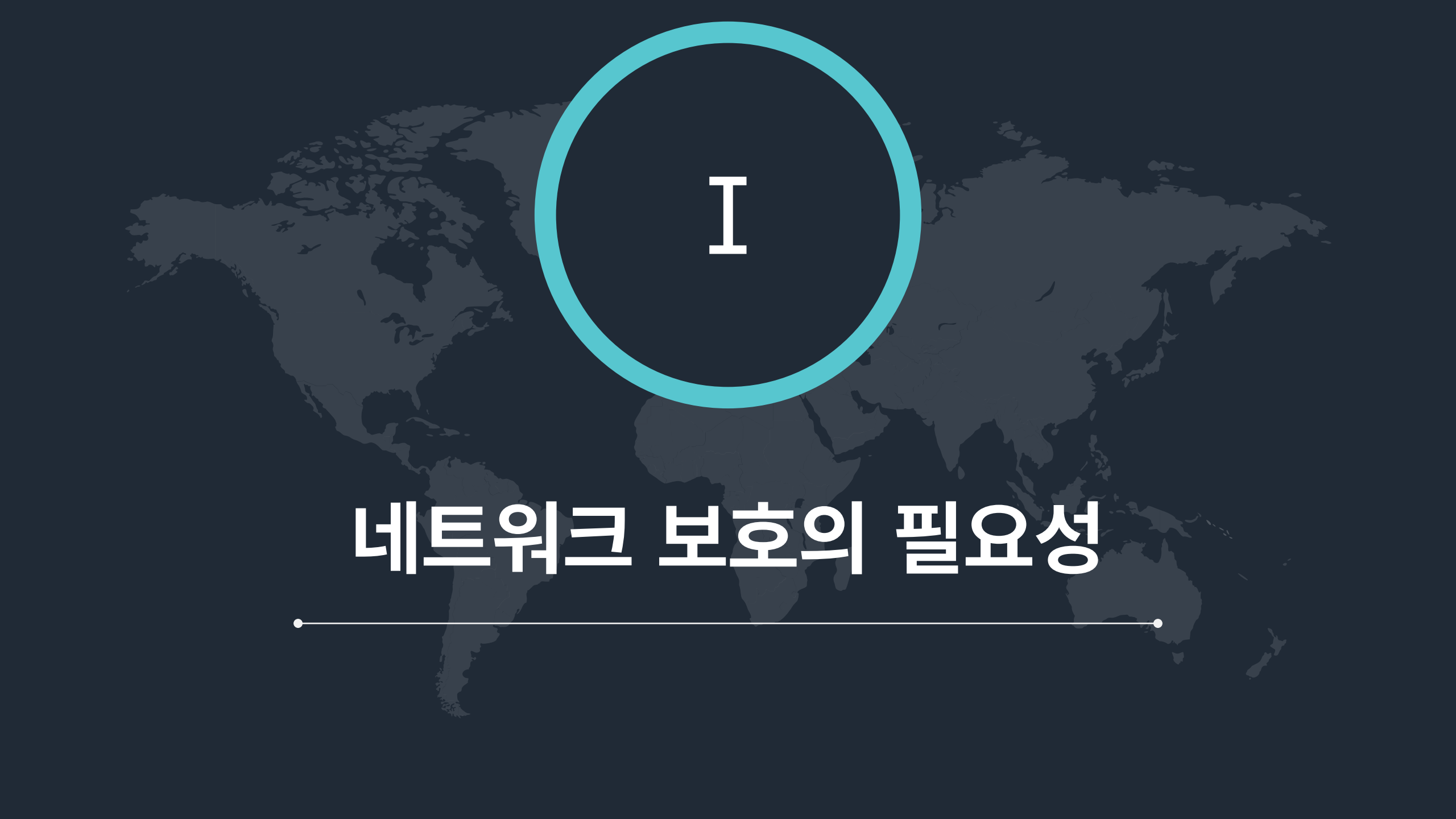
CHAPTER 06

네트워크 보호

이현호 hyeonholee@korea.com

목차



I

네트워크 보호의 필요성

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

보안관제사

보안관제 시스템

SIEM(보안 정보 및 이벤트 관리)

법규 준수 및 콤플라이언스 관리

로그(보안 정보 및 이벤트 기록)

정보보호 시스템

방화벽, IDPS, NAC, NDR, DDoS 대응 등

안티 바이러스, EDR, DLP, 호스트 방화벽, 보안OS 등

웹쉘 탐지, 웹변조 탐지, 취약점 진단 등

DB 암호화, DB 접근통제 등

보호 대상 정보자산

네트워크 장비

호스트 (서버, 단말기 등)

응용프로그램

데이터베이스 관리시스템

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

보안관제사

보안관제 시스템

SIEM(보안 정보 및 이벤트 관리)

법규 준수 및 콤플라이언스 관리

로그(보안 정보 및 이벤트 기록)

정보보호 시스템

방화벽, IDPS, NAC, NDR, DDoS 대응 등

안티 바이러스, EDR, DLP, 호스트 방화벽, 보안OS 등

웹쉘 탐지, 웹변조 탐지, 취약점 진단 등

DB 암호화, DB 접근통제 등

보호 대상 정보자산

네트워크 장비

호스트 (서버, 단말기 등)

응용프로그램

데이터베이스 관리시스템

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

▪ 정보통신망 및 정보시스템

- 보호 대상 정보자산으로 구성되는 보안관제의 대상

네트워크 장비	• 라우터 • 허브 • 스위치 • 모뎀 • 리피터 • 무선 AP 등
호스트 (컴퓨터)	• 서버 : 자료 · 정보를 종합 · 처리하며 **정보시스템의 환경과 기능을 제공**하는 컴퓨터 • 단말기 : 서버에 접속하여 **서버의 자원을 활용**하는 컴퓨터로 실제 사용자들이 **정보의 입 · 출력**을 위해 사용
응용프로그램	• 정보시스템의 목적을 달성하기 위해 **관련 기능들을 제공**하는 컴퓨터 프로그램
데이터베이스 관리시스템	• **데이터베이스를 처리 · 관리**하기 위한 소프트웨어

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

▪ 정보통신망 및 정보시스템의 법령상 정의

지능정보화 기본법(법률, 과학기술정보통신부) :: 제2조(정의)

⑧ "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체제를 말한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률, 과학기술정보통신부) :: 제2조(정의)

① "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체제를 말한다.

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

- **정보통신망 및 정보시스템의 법령상 정의**

전자정부법(법률, 행정안전부) :: 제2조(정의)

⑬ "정보시스템"이란 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

보안관제사

보안관제 시스템

SIEM(보안 정보 및 이벤트 관리)

법규 준수 및 콤플라이언스 관리

로그(보안 정보 및 이벤트 기록)

정보보호 시스템

방화벽, IDPS, NAC, NDR, DDoS 대응 등

안티 바이러스, EDR, DLP, 호스트 방화벽, 보안OS 등

웹쉘 탐지, 웹변조 탐지, 취약점 진단 등

DB 암호화, DB 접근통제 등

보호 대상 정보자산

네트워크 장비

호스트 (서버, 단말기 등)

