답안지

과정명	오픈소스 기반 보안 취약점 분석 실무자 양성	담당교사	홍제준	월차	
과목명	보안위협관리통제	훈련생 이름	임서규	평가일자	9월 27일
평가 방법	문제해결 시나리오				

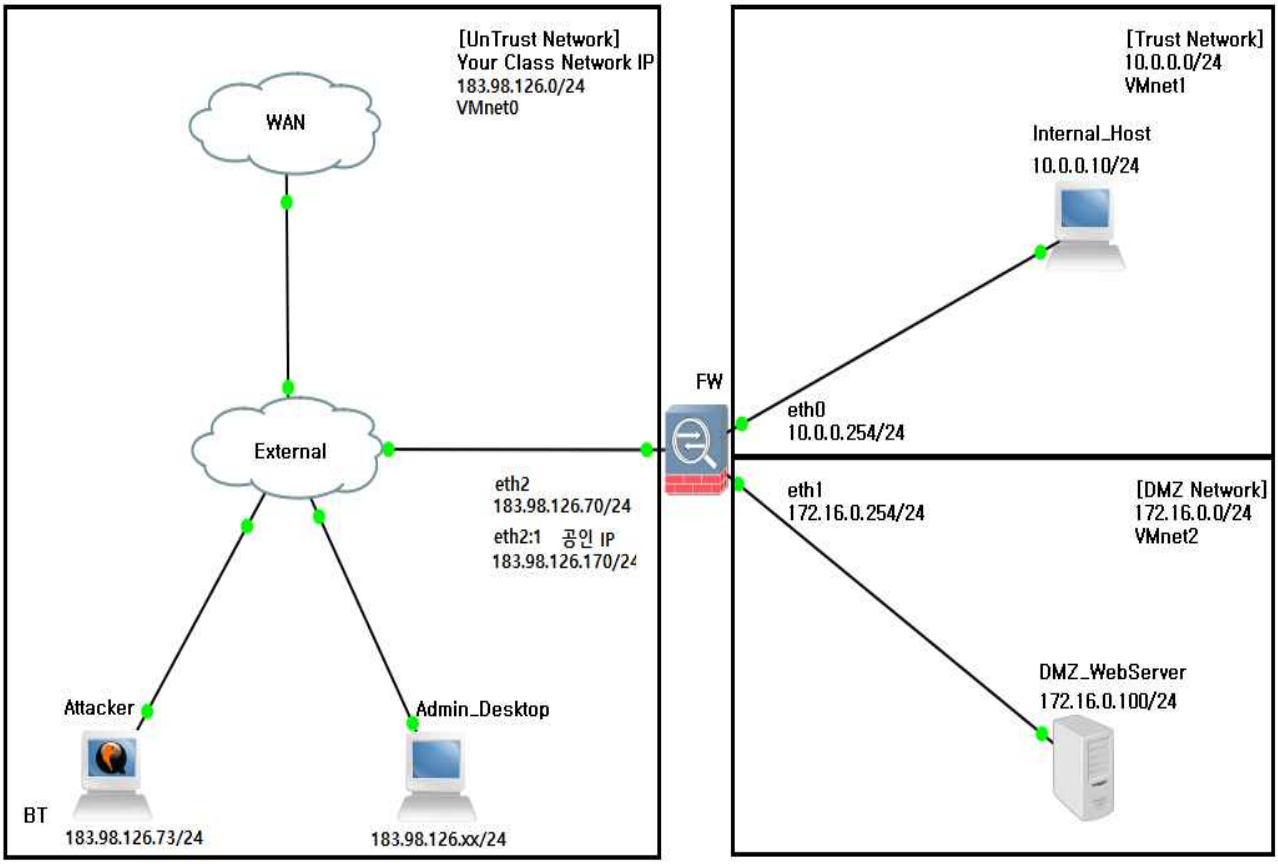
답안

보안 위협 관리 통제

- 목차 -

1. 토폴로지 개요

토폴로지 전체적인 구성도는 다음과 같습니다.



UnTrust Network는 외부 네트워크 뜻하며 Trust Network는 내부 네트워크를 말합니다.
DMZ Network는 비무장지대를 뜻하며 조직의 내부 네트워크와 외부 네트워크 사이에 위치한 서브넷입니다. 내부 네트워크와 외부 네트워크가 DMZ로 연결할 수 있도록 허용 하면서도, DMZ 내의 컴퓨터는 오직 외부 네트워크에만 연결할 수 있도록 합니다. 즉 DMZ는 외부에 서비스를 제공해야 하는 상황에서 내부 자원을 보호하기 위해 내부 네트워크와 분리시킨 공간을 말합니다.
외부 네트워크는 eth2:1를 제외한 모든 IP가 자동할당 상태이며 eth2:1은 수동설정 하였습니다. 또한 외부네트워크는 VMnet0으로 설정되어있습니다. 내부 네트워크는 eth0로 등록 되어 있으며 VMnet1로 설정되어 있으며, DMZ 네트워크는 eth1과 VMnet2로 설정 되어 있습니다.
다음은 각 토폴로지의 IP구성 사진입니다.

