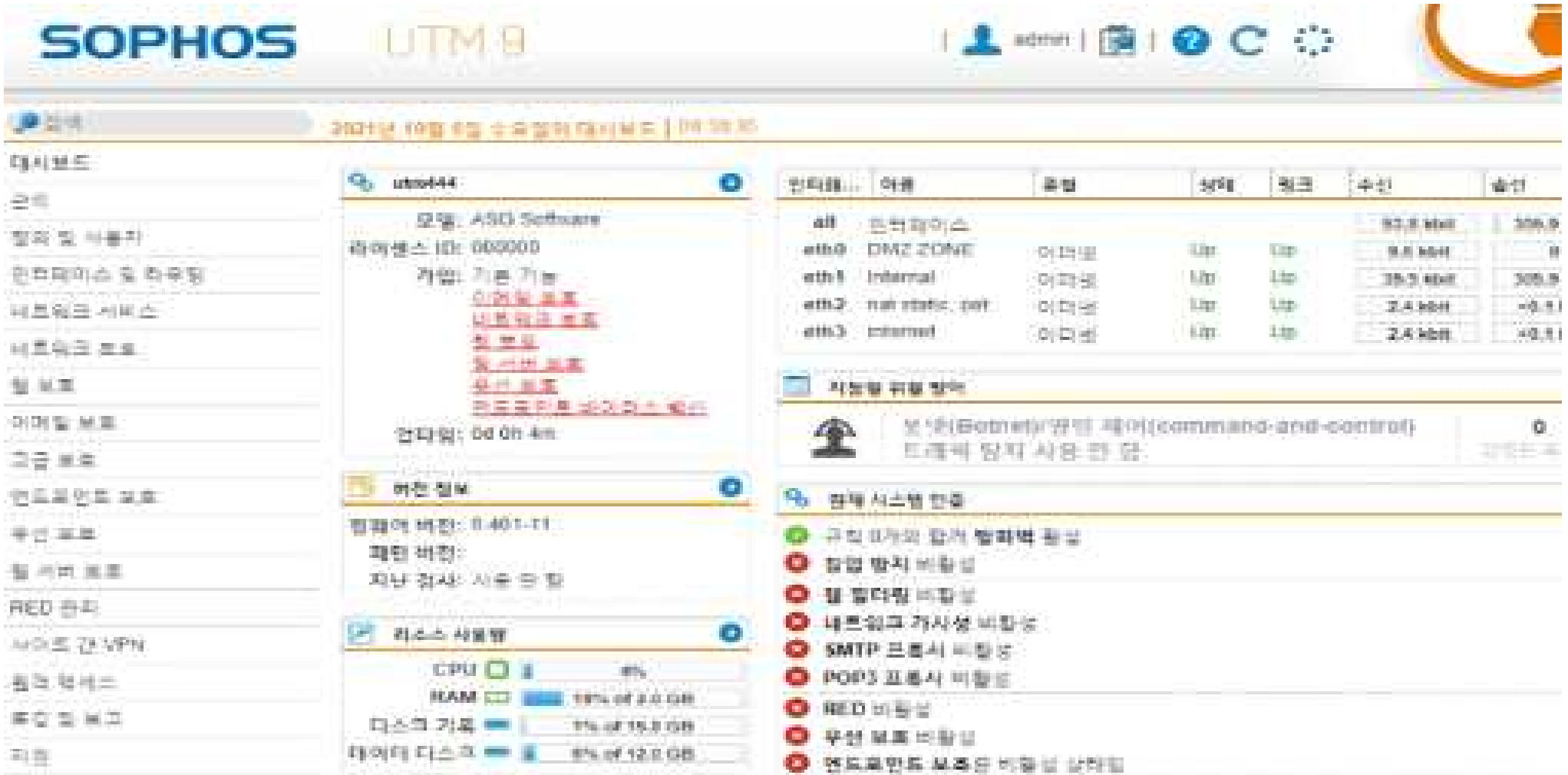
보안 솔루션인 NAT,PAT 설치

2.2 개발 내용 및 실습

```
speed auto
standby 1 ip 172.168.20.254
standby 1 timers 1 3
standby 1 priority 120
standby 1 preempt delay minimum 5
standby 1 authentication md5 key-string hhs
standby 1 track 1 decrement 30


outer ospf 1
log-adjacency-changes
passive-interface FastEthernet0/1
passive-interface FastEthernet1/0
network 23.0.0.0 0.0.0.255 area 0