응용프로그램

데이터베이스 관리시스템

I 네트워크 보호의 필요성

1 보안관제시스템의 구성

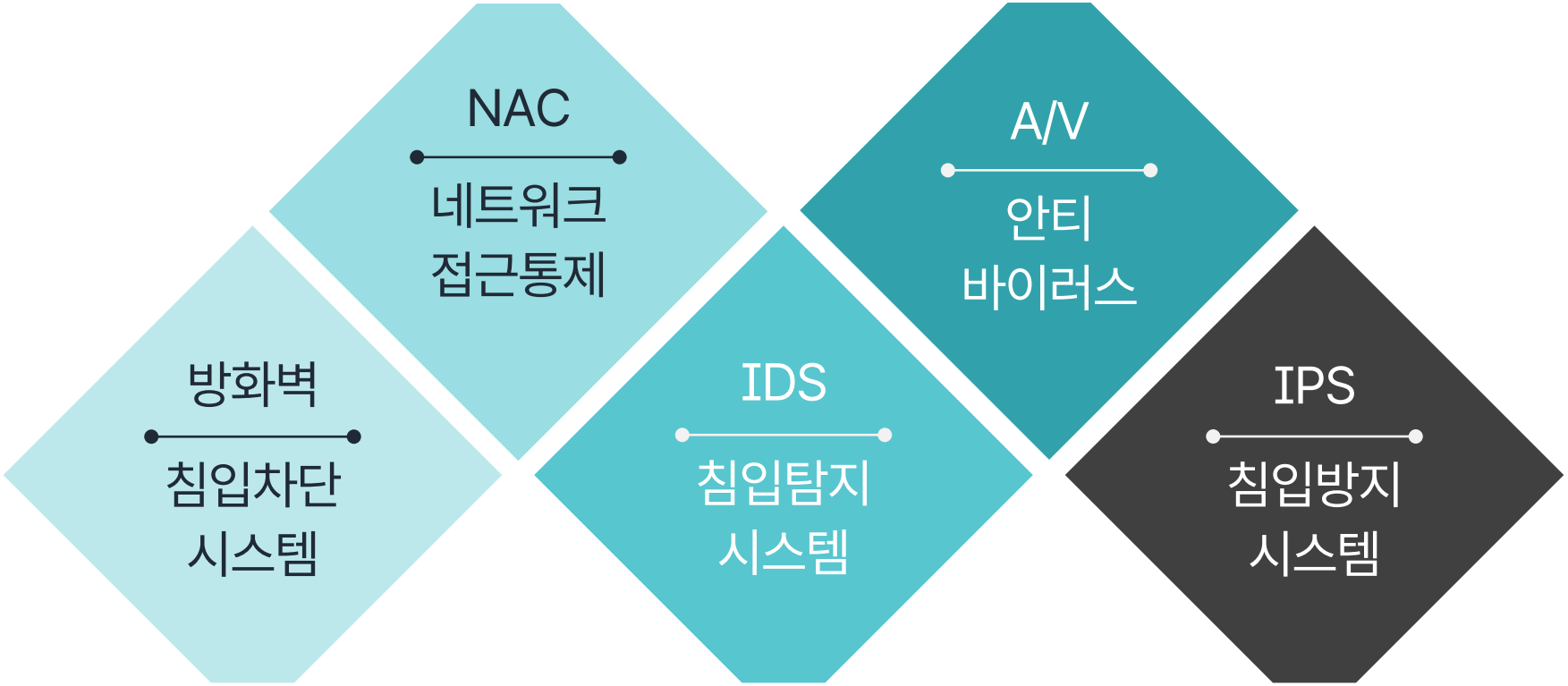
- **정보보호시스템**
  - 정보의 접근통제 등을 위해 사용하는 어플라이언스 또는 소프트웨어

어플라이언스	소프트웨어
소프트웨어를 내장한 하드웨어 형태(하드웨어 + 소프트웨어)	호스트에 설치할 수 있는 컴퓨터 프로그램 형태

  - 사이버공격 및 침해시도를 탐지하거나 차단하고 보안 정보 및 이벤트로 보관
  - 과거에는 보안관제사가 개별 정보보호시스템을 각각 들여다보는 방식으로 관제 업무 수행

1 보안관제시스템의 구성

- **정보보호시스템**
  - 주요 정보보호시스템



네트워크 보호의 필요성

1 보안관제시스템의 구성

▪ 정보보호시스템의 법령상 정의

지능정보화 기본법(법률, 과학기술정보통신부) :: 제2조(정의)

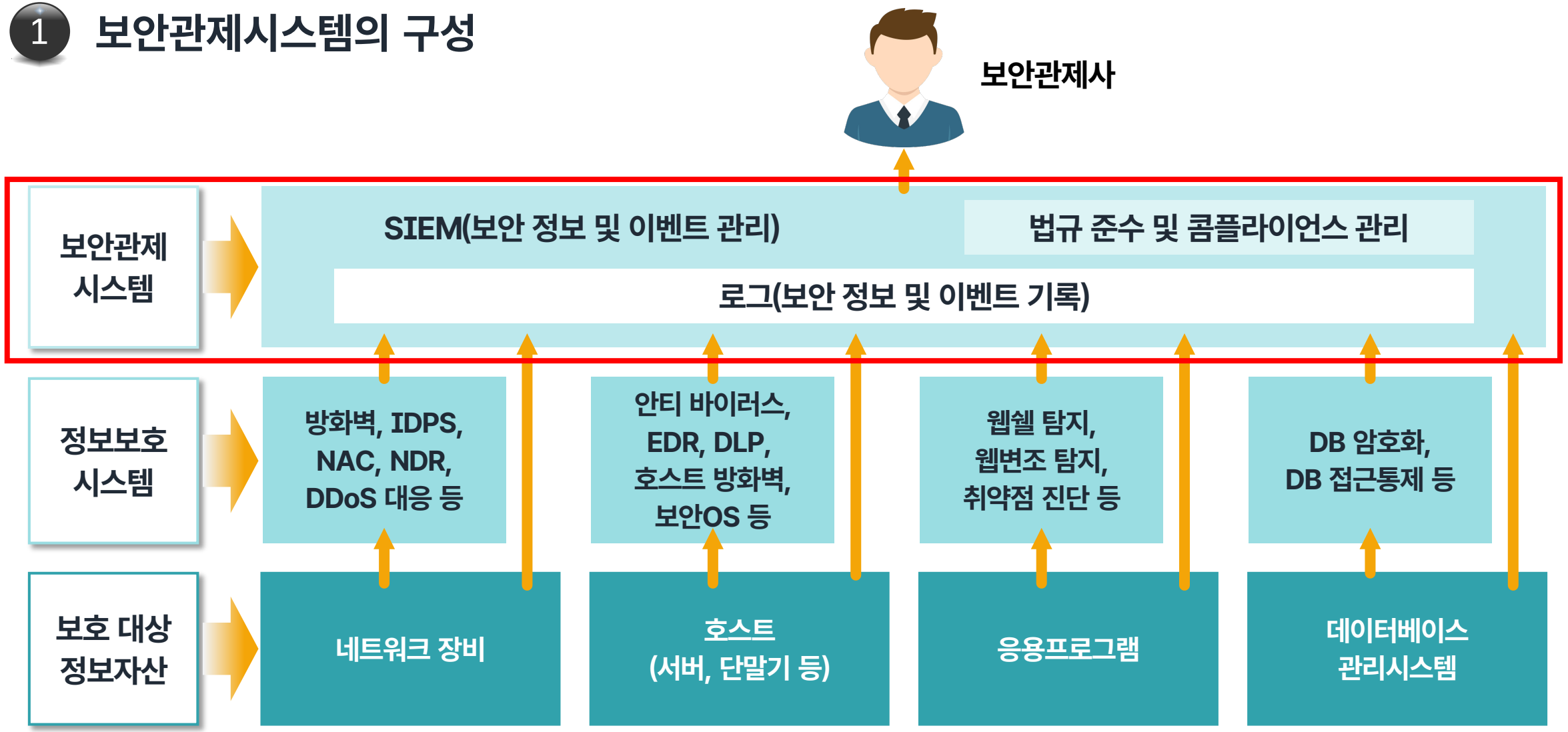
⑮ "정보보호"란 정보의 수집 · 가공 · 저장 · 검색 · 송신 또는 수신 중 발생할 수 있는 정보의 훼손 · 변조 · 유출 등을 방지하기 위한 관리적 · 기술적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다.

국가 정보보안 기본지침(국가정보원 지침, 국가정보원) :: 제2조(정의)

⑳ "정보보호시스템"이라 함은 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.