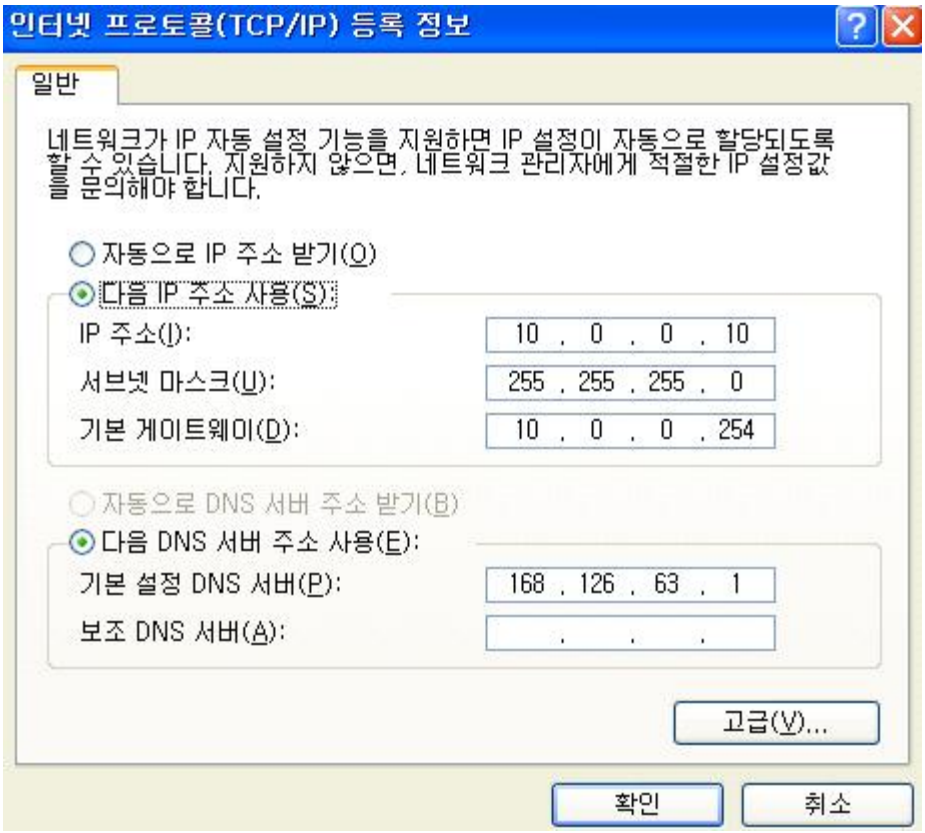
< Attacker (BackTrack5 R3) >

```
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9e:a3:68
          inet addr:183.98.126.73  Bcast:183.98.126.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9e:a368/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:256564 (256.5 KB)  TX bytes:3074 (3.0 KB)
```

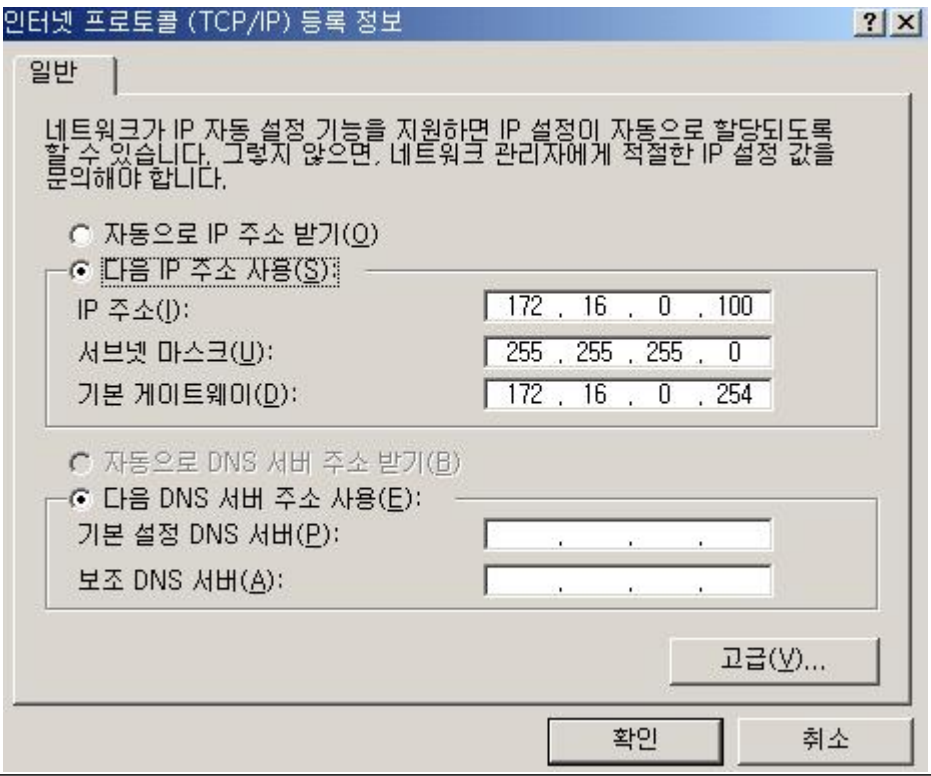
< FW (Cent OS) >

```
eth0      Link encap:Ethernet  HWaddr 00:0C:29:3C:47:2B
          inet addr:10.0.0.254  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3c:472b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1375 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:419251 (409.4 KiB)  TX bytes:3564 (3.4 KiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:3C:47:35
          inet addr:172.16.0.254  Bcast:172.16.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3c:4735/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:393936 (384.7 KiB)  TX bytes:258 (258.0 b)

eth2      Link encap:Ethernet  HWaddr 00:0C:29:3C:47:3F
          inet addr:183.98.126.70  Bcast:183.98.126.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3c:473f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:57980 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3800563 (3.6 MiB)  TX bytes:8008 (7.8 KiB)

eth2:1    Link encap:Ethernet  HWaddr 00:0C:29:3C:47:3F
          inet addr:183.98.126.170  Bcast:183.98.126.255  Mask:255.255.255.0
```