o ip http server
o ip http secure-server
p forward-protocol nd


p nat inside source list 1 interface FastEthernet0/0 o
p nat inside source static 172.168.20.100 23.0.0.100
p nat inside source static 172.168.20.200 23.0.0.200
p nat inside source static 172.168.20.250 23.0.0.250
```

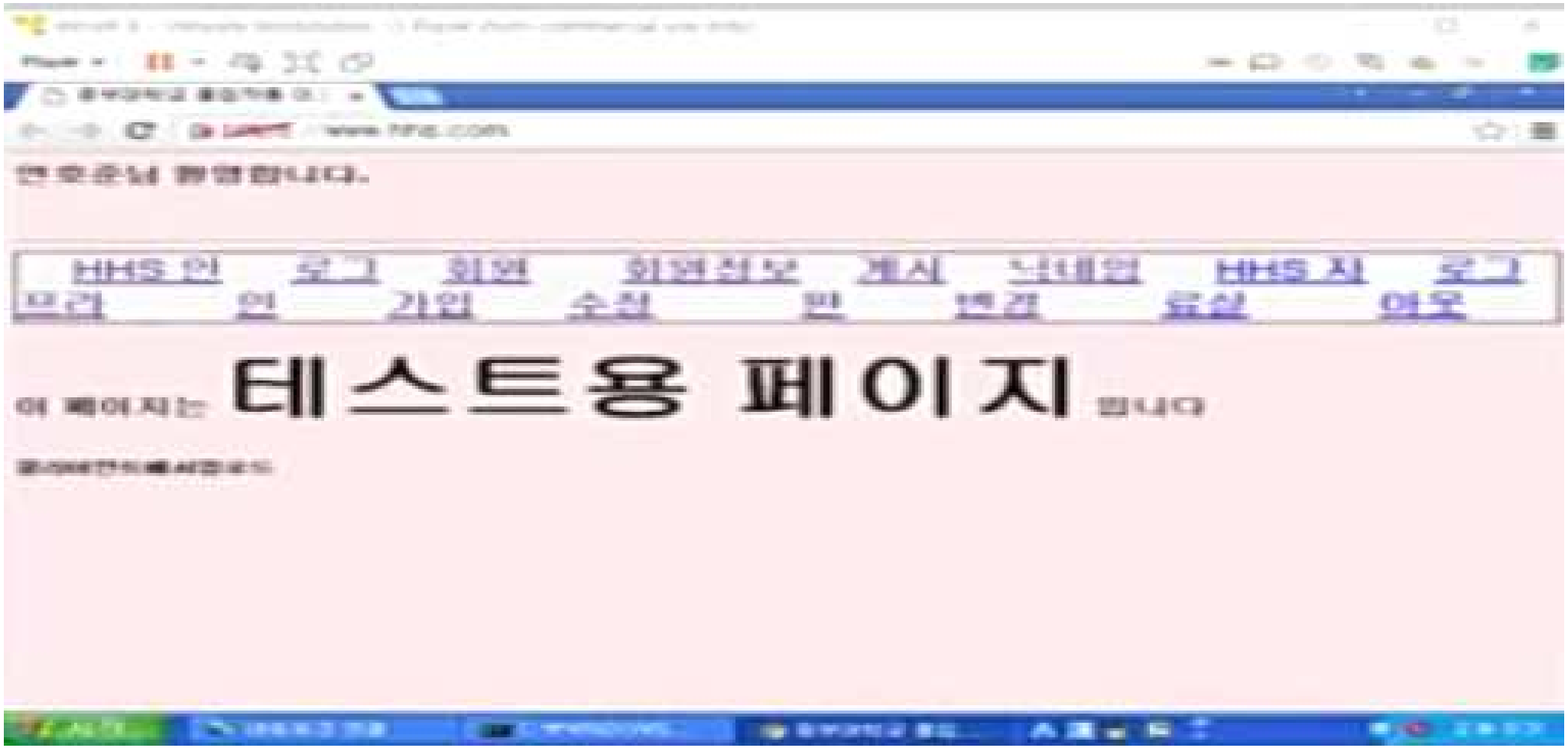
각 토폴로지에 알맞은 IP 설정 후 가상의 회사망을 구축함
(사진은 NAT,OSPF,이중화 등)