I 네트워크 보호의 필요성

1 보안관제시스템의 구성



I 네트워크 보호의 필요성

1 보안관제시스템의 구성

- **보안관제시스템**
  - 보안관제 업무를 원활하게 수행할 수 있도록 수집, 분석, 가시화/시각화 등의 기능을 통합적으로 제공

정보시스템·정보통신망, 정보보호체계에 보관된 **보안 정보 및 이벤트 기록을 모아서 보관**하는 기능

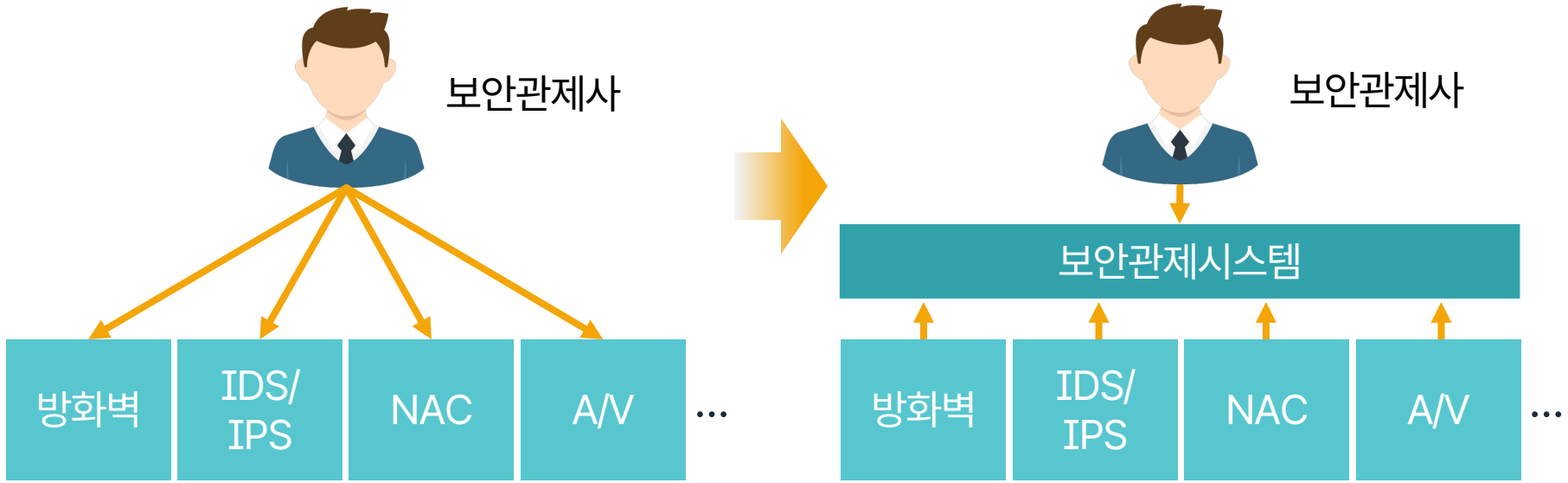
수집된 **보안 정보 및 이벤트 기록을 분석**하는 기능

수집 및 분석된 결과를 보안관제사가 쉽게 이해할 수 있게 **그림, 그래프, 애니메이션 등의 형태로 표현**하는 기능

네트워크 보호의 필요성

1 보안관제시스템의 구성

- **보안관제시스템**
  - 외부의 침해시도 뿐 아니라 내부의 보안위협을 모니터링하는 데에도 활용되며, 최근에는 법규 · 방침 등 콤플라이언스 준수 여부 모니터링 기능을 포함
  - 보안관제시스템 도입 시 보안관제사는 개별 정보보호시스템을 각각 들여다볼 필요 없이 보안관제시스템만 보면 되기 때문에 업무 효율 향상 가능



2 네트워크 보호의 필요성

출처 중국 해킹그룹, 국내 12개 학술기관 해킹, MBC뉴스(2023.01.25), https://www.youtube.com/watch?v=oSnkr3uvk5s

2 네트워크 보호의 필요성

중국 해킹그룹 샤오치잉의 해킹 사례

중국 해킹그룹
샤오치잉 추정
공격자

우리말학회,
대한건설정책연구원 등
국내 12개 학술기관

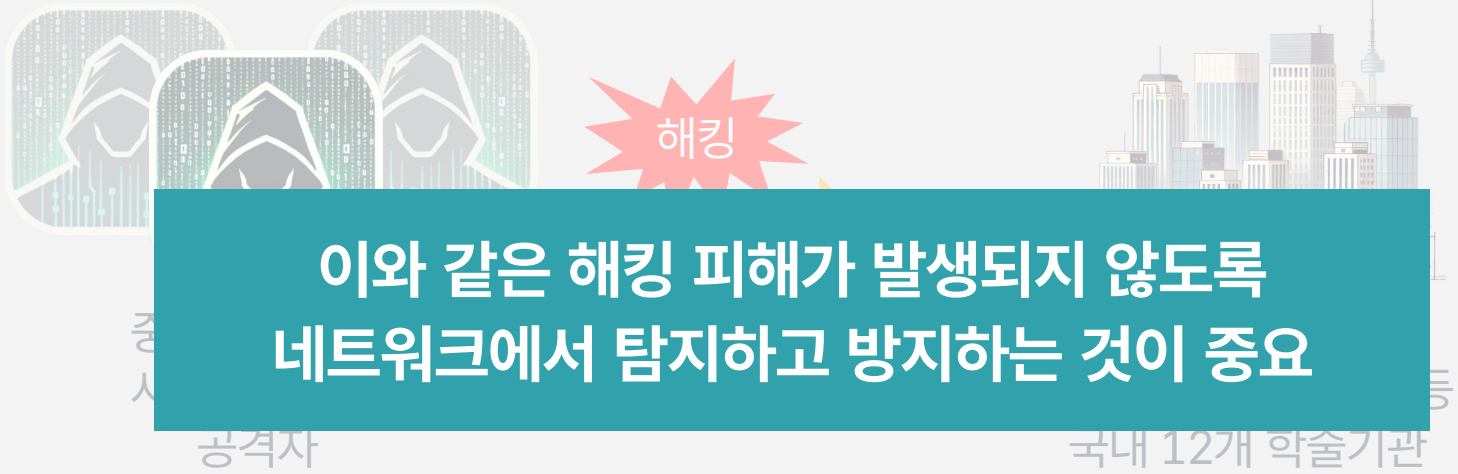
해킹조직 로고와 함께 계속해서 정부 네트워크 추가 해킹 공격 예고 메시지 노출

공개되어서는 안 되는 웹진 신청 이메일 주소 목록 60건의 유출 피해 의심

출처 중국 해킹그룹, 국내 12개 학술기관 해킹, MBC뉴스(2023.01.25), https://www.youtube.com/watch?v=oSnkr3uvk5s