< Internal_Host (XP) >



< DMZ_WebServer (win 2k) >



2. 화이트 리스트 구성

화이트 리스트란 '안전'이 증명된 것만을 허용하는 것으로 '악의성'이 입증된 것을 차단하는 블랙리스트 보안과 상반되는 보안 방식입니다. 즉, 사전에 허용된 정책이외에는 모두 차단합니다.
일반적으로 모든 패킷에 대해서 무시하는 것이 방화벽의 기본 정책입니다.

```
[root@localhost ~]# iptables -P INPUT DROP
[root@localhost ~]# iptables -P OUTPUT DROP
[root@localhost ~]# iptables -P FORWARD DROP
[root@localhost ~]# iptables -A INPUT -i lo -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -o lo -j ACCEPT
[root@localhost ~]# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
```

1. INPUT(입력체인)
2. FORWARD(포워딩체인)
3. OUTPUT(출력체인)

기본 규칙 체인인 3가지 모두 DROP으로 설정합니다. 이것은 어떠한 패킷이든 들어오고 나갈 수 없는 상태임을 의미하며, 로컬이든 외부에서 로컬 컴퓨터로는 네트워크가 차단된 것처럼 연결할 수 없게 됩니다. INPUT체인과 OUTPUT체인에 로컬 Loopback 장치 트래픽 허용 합니다. 이는 디지털 전송장비를 이용한 선로(회선) 및 장비를 시험하기 위해서 필요한 설정입니다. 이는 Trust구간에 들어오는 비정상 패킷이나 잘못된 세션을 거부합니다.

3. Trust site 정책 구성

< NAT 구성 및 MASQUERAD 설정 >

내부 네트워크의 Trust Network 구간과 DMZ Network 구간을 NAT 구성을 합니다.

NAT란 네트워크 주소 변환을 뜻하며 사설 네트워크에 속한 여러 개의 호스트가 하나의 공인 IP 주소를 사용하여 인터넷에 접속하기 위함입니다. 또한 공공망과 연결되는 사용자들의 고유한 사설망을 침입자들로부터 보호할 수 있는 장점이 있습니다.

■ XP NAT 구성

```
[root@localhost ~]# iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth2 -j MASQUERADE
[root@localhost ~]#
```

NAT는 내부 사설 IP의 PC들이 외부 인터넷이 연결 가능하도록 해줍니다.

10.0.0.0/24 네트워크 대역대에서 나가는 출력패킷이 외부IP인 eth2 인터페이스를 통하여 NAT합니다.

■ 2K DNAT 구성

```
[root@localhost ~]# iptables -t nat -A PREROUTING -p tcp -m multiport --dport 22,80,443 -i eth2 -
d 183.98.126.170 -j DNAT --to 172.16.0.100
[root@localhost ~]#
```

외부에서 방화벽으로 요청되는 주소로 내부 사설 IP로 변합합니다.

외부 네트워크 공인IP인 eth2:1를 통하여 DMZ서버인 172.16.0.100/24 IP의 서버로 들어오는 입력패킷의 TCP프로토콜인 22(ssh),80(http),443(https)를 허용하도록 DNAT설정을 합니다.

< Trsut에서 UnTrust 구간 DNS 서비스 허용 >

■ 상태추적이란?

