PBL 과제 풀이 및 모범답안

문제 1 – 소규모 사무실 네트워크 인프라 기본 설계

문제 풀이

이 문제는 사설 IP 를 이용한 기본 네트워크 설계 능력을 묻는 과제입니다. 클래스 C 주소대역(192.168.x.x/24)을 기준으로, 5 개의 PC 에 각기 다른 IP 를 수동으로 부여하고, 기본 게이트웨이는 공유기의 IP(예: 192.168.10.1)로 설정합니다. PC 간 통신 및 인터넷이 가능해야 합니다.

모범답안 예시

- IP 할당표:
  - PC1: 192.168.10.11
  - PC2: 192.168.10.12
  - ...
- 구성도: 공유기 – 스위치 – PC1~5
- Ping 결과: 각 PC 에서 ping 192.168.10.1 및 상호 ping 수행 결과 캡처

문제 2 – 라우팅 테이블 오류 진단 및 수정

문제 풀이

Traceroute 결과를 통해 중간 홉에서 경로가 끊기거나 잘못된 라우팅 설정이 확인되면, 해당 라우터에서 정적 라우트를 수정해야 합니다.

모범답안 예시

- 문제 원인: 본사 라우터에 지사 네트워크(192.168.1.0/24)에 대한 라우트 누락
- 수정 명령: ip route 192.168.1.0 255.255.255.0 10.0.0.2
- 캡처: 라우팅 테이블 수정 전후 비교

문제 3 – 초기 방화벽 ACL 정책 적용

문제 풀이

HTTP(80), HTTPS(443)만 허용하고 나머지는 차단해야 합니다. ACL 규칙은 순서대로 적용되므로, 반드시 마지막에 deny all 을 추가해야 합니다.

모범답안 예시

- 예시 ACL:
  - permit tcp any any eq 80
  - permit tcp any any eq 443
  - deny ip any any
- 테스트 결과: 포트 80 은 접속 성공, 포트 22, 25 는 차단됨 확인

문제 4 – NAT 설정 실습

문제 풀이

1. 내부 PC 가 사용할 IP 및 기본 게이트웨이 설정 (예: 192.168.10.10 / 192.168.10.1)
2. 라우터의 내부/외부 인터페이스에 IP 및 NAT 역할 지정
3. PAT 설정: ACL 작성 및 NAT 오버로드 설정
4. ping 테스트 및 NAT 변환 확인.

모범답안 예시

1. NAT 설정 명령어 (Cisco)

```
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
interface FastEthernet0/1
 ip address 203.0.113.2 255.255.255.0
 ip nat outside
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface FastEthernet0/1 overload
```

2. 확인 명령어

```
ping 203.0.113.1
show ip nat translations
```

결과 스크린샷 제출 예시

- ping 결과 성공 스크린샷

- show ip nat translations 명령 결과 스크린샷

분석 및 비교 정리

구분	설정 전	설정 후
인터넷 접속 가능 여부	X	O
NAT 테이블 확인	없음	매핑 생성됨
PC 에서 외부와 통신 가능	불가	가능

문제 5 – VPN 기본 구성 실습

문제 풀이

5. Router A, B 의 내부/외부 인터페이스 설정
6. GRE 터널 인터페이스(Tunnel0) 구성
7. Tunnel IP 부여 및 상대방 설정
8. 정적 라우팅으로 내부망 연동
9. ping 테스트

모범답안 예시

1. GRE 터널 구성 (Router A/B)

interface Tunnel0

ip address 172.16.0.1 255.255.255.0 (A)

tunnel source 10.0.0.1

tunnel destination 10.0.0.2

interface Tunnel0

ip address 172.16.0.2 255.255.255.0 (B)

tunnel source 10.0.0.2

tunnel destination 10.0.0.1

2. 정적 라우팅 명령어

Router A: ip route 192.168.20.0 255.255.255.0 172.16.0.2

Router B: ip route 192.168.10.0 255.255.255.0 172.16.0.1

결과 스크린샷 제출 예시

- Branch A PC 에서 Branch B PC 로 ping 성공 화면

- show ip route 결과

- show interface tunnel0 결과

분석 및 비교 정리

구분	설정 전	설정 후
PC 간 통신	불가	가능
라우팅 상태	직접 연결 없음	터널 경유 라우팅 생성
Tunnel 상태	down/down	up/up

문제 6 – TCP SYN Flooding 공격 실습 및 방어

문제 풀이

10. 공격자 시스템(hping3 사용)에서 대상 웹 서버로 SYN Flooding 공격 수행
11. 피해 서버에서 netstat 또는 ss 명령어로 SYN_RECV 상태 확인
12. 커널 설정 또는 iptables 를 통해 SYN Flooding 방어 조치 적용
13. 공격 전/후 상태를 비교하여 방어 효과 분석

모범답안 예시

1. 공격자에서 SYN Flood 생성

```
sudo hping3 -S --flood -V -p 80 192.168.100.10
```

2. 피해 서버에서 확인 명령어

```
sudo netstat -ant | grep SYN_RECV
```

또는

```
sudo ss -n state syn-recv
```

3. 방어 조치 – 커널 설정

```
sudo sysctl -w net.ipv4.tcp_syncookies=1
```

4. 방어 조치 – iptables 설정

```
sudo iptables -A INPUT -p tcp --syn -m limit --limit 5/s --limit-burst
10 -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --syn -j DROP
```

결과 스크린샷 제출 예시

- 스크린샷 1: 공격 전 netstat 또는 ss 명령어 결과 (SYN_RECV 다수 확인)

- 스크린샷 2: 방어 설정 후 SYN_RECV 감소 확인

- 스크린샷 3: 웹 서비스 정상 응답 상태 유지 여부 확인

분석 및 비교 정리

구분	공격 전	공격 후
SYN_RECV 수	50 개 이상 지속 증가	5~10 개 이내로 감소
CPU 사용률	과부하 발생	안정 유지
웹 서비스 응답	지연 또는 다운	정상 유지