2 네트워크 보호의 필요성

중국 해킹그룹 샤오치잉의 해킹 사례



이와 같은 해킹 피해가 발생되지 않도록
네트워크에서 탐지하고 방지하는 것이 중요

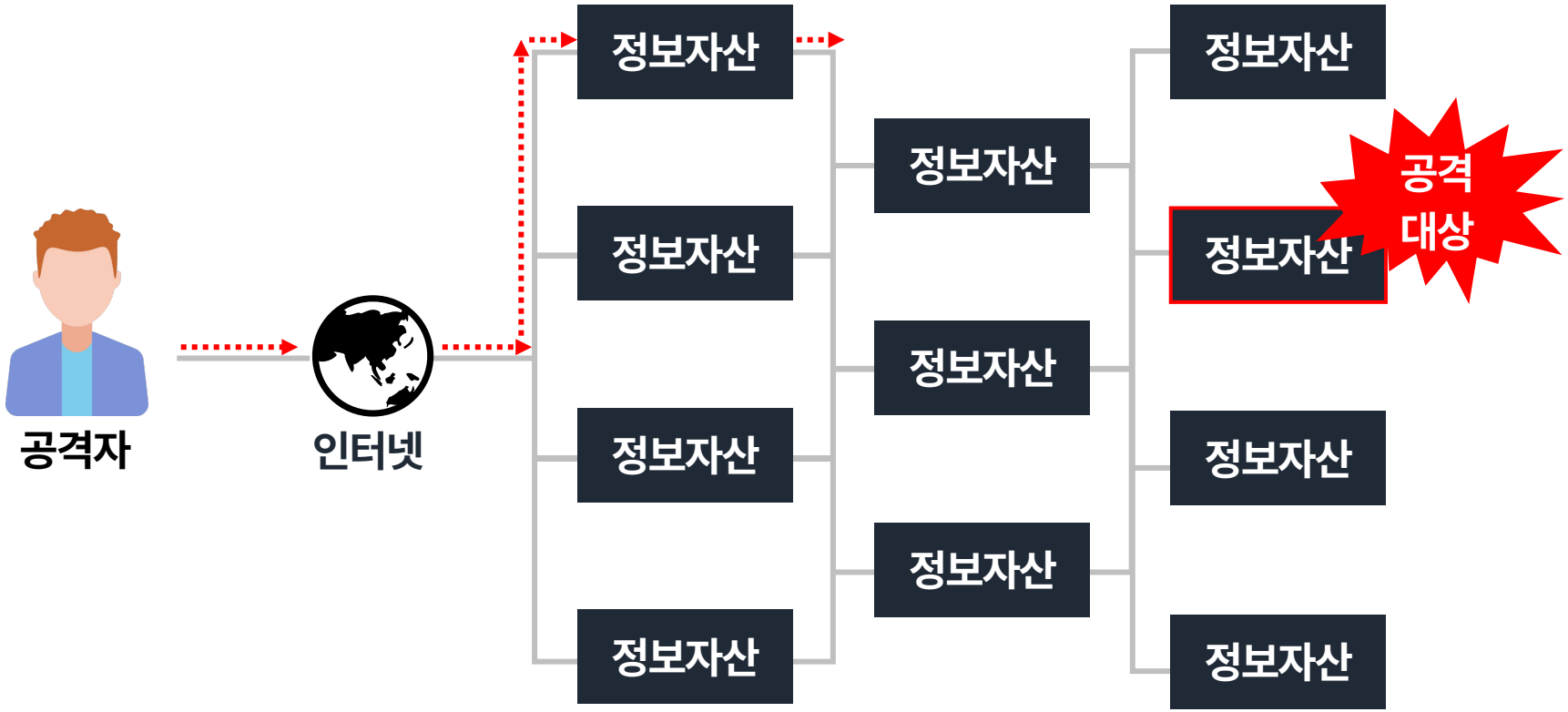
해킹조직 로고와 함께 계속해서 정부 네트워크 추가 해킹 공격 예고 메시지 노출

공개되어서는 안 되는 웹진 신청 이메일 주소 목록 60건의 유출 피해 의심

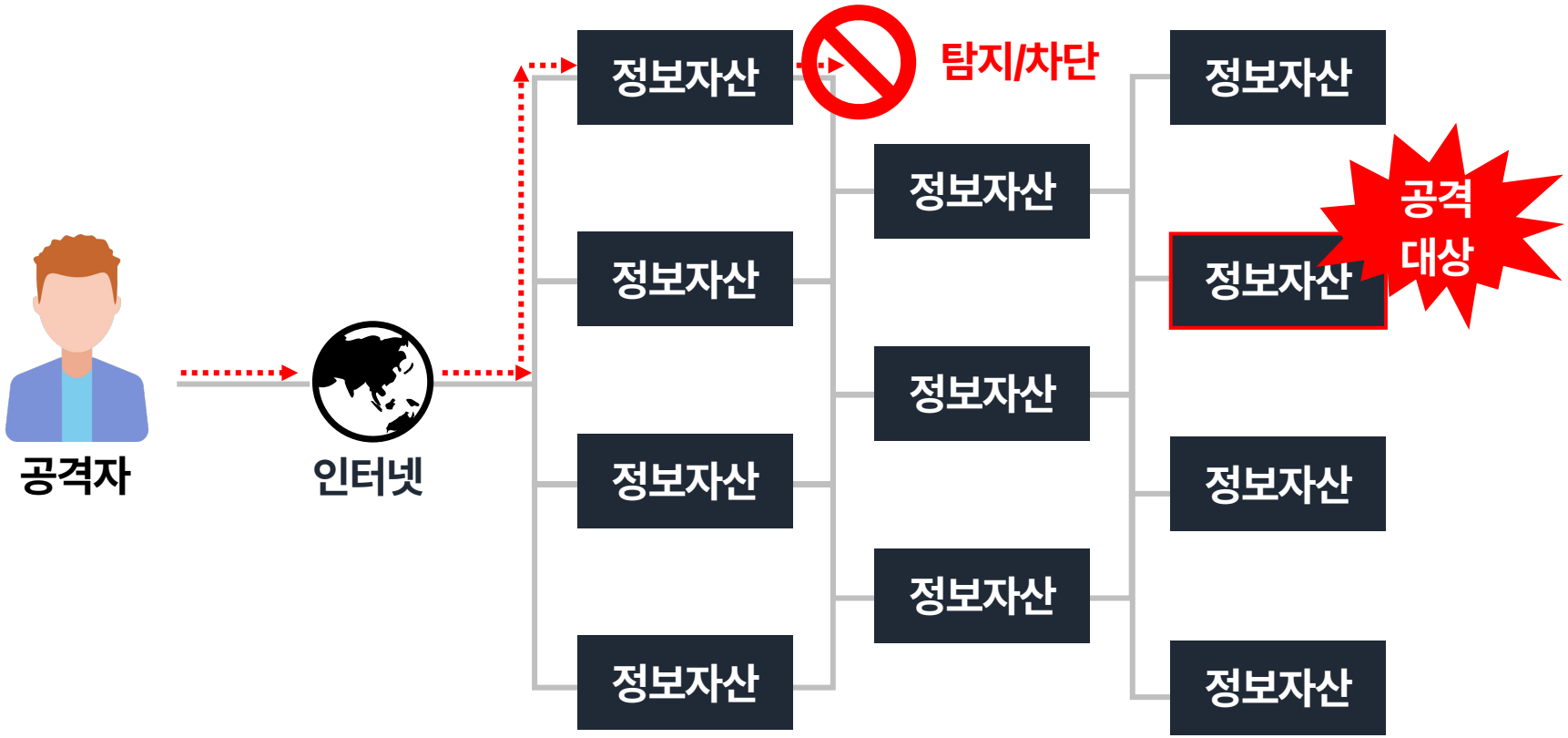
출처 중국 해킹그룹, 국내 12개 학술기관 해킹, MBC뉴스(2023.01.25), https://www.youtube.com/watch?v=oSnkr3uvk5s

2 네트워크 보호의 필요성

2 네트워크 보호의 필요성



2 네트워크 보호의 필요성



3 네트워크 보호의 중요성

사이버 공격

침해 시도

공격 대상
정보자산

침해사고 발생 시 원인을 규명하고 **복구하기 위한 노력**이 많이 필요

침해사고로 이어지기 전, **공격이 들어오는 경계 또는 통로**에서
사이버 공격과 침해 시도를 탐지하여 차단하는 것이 중요

네트워크 보호의 필요성

3 네트워크 보호의 중요성

네트워크 보호

침해사고로 이어지기 전,
사이버 공격이 들어오는
경계 또는 통로에서
침해 시도를 탐지하여
차단하는 것

II

OSI 참조 모형

(OSI 7계층)

II OSI 참조 모형 (OSI 7계층)

1 정보시스템과 네트워크

정보시스템(Information System)

정보를 수집·가공·저장·검색하거나 송신·수신 및 배포하도록 설계·조직화된 시스템

▪ 정보시스템의 형태

스탠드얼론 (Standalone, SA)	네트워크 (Network)
네트워크 연결 없이 **독립적인 단일 컴퓨터**로만 구성된 형태	2대 이상의 컴퓨터를 **통신매체만으로 상호 연결**하거나 **통신장치(네트워크 장비)를 두고 연결**·구성된 형태
단일 컴퓨터는 정보시스템의 최소 단위가 될 수 있음	오늘날 가장 보편적인 형태 구체적으로는 C/S(Client/Server), 웹 기반(Web-based)으로 분류

II OSI 참조 모형 (OSI 7계층)

1 정보시스템과 네트워크

- **네트워크가 일상적인 환경으로 자리잡은 이후 스탠드얼론 형태는 잘 사용되지 않음**
  - 한 번에 한 명의 사용자만 사용할 수 있어 비효율적이기 때문

OSI 참조 모형 (OSI 7계층)