Stateful Inspection이라고 하며 상태기반 감시를 말합니다. 일정 시간 동안 통신 패킷을 추적함으로써 보다 강화된 보안을 제공합니다. 송수신 되는 모든 패킷들을 검사하는데 특정한 형태의 수신 패킷을 요청하는 송신 패킷들도 추적되며, 오직 적절한 응답이라고 판단되는 수신 패킷에 대해서만 방화벽 통과가 허용됩니다. 패킷의 헤더만을 검사하는 정적 패킷 필터링과는 달리, 상태기반 감시는 응용계층 아래에서 분석합니다.

```
[root@localhost ~]# iptables -N T_DNS
iptables: Chain already exists.
[root@localhost ~]# iptables -A T_DNS -p udp --sport 53 -d 10.0.0.0/24 -m state --state NEW,ESTAB
LISHED -j ACCEPT
[root@localhost ~]# iptables -A T_DNS -p udp --dport 53 -s 10.0.0.0/25 -m state --state ESTABLISH
ED -j ACCEPT
[root@localhost ~]# iptables -A FORWARD -j T_DNS
[root@localhost ~]#
```

T_DNS라는 새로운 규칙을 생성한 후, 상태추적이 가능하도록 udp 프로토콜인 DNS(53)를 열어줍니다. dns에 대한 질의와 재귀적 dns를 허용합니다. 외부에서 들어오는 패킷은 새로운 연결을 요청하는 패킷인 NEW와 기본연결의 일부인 패킷인 ESTABLISHED 두 가지를 연결추적 설정합니다. 반대로 내부에서 외부로 나가는 설정은 기본연결만 설정한 후에 포워딩합니다.

```
Windows IP Configuration


Ethernet adapter 로컬 영역 연결:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.0.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.0.254

C:₩Documents and Settings₩Administrator>nslookup
Default Server:  kns.kornet.net
Address:  168.126.63.1

> www.naver.com
Server:  kns.kornet.net
Address:  168.126.63.1

Non-authoritative answer:
Name:    www.naver.com.nheos.com
Addresses:  210.89.164.90, 125.209.222.141
Aliases:  www.naver.com
```

규칙을 선정 후 XP에서 nslookup명령을 통하여 통신 원활히 되는지 확인합니다.

< Trust에서 모든 구간 WEB서비스(http,https) 허용 >

```
[root@localhost ~]# iptables -N T_WEB
iptables: Chain already exists.
[root@localhost ~]# iptables -A T_WEB -p tcp -m multiport --dport 80,443 -j ACCEPT
```

먼저 T_WEB이라는 새로운 규칙을 생성한 후 80(http),443(https)번 포트를 허용하도록 지정합니다.

■ 내부사용자 WEB 서비스 허용

```
[root@localhost ~]# iptables -A T_WEB -p tcp -m multiport --dport 80,443 -s 10.0.0.0/24 -m state
--state NEW -m limit --limit-burst 10 --limit 10/m -j LOG --log-prefix "[T_WEB]"
[root@localhost ~]# iptables -A T_WEB -p tcp -m multiport --dport 80,443 -s 10.0.0.0/24 -m state
--state NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A T_WEB -p tcp -m multiport --sport 80,443 -d 10.0.0.0/24 -m state
--state ESTABLISHED -j ACCEPT
```

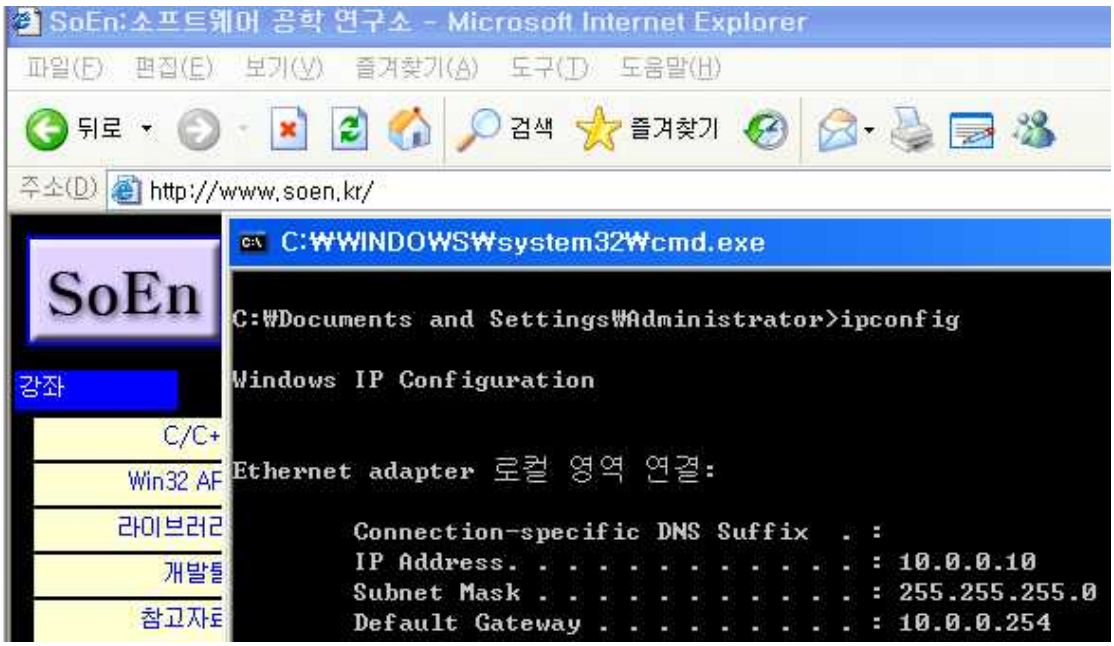
먼저 조건에 따라 로그를 먼저 남긴후 트래픽을 허용하도록 설정합니다.
연결이 되었을시 10회 저장 후 분당 10번씩 로그가 저장되도록 설정합니다. 10.0.0.0/24 대역으로 오는 모든 패킷에 대해 WEB 서비스를 허용하도록 설정합니다.