2.2 개발 내용 및 실습



여러 개의 보안 기능이 통합 되어있는 장비인 UTM 대시보드 구현(현재 실습한 기능은 없음) 있고 여기에서 공간 절약,네트워크 구조 단순화,비용 절감 등의 장점을 얻을 수있다.

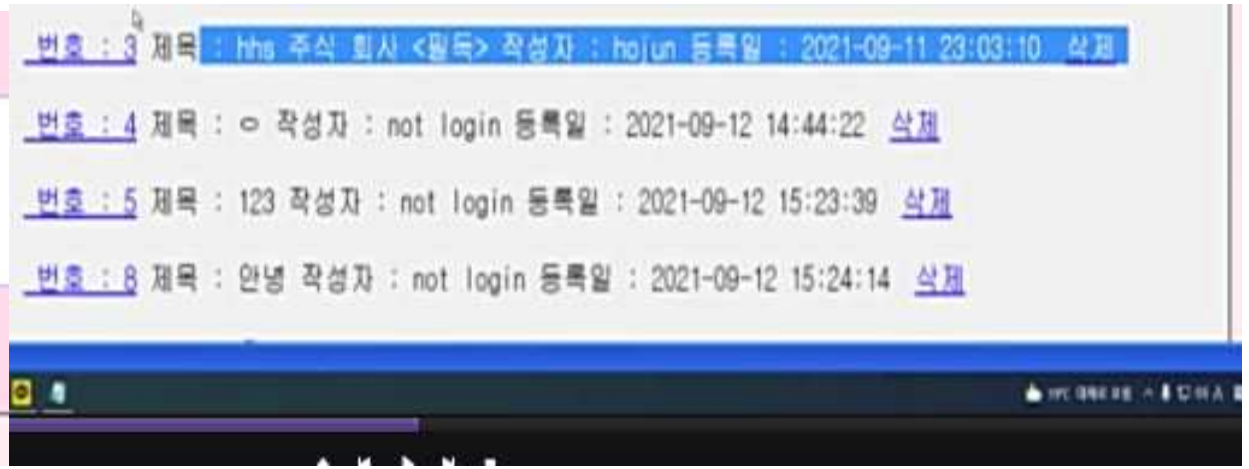
2.3 모의 해킹 실습



메인 홈페이지 에서 실습

2.3 모의 해킹 실습

1.간단한 xss 공격



1. 기존에 게시판에 등록 되어 있던 글이 삭제 된다.