2 네트워크를 통한 자료/정보의 전달

- **네트워크의 구성 단위 구분**

근거리통신망 (Local Area Network, LAN)	광역통신망 (Wide Area Network, WAN)
네트워크의 **최소 단위**	**여러 개의 근거리통신망이** **넓은 지역**에 걸쳐 구성
일반적으로 '네트워크를 구성한다' 내지는 '네트워크 영역을 나눈다'고 할 때 근거리통신망을 기본 단위로 함	기간망(Backbone Network) : 광역통신망에서 효율적인 장거리통신을 위해 주요 노드들을 간선으로 연결하여 중추 역할을 수행하는 최상위 회선을 구축한 것

II OSI 참조 모형 (OSI 7계층)

2 네트워크를 통한 자료/정보의 전달

- 전기 · 전자적 방식이나 빛 등을 활용하여 신호를 주고받는 방법으로 자료/정보를 송 · 수신
- 한 번에 전달할 수 있는 자료/정보의 크기에 물리적 제한

전달에 용이한 크기로 **작게 조각** → 이를 **기본 단위**로 신호를 주고받음

- 각 장치들의 특성을 고려하지 않고 신호를 무작정 흘려보내면 자료/정보가 원활하게 전달될 수 없고 갑작스러운 장애 발생 가능
- 자료/정보를 주고 받는 통신장치들 간 상호 호환 가능한 기술 표준 규격 필요

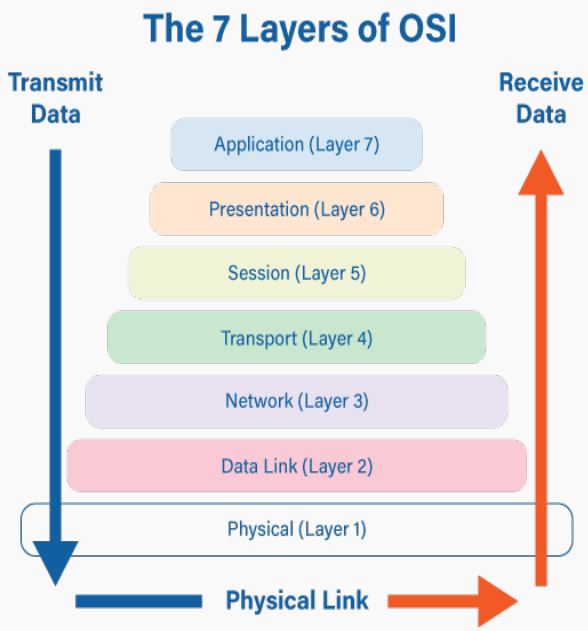
자료/정보 전달 시 각 통신장치 개발사들이 참조할 수 있도록 전달 구조를 국제적인 표준 모형으로 규정 필요

OSI 참조 모형 (OSI 7계층)

3 OSI 참조 모형의 이해

- **OSI : 개방 시스템 간 상호 연결 (Open Systems Interconnection)**

OSI 참조 모형



네트워크를 통해 자료/정보를 전달함에 있어
각 통신장치 개발사들이 참조할 수 있도록
자료/정보의 송신 및 수신 구조를
국제표준화기구(ISO)에서
표준 모형으로 정한 것

OSI 참조 모형 (OSI 7계층)

3 OSI 참조 모형의 이해

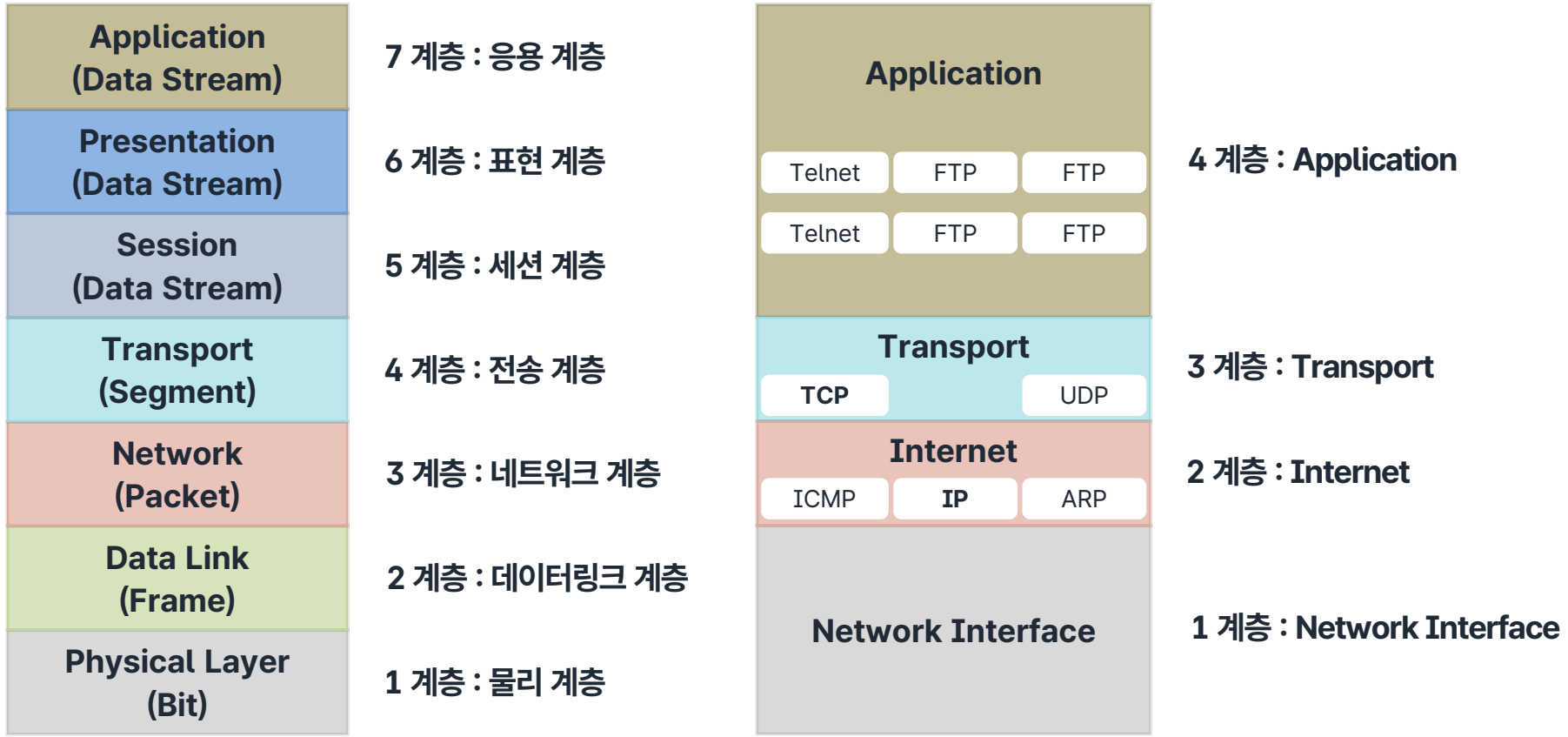
- **OSI 참조 모형은 7개의 계층으로 구성되어 있어 OSI 7계층이라고도 함.**

7계층(응용 계층)	응용서비스	메시지 / 데이터스트림
6계층(표현 계층)	부호화 / 암호화 / 복호화 / 압축	메시지 / 데이터스트림
5계층(세션 계층)	세션 / 동기화 / 오류복구	메시지 / 데이터스트림
4계층(전송 계층)	흐름 · 오류제어(TCP / UDP)	세그먼트
3계층(네트워크 계층)	IP(인터넷 프로토콜) 주소	패킷
2계층(데이터링크 계층)	MAC(매체접근통제) 주소	프레임
1계층(물리 계층)	회선 등 물리적인 통신매체	비트

OSI 참조 모형 (OSI 7계층)