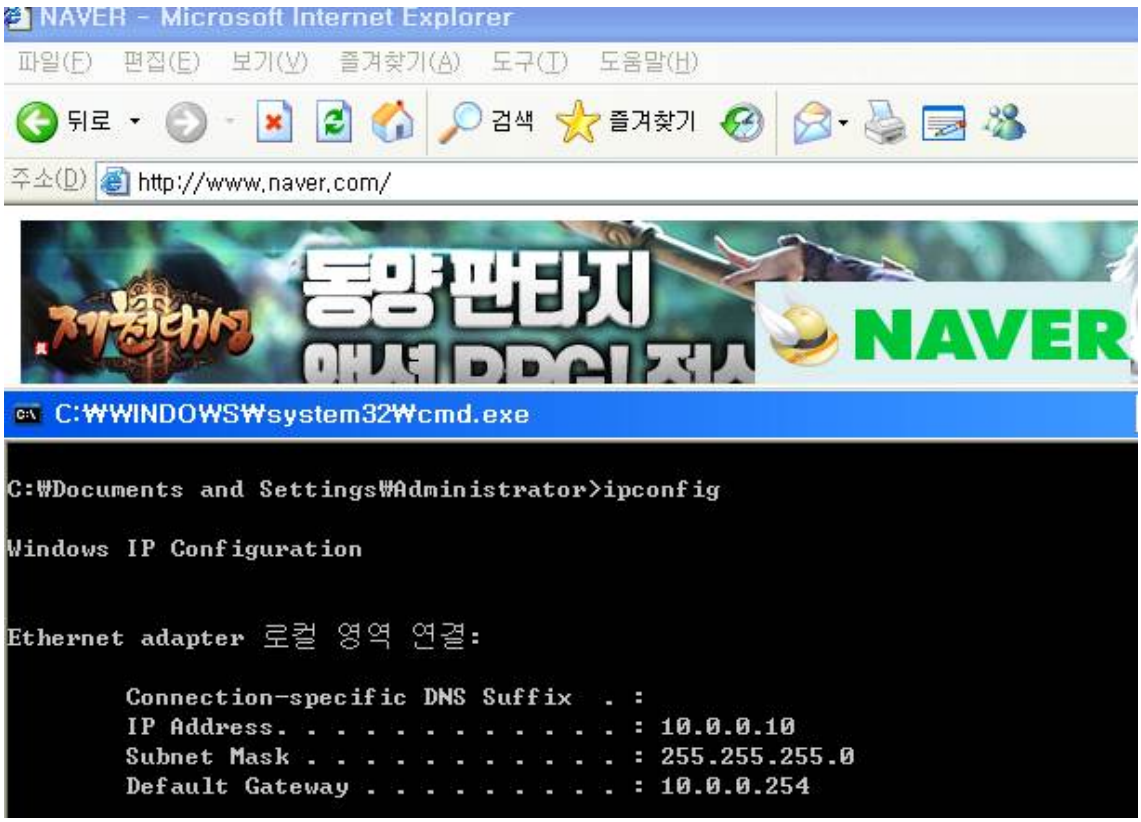
```
[root@localhost ~]# iptables -A FORWARD -j T_WEB
[root@localhost ~]#
```

모든 설정을 완료한 후 포워딩합니다.

이후 WEB서비스가 가동되고 있는지 Inter_Host(XP)에서 확인합니다.
다음으로 넘어갑니다.

■ 내부사용자(XP) WEB 서비스 확인





http와 https 서비스 모두 가동되는 것을 확인합니다.