등록된 글을 누르면

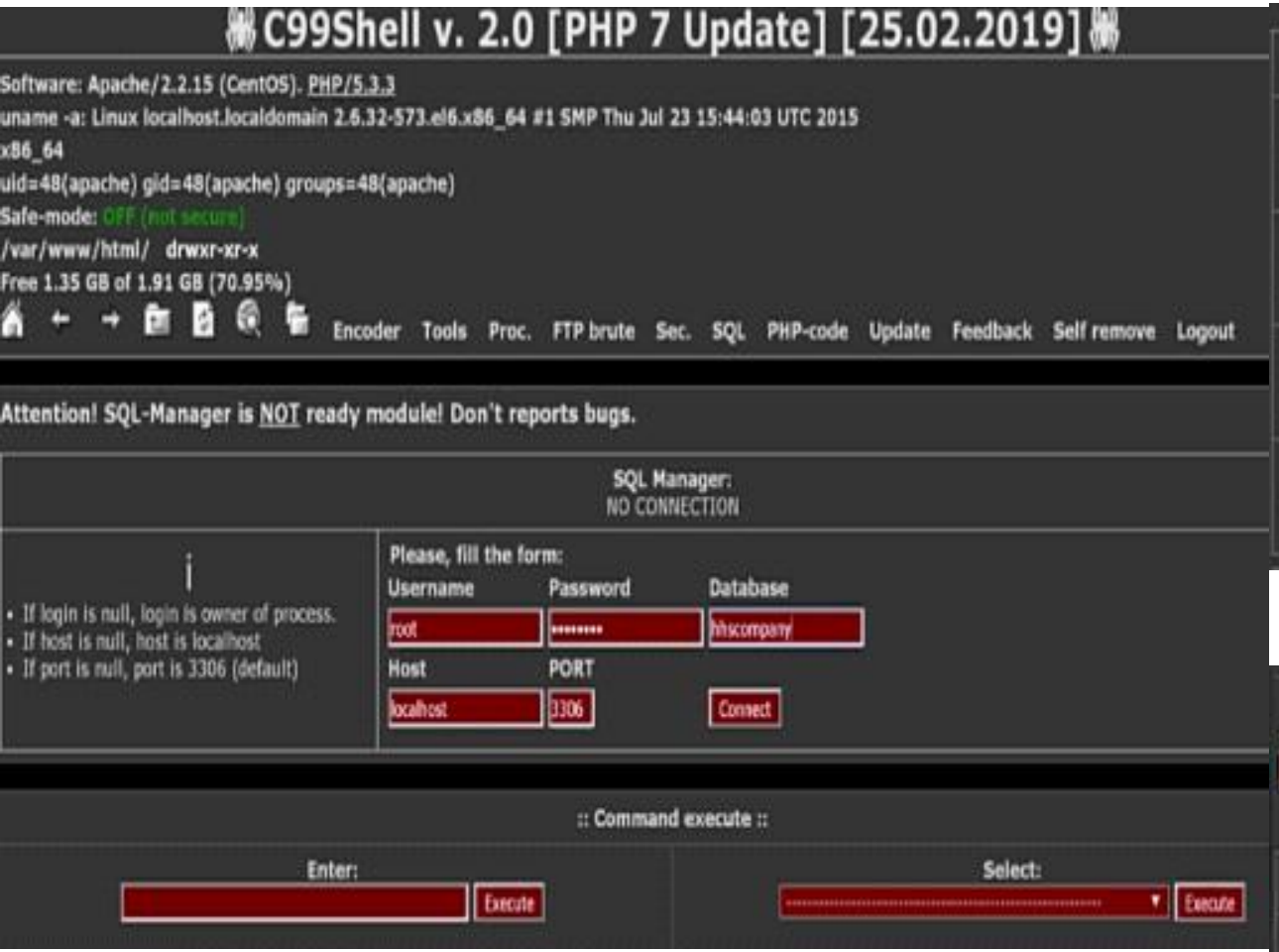
2.3 모의 해킹 실습

악의적인 글을 등록

이글을 누르면

의도하지 않은 글이 작성 된다.

2.3 모의 해킹 실습



C99Shell 메인

no	name	id	pass	phone	email	address	sex	in_date	Action
1	admin	admin	1234	01072775752	hyo@hhs.com	??? ???	man	2021-09-11 22:40:00	
2	fun :)	hojun	1234	010-3953-8725	jun@hhs.com	경기도 ㅠ 수시 미래로422	M	2021-09-11 22:40:25	
3	cheack	hong	123456	010-1111-1111	ghdtjdcks22@naver.com	위시티3로	M	2021-09-12 14:41:35	
5	hacker	hacker	1234	hacker	hacker	hacker	M	2021-09-12 18:07:03	