3 OSI 참조 모형의 이해

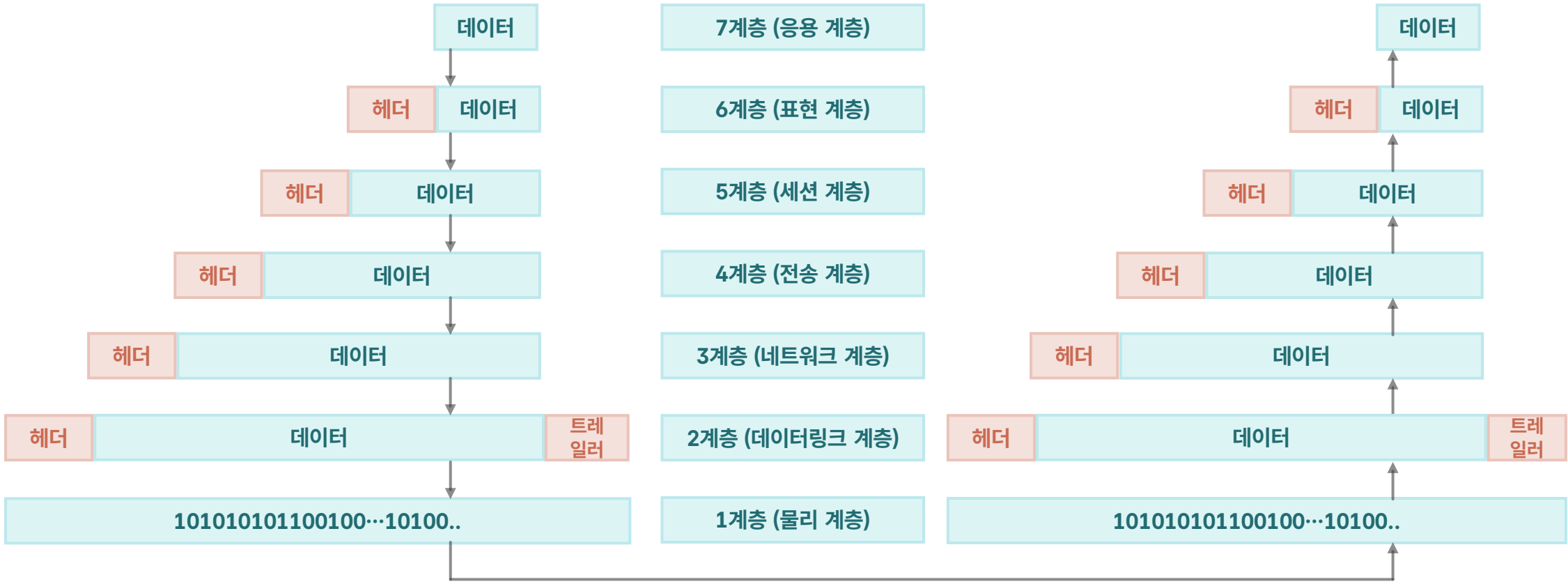
- **OSI 참조 모형은 이론적인 모형이며, 실제 현실세계에서는 TCP/IP 프로토콜로 구현**



OSI 참조 모형 (OSI 7계층)

3 OSI 참조 모형의 이해

- 캡슐화와 역캡슐화



OSI 참조 모형 (OSI 7계층)

4 1계층 (물리 계층)

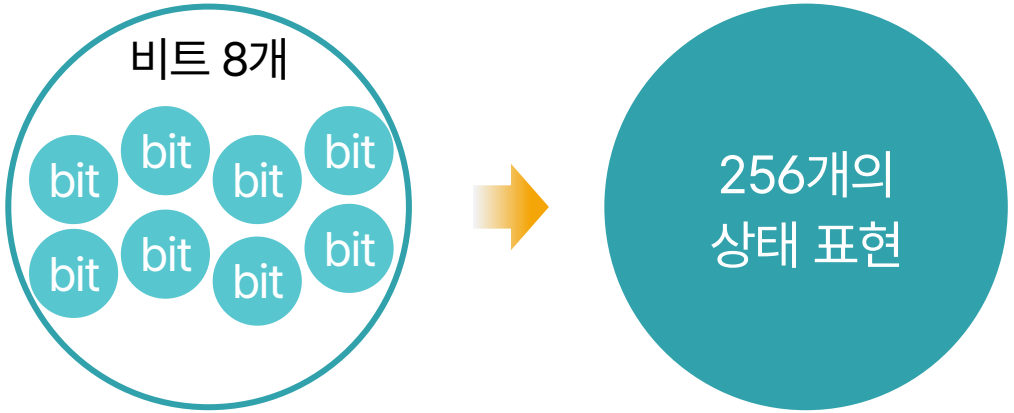
- **비트(Bit)**
  - 컴퓨터가 사용하는 전기 · 전자적 신호

양(+)	음(-)
• 참(True)에 대응 • 이진법의 수 1에 대응	• 거짓(False)에 대응 • 이진법의 수 0에 대응

OSI 참조 모형 (OSI 7계층)

4 1계층 (물리 계층)

- **비트(Bit)**
  - 비트 자체로는 사람이 활용하기에 유의미하지 않으므로 여러 개의 비트를 묶어 사용

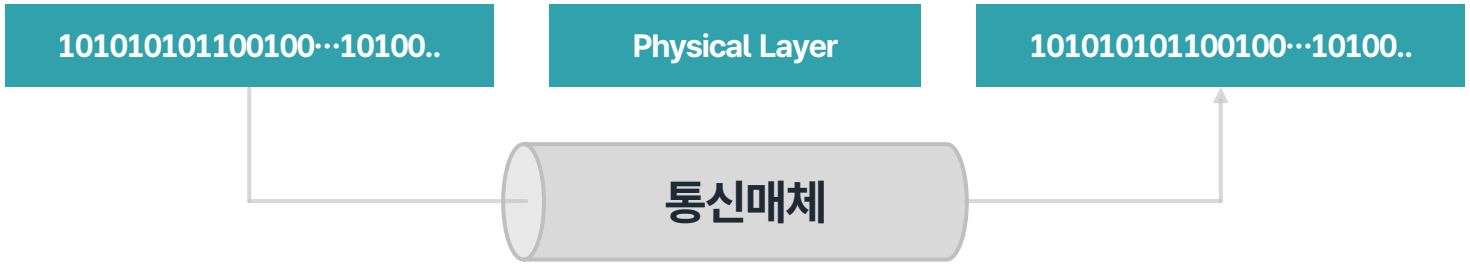


  - 바이트(Byte) : 8비트로 구성되어, 사람이 사용하는 십진법의 수와 영문 대 · 소문자 등 기본적인 문자들을 표현하기에 용이

OSI 참조 모형 (OSI 7계층)

4 1계층 (물리 계층)

- 물리 계층에서는 전기적인 신호로 자료/정보를 주고 받기 때문에 비트열 단위로 데이터 전달
- 다만, 컴퓨터는 디지털 방식으로 데이터를 처리하므로,
  물리 계층에서 전송 가능한 아날로그 방식의 전기적 신호로 변환해야 할 필요
- 아날로그 신호와 디지털 신호를 상호 변환하는 장치를 변복조장치라고 하며,
  실제 데이터 전달은 통신매체를 통해 이루어짐.



OSI 참조 모형 (OSI 7계층)

4 1계층 (물리 계층)

▪ 통신매체

- 물리 계층의 데이터 전달을 목적으로 정보통신망을 구성하기 위해 사용하는 물리적 · 전자기적 매개체
- 유도매체 : 유선 통신구간을 구성하기 위해 사용

꼬임쌍선 케이블	동축 케이블	광케이블
• **근거리통신망 구성**을 위해 일반적으로 널리 사용되어 흔히 접할 수 있는 케이블 • **8가닥의 구리선**을 한 쌍씩 꼬아낸 후 피복을 입히는 방식 구성	• **TV 안테나 연결** 등을 위해 활용 • **안테나선**이라고도 함 • **도체로 이루어진 도선을 절연체로 둘러싼** 후 **다시 도체로 둘러싼** 후 피복을 입히는 방식 구성	• **초고속 통신**을 위해 빛을 주고 받을 수 있음 • 이를 위해 **유리, 플라스틱 등 광섬유** 활용 구성

OSI 참조 모형 (OSI 7계층)

4 1계층 (물리 계층)

- **통신매체**
  - 비유도매체 : 물리적인 연결 없이 공기 또는 물을 통해 전달되는 전자기파 신호로, 주파수의 파장 등에 따라 구분되며 송수신을 위한 안테나 등의 장치 필요

극초단파	초고주파	초장파
Wi-Fi, 무선 이동통신에 사용	**위성통신**에 사용	**잠수함 통신**에 사용

OSI 참조 모형 (OSI 7계층)

5 2계층 (데이터링크 계층)