< Trust에서 UnTrust 구간 FTP 서비스(Active/Passive) 허용 >

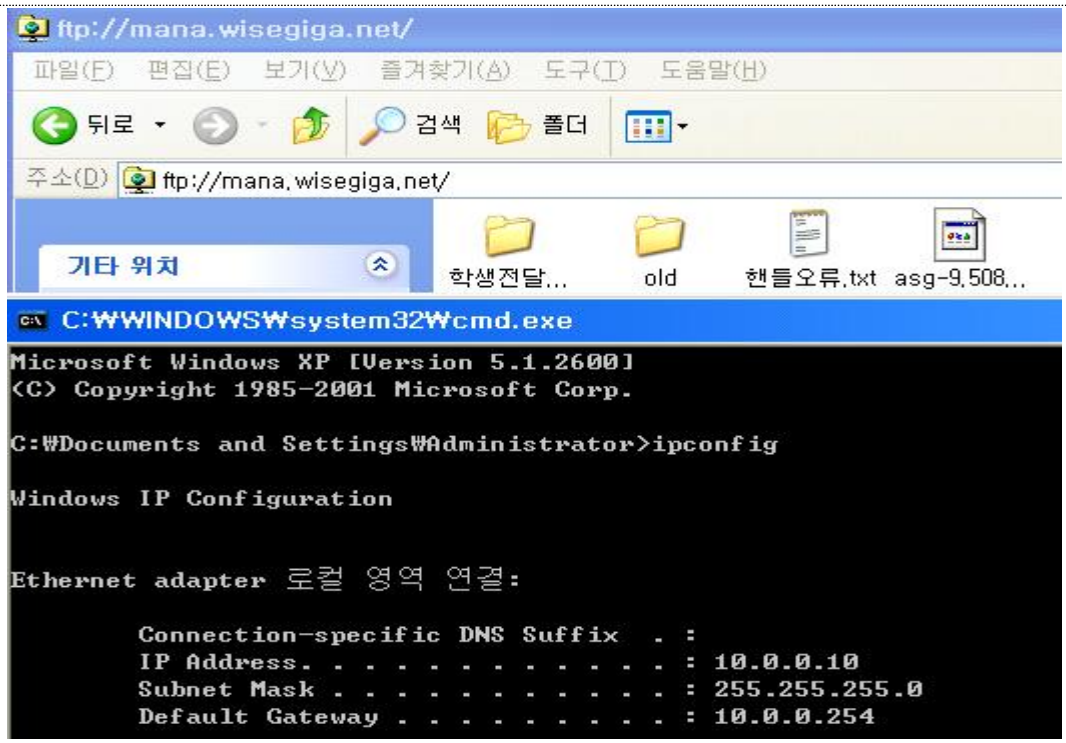
FTP에는 액티브와 패시브 모드 2가지가 존재합니다. 액티브모드에서는 외부에서 오는 데이터를 차단하기 때문에 일반적으로 불가능하며 패시브모드에서는 서버가 임의의 데이터 전송포트를 생성하여 클라이언트가 접속하도록 유도하여 데이터를 주고받습니다.

```
[root@localhost ~]# iptables -A T_FTP -p tcp -m multiport --dport 20,21 -s 10.0.0.0/24 -m state -
-state NEW -m limit --limit-burst 20 --limit 7/s -j LOG --log-prefix "[T_FTP]"
[root@localhost ~]# iptables -A T_FTP -p tcp -m multiport --dport 20,21 -s 10.0.0.0/24 -m state -
-state NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A T_FTP -p tcp -m multiport --sport 20,21 -d 10.0.0.0/24 -m state -
-state ESTABLISHED,RELATED -j ACCEPT
[root@localhost ~]# iptables -A FORWARD -j T_FTP
```

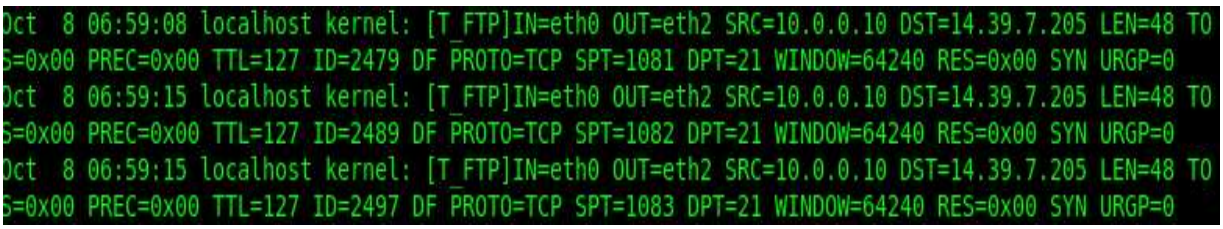
T_FTP라는 새로운 규칙을 생성한 후 조건대로 20회 저장후 초당 7번씩 로그를 저장하도록 설정합니다. 내부 네트워크로부터 20,21번 포트에 대한 새로운 연결과 기본연결을 허용하고 내부네트워크로 들어오는 20,21번 포트에 대해서는 기본 연결과 새로운 연결(RELATED)을 허용합니다. 21번으로 연결했다면 20번으로 데이터 전송을 하기 때문에 이 설정은 필요합니다. 설정을 끝내고 포워딩을 합니다.

```
[root@localhost ~]# iptables -A T_FTP -p tcp --dport 1024:65535 -s 10.0.0.0/24 -m state --state N
EW,ESTABLISHED,RELATED -j ACCEPT
[root@localhost ~]# iptables -A T_FTP -p tcp --sport 1024:65535 -d 10.0.0.0/24 -m state --state E
STABLISHED,RELATED -j ACCEPT
```

실질적으로 데이터 전송이 가능하도록 Wellknown 포트를 제외한 1024~65535 포트에 대한 연결을 개방합니다.
설정을 끝내고 다음은 내부에서 FTP서비스에 대한 테스트를 진행하겠습니다.



위와 같이 XP에서 외부로 FTP접속을 시도한 결과 정상적으로 데이터 목록을 불러 올 수 있었습니다.



