네트워크 보안의 이해

네트워크 보안(Network Security)

- “네트워크 인프라, 장비, 데이터, 사용자 등을 외부의 위협이나 내부의 침해로부터 보호하기 위한 기술, 정책, 절차의 집합” 입니다.

네트워크 보안의 목적

- 기밀성(Confidentiality): 인가된 사용자만 정보에 접근
- 무결성(Integrity): 정보가 변조되지 않도록 보장
- 가용성(Availability): 언제든지 정보에 접근 가능하게 유지

왜 네트워크 보안이 필요한가?

- 네트워크는 공격의 경로가 될 수 있음
- 사용자 인증 필요성 증가
- 민감 정보 보호 필요
- 서비스 중단(DDoS 등) 방지 필요

주요 보안 위협 유형

- 사회공학: 피싱 등 심리 기법
- DoS/DDoS: 서비스 중단 공격
- 스푸핑: MAC/IP 위장
- 패킷 스니핑: 패킷 탈취
- MITM: 중간자 공격

네트워크 보안 적용 대상

- 네트워크 장비: 라우터, 스위치, 방화벽 등
- 사용자 계정: 인증, 권한 설정
- 데이터 흐름: 트래픽 필터링, 암호화
- 운영 정책: 로그, 백업, 업데이트

네트워크 보안 기법 개요

- 방화벽: 트래픽 필터링
- 포트 보안: MAC 수 제한
- IDS/IPS: 침입 탐지 및 차단
- VLAN: 네트워크 분리
- ACL: IP/포트 제어
- DHCP Snooping, ARP Inspection : ARP/DHCP 스푸핑 대응
- VPN, IPsec, 인증서 기반 보안

보안 장비 및 역할

- 방화벽: 접근 제어
- IDS: 침입 탐지
- IPS: 탐지 + 차단
- NAC: 인증된 장비만 접속
- 보안 스위치: 다양한 보안 기능