- **데이터링크 계층에서는 물리 주소를 기반으로 통신**
- **물리 주소를 MAC(Media Access Control) 주소라고도 함.**
  - MAC 주소는 16진수로 표현하며, 총 6 Bytes(=48 Bits)로 구성
  - 상위 3 bytes는 장치의 제조업체 식별자인 OUI(Organizational Unique Identifier)
  - 하위 3 bytes는 장치에 부여된 일련번호

예 **MAC : 16진수, 고유의 주소**

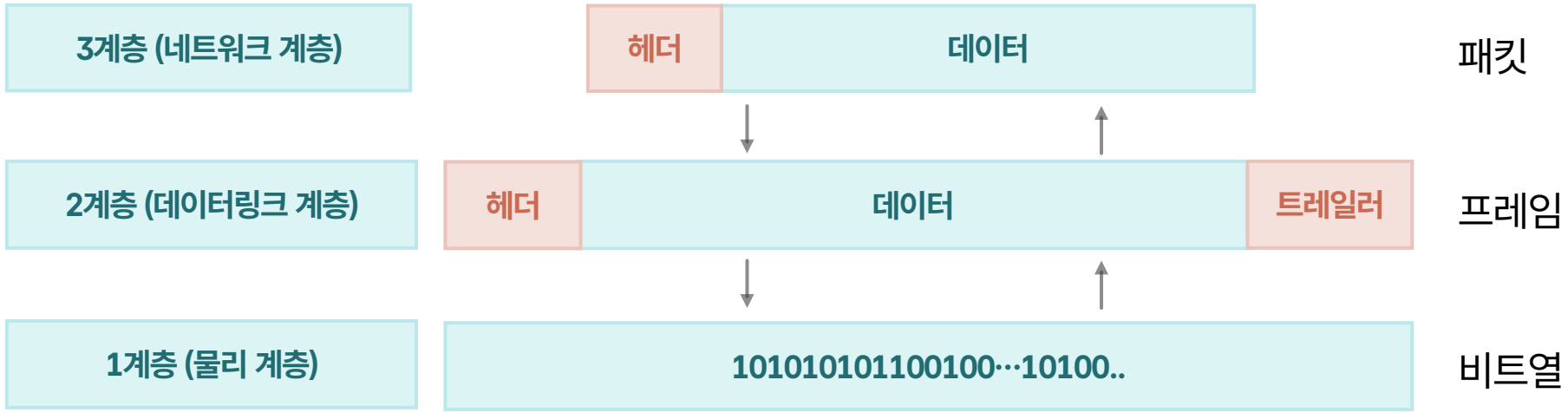
a4 : 5e : 60 : cd : 4f : 0d

제조업체 식별코드 **업체 랜카드 정보**

II OSI 참조 모형 (OSI 7계층)

5 2계층 (데이터링크 계층)

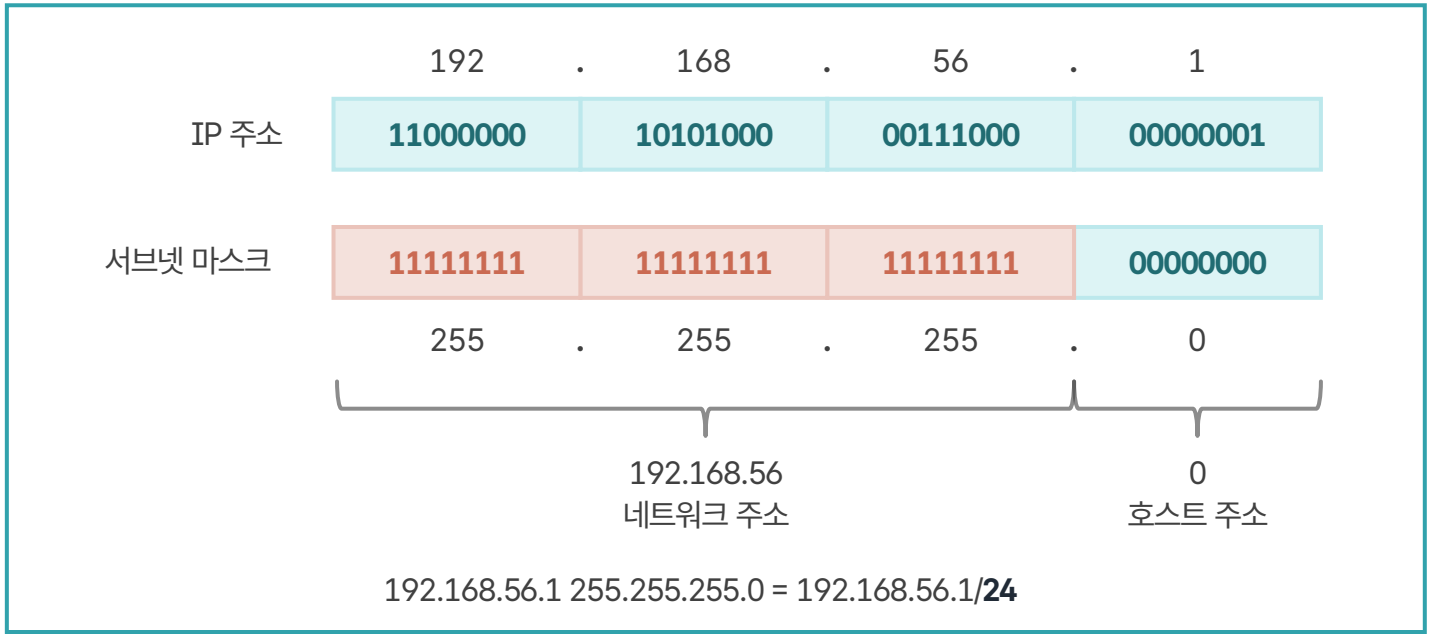
- 데이터링크 계층의 전송 단위를 프레임이라고 하며,
  상위 계층인 네트워크 계층의 패킷에 헤더와 트레일러가 붙어 캡슐화 된 데이터
- 프레임을 아날로그 신호로 변환한 것이 곧 물리 계층에서 전송되는 비트열 데이터



OSI 참조 모형 (OSI 7계층)

6 3계층 (네트워크 계층)

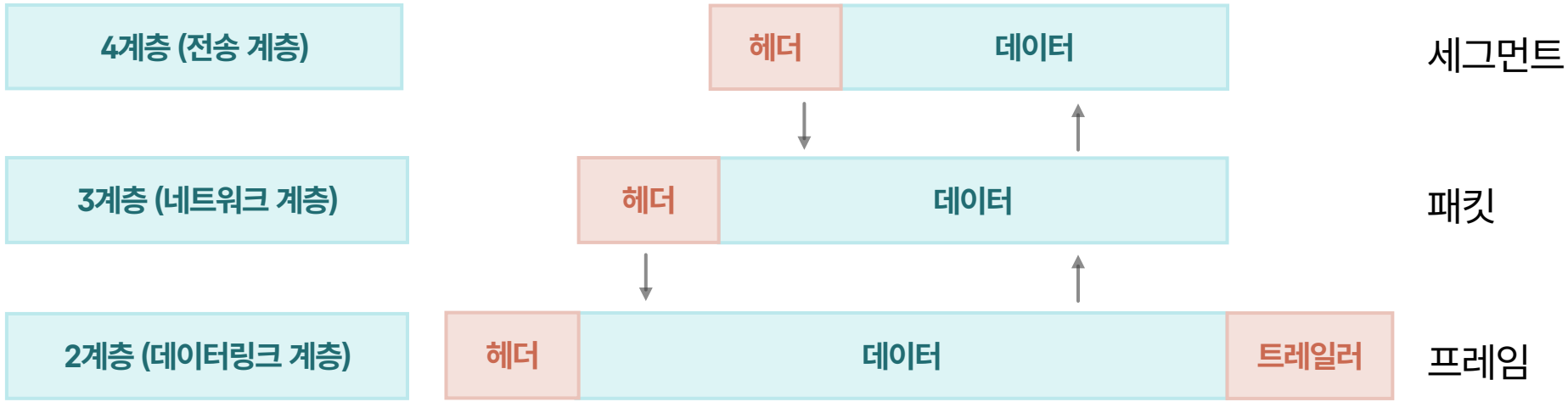
- **네트워크 계층에서는 논리 주소를 기반으로 통신**
- **대표적인 논리 주소에는 IP(Internet Protocol) 주소가 사용되며, IPv4가 널리 사용 중**
  - IPv4는 8 bits의 수 4개, 즉 4 bytes로 구성
  - IPv6는 16 bits의 수 8개, 즉 16 bytes로 구성