로그파일에도 FTP 접속에 관한 트래픽이 정상적으로 기록되는 것을 확인합니다.

< 일베 접속 차단 >

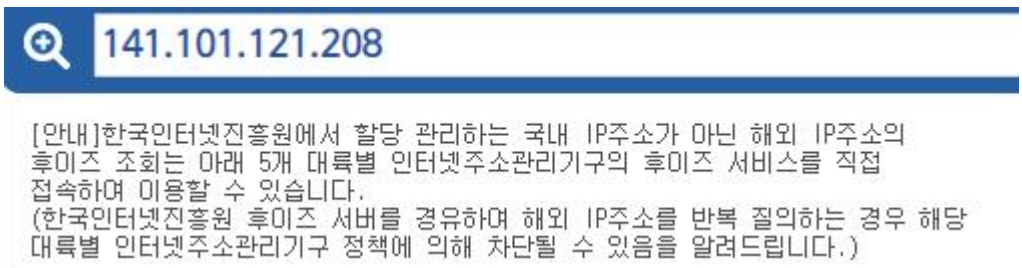
www.ilbe.com 라는 사이트에 접속하지 못하도록 차단합니다.

조건에 따라 3회 저장후 분당 10번씩 로그가 기록되도록 설정합니다.

먼저 www.netcraft.com 에서 정보수집을 합니다.

Site	http://www.ilbe.com	Netblock Owner	CloudFlare CDN network
Domain	ilbe.com	Nameserver	nia.ns.cloudflare.com
IP address	141.101.121.208 (VirusTotal)	DNS admin	dns@cloudflare.com
IPv6 address	2400:cb00:2048:1:0:0:8d65:79cf	Reverse DNS	unknown
Domain registrar	gabia.com	Nameserver organisation	whois.cloudflare.com
Organisation	Whois Privacy Services by gabia, U-Space1 Complex B, 4F, 660, Daewangpangyo-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Gyeonggi, 463400, KR	Hosting company	unknown
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	EU		

정보검색을 해본 결과 CloudFlare라는 호스팅업체의 서비스를 이용하고 있는 것을 확인하였습니다. 해외 IP인 141.101.121.207 ~ 208을 이용하고 있습니다.



국내 whois.kisa.or.kr 에서는 조회되지가 않습니다.

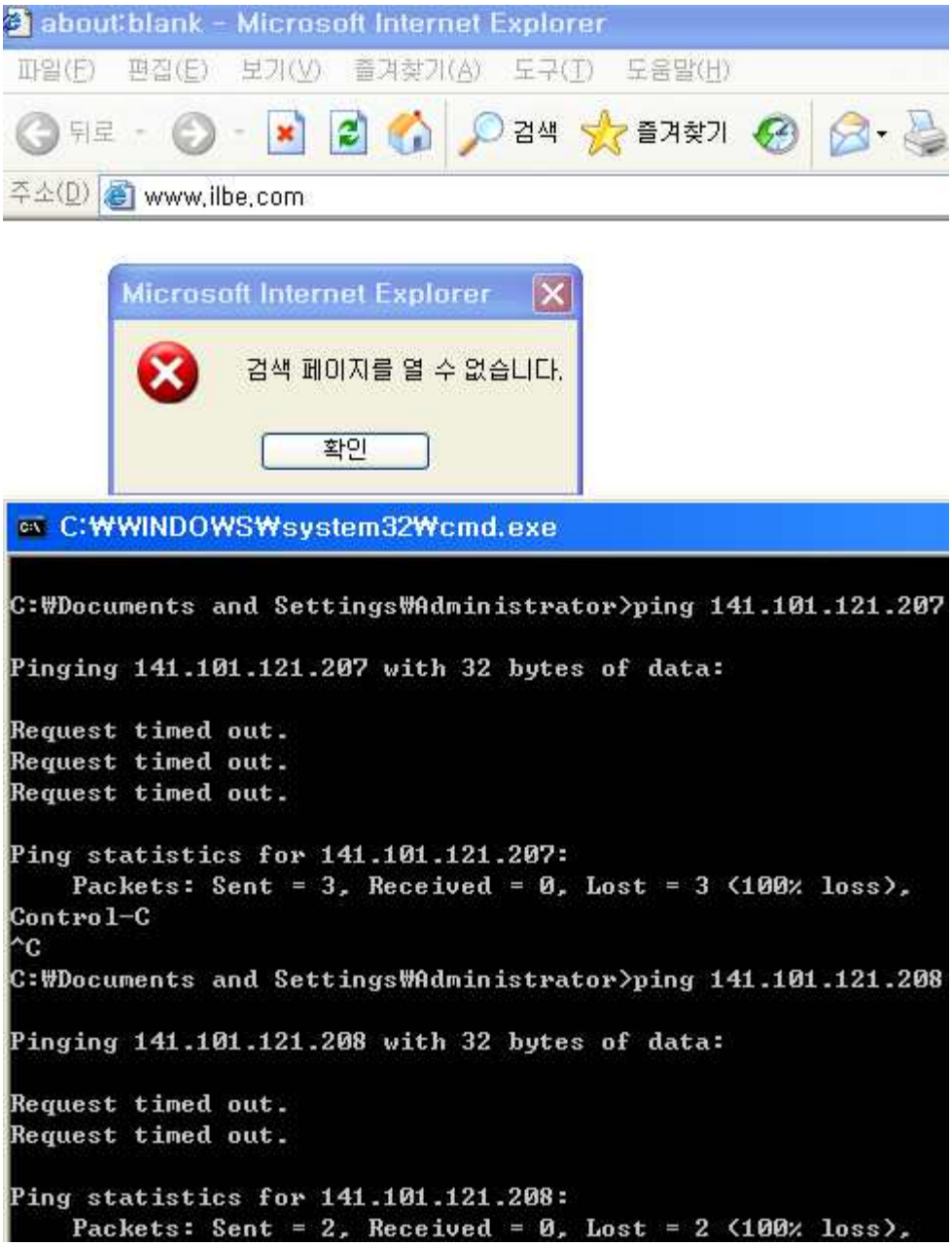
```
[root@localhost ~]# iptables -N T_ILBE
[root@localhost ~]# iptables -A T_ILBE -p tcp -d 141.101.121.208 -j DROP
[root@localhost ~]# iptables -A T_ILBE -p tcp -d 141.101.121.207 -j DROP
[root@localhost ~]# iptables -I FORWARD -j T_ILBE
```