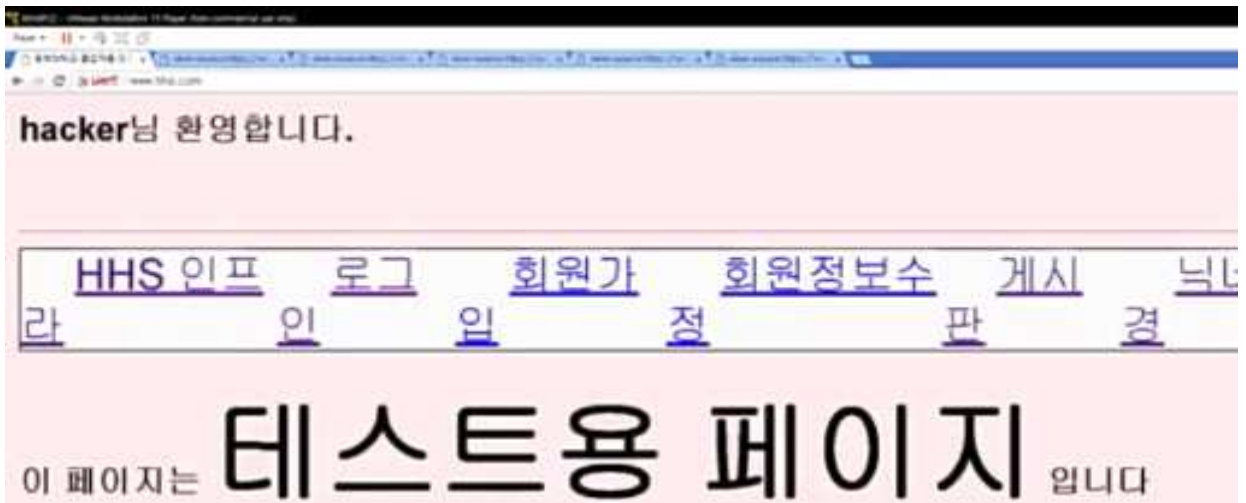
C99Shell 에서 탈취된 사용자 개인정보

Table	Rows	Type	Created	Modified	Size	Action
board	30		2021-09-11 22:24:37		16 KB	
member	4		2021-09-11 21:02:45		16 KB	
upload	3		2021-09-12 16:43:25		16 KB	
3 table(s)	37				48 KB	

C99Shell 에서 탈취된 테이블 정보

2.3 모의 해킹 실습

SQL injection



암호없이 로그인이 되버린다.

2.3 모의 해킹 실습

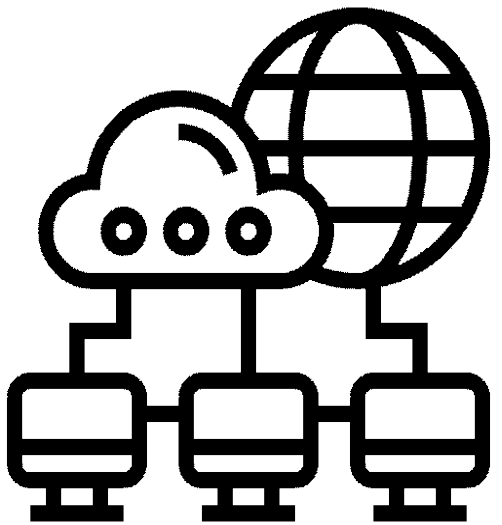
의도하지 않은 팝업 메세지가 삽입 된다(xss)

결론

GNS3라는 가상의 환경을 이용하여 쉽게 고가의 보안장비들을 가상으로 이용해 CLI 환경에서 활용해 볼 수 있었고, 이로 인해서 보다 더 쉽게 다가 갈 수 있었다.
실제로 활용하기 어려운 장비들을 가상으로 활용해 관심있는 사람들이나 공부하고 있는 사람들이 이를 통해서 더욱 익숙해지고, 흥미를 가질 수 있을 것이다

향후 계획

GNS3 내부에서 다양한 보안장비들을 더 도입하여서(UTM 적극활용)
한층 보안이 강화되어 패턴 기반 IDS,IPS를 더 세밀하게 구축하여
보안성이 뛰어나게 만들어 보려 한다.




감사합니다