OSI 참조 모형 (OSI 7계층)

6 3계층 (네트워크 계층)

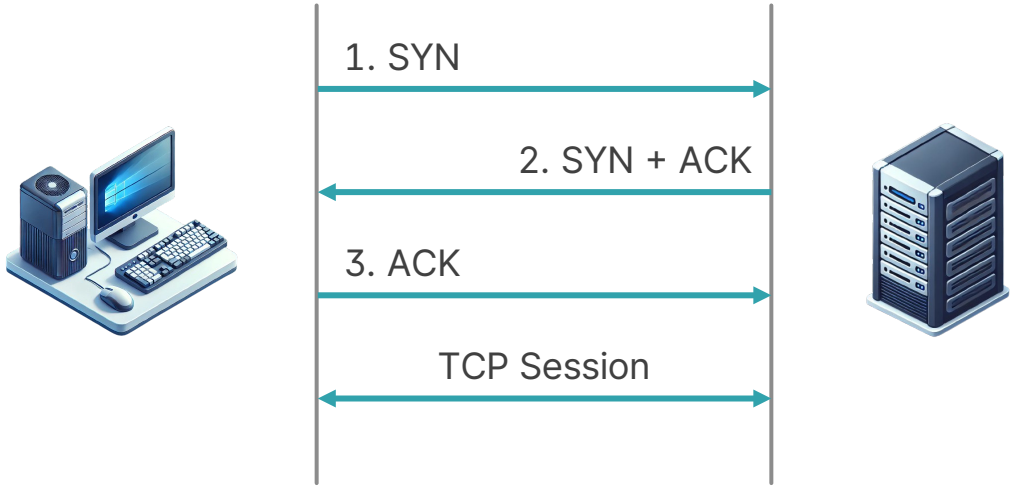
- **네트워크 계층의 전송 단위를 패킷이라고 하며,**
  상위 계층인 전송 계층의 세그먼트에 헤더가 붙어 캡슐화 된 데이터



II OSI 참조 모형 (OSI 7계층)

7 4계층 (전송 계층)

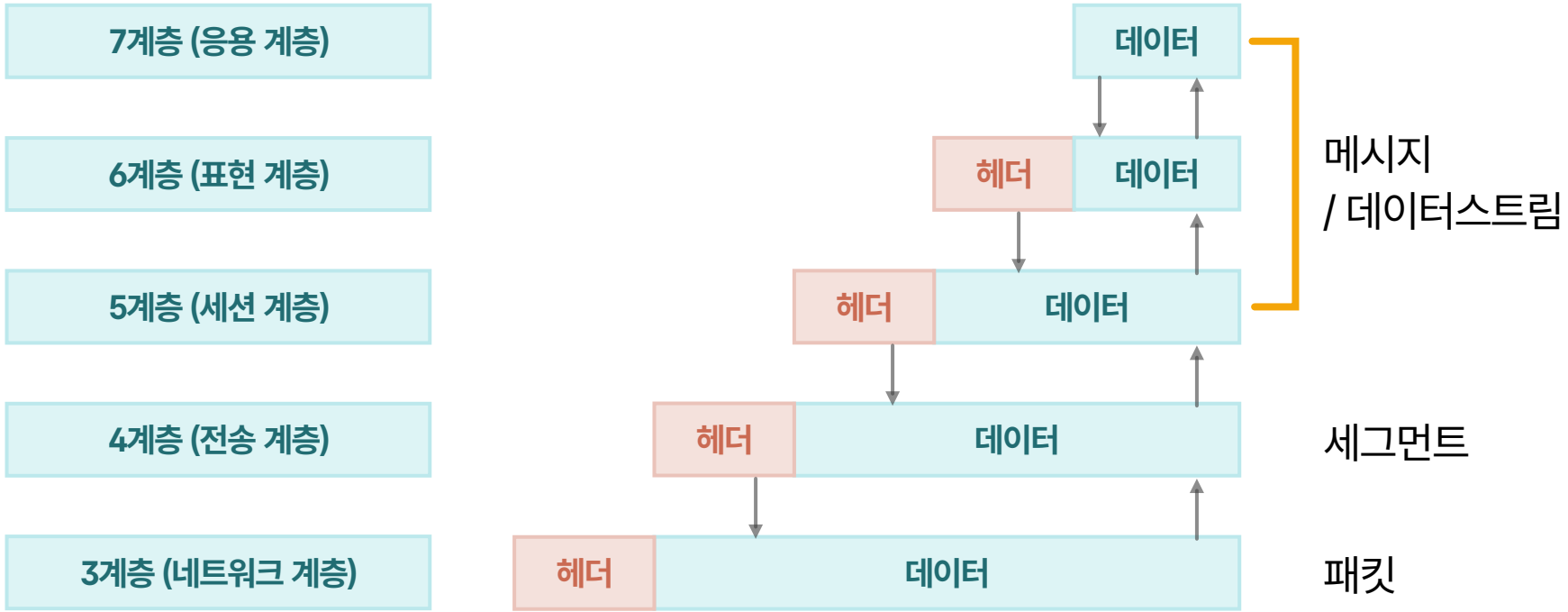
- **전송 계층은 데이터의 전송 방식에 대한 계층으로, 두 가지 방식이 존재**
  - TCP(Transmission Control Protocol) : 신뢰성과 정확성에 방점을 두어 전송하는 방식
  - UDP(User Datagram Protocol) : 빠르고 효율적으로 전송하는 방식
- **TCP 프로토콜은 신뢰성과 정확성을 검증하기 위해 3-Way Handshake 채택**
  - 연결을 성립하기 위해 세 차례에 걸쳐 패킷을 교환하는 절차



OSI 참조 모형 (OSI 7계층)

7 4계층 (전송 계층)

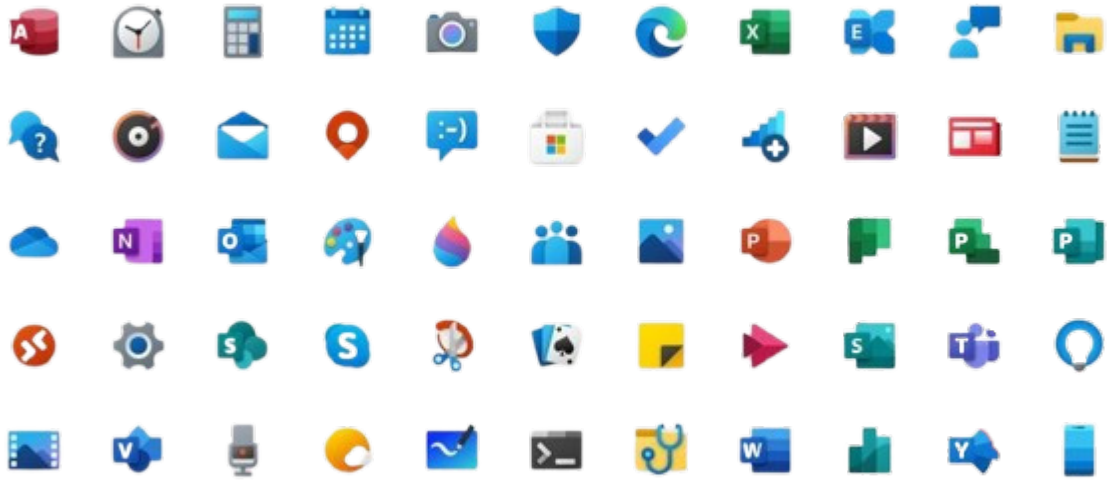
- **전송 계층의 전송 단위를 세그먼트이라고 하며,**
  상위 계층인 세션 · 표현 · 응용 계층의 메시지에 헤더가 붙어 캡슐화 된 데이터



II OSI 참조 모형 (OSI 7계