T_ILBE라는 새로운 규칙을 생성하고 141.101.121.207~207 ip를 차단합니다. 일베를 차단하기 위한 새로운 규칙을 T_WEB보다 먼저 적용되도록 순서를 맨위로 올린 후 포워딩합니다.

```
[root@localhost ~]# iptables -A T_ILBE -p tcp -m multiport --dport 80,443 -d 141.101.121.0/24 -m
state --state NEW -m limit --limit-burst 3 --limit 10/m -j LOG --log-prefix "[T_ILBE]"
```

그리고 조건에 맞게 141.101.121.0/24 대역대에 http,https로 접속을 시도할 경우 3회 저장 후 분당 10번씩 저장되도록 설정합니다.

iptables를 이용하지 않고는 윈도우 내의 호스트파일을 수정하여 일베사이트에 접속하지 못하도록 수정하는 방법이 있겠습니다.



내부네트워크 사용자인 Internal_Host(XP)에서 일베에 접속을 요청한 결과 ip가 차단되어 접속하지 못하는 것을 확인합니다.

4. Untrust site 정책 구성

< DMZ의 WEB 서버 접근을 제외한 모든 통신 차단 >

```
[root@localhost ~]# iptables -A U_WEB -p tcp -m multiport --sport 80,443 -d 172.16.0.100 -m state
 --state NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A U_WEB -p tcp -m multiport --dport 80,443 -s 172.16.0.100 -m state
 --state ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A FORWARD -j U_WEB
```

앞서 화이트 리스트구성으로 모든패킷은 막혀있습니다.

따라서 웹 서버인 172.16.0.100으로 향하는 http,https서비스를 허용한 후 포워딩합니다.

< UnTrust 구간 관리자 PC에서 DMZ_WebServer로 SSH 접속 허용 >

```
이더넷 어댑터 이더넷:

   연결별 DNS 접미사. . . . : kornet
   링크-로컬 IPv6 주소 . . . . : fe80::81d6:8ea4:15c4:bd2a%13
   IPv4 주소 . . . . . . . . . : 183.98.126.86
   서브넷 마스크 . . . . . . . : 255.255.255.0
   기본 게이트웨이 . . . . . . : 183.98.126.254
```

먼저 호스트 pc인 Admin_Desktop의 ip입니다.

```
[root@localhost ~]# iptables -N U_SSH
[root@localhost ~]# iptables -A U_SSH -p tcp --dport 22 -s 183.98.126.86 -d 172.16.0.100 -m state
 --state NEW,ESTABLISHED -j ACCEPT
[root@localhost ~]# iptables -A U_SSH -p tcp --sport 22 -d 183.98.126.86 -s 172.16.0.100 -m state
 --state ESTABLISHED -j ACCEPT
```

U_SSH라는 새로운 규칙을 생성한후 호스트 pc의 ip를 허용한후 포워딩합니다.

```
C:₩WINNT₩system32₩cmd.exe - nc -lvp 22

C:₩>nc -lvp 22
listening on [any] 22 ...
```

2K 서버에서 22번포트를 열어줍니다. 호스트 pc에서 PuTTY를 통하여 ssh 접속을 시도합니다.

```
선택 C:₩WINNT₩system32₩cmd.exe - nc -lvp 22
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:₩>nc -lvp 22
listening on [any] 22 ...
183.98.126.86: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [172.16.0.100] from (UNKNOWN) [183.98.126.86] 57219: NO_DATA
```

host로부터 22번을 통한 접속이 시도된 것을 확인 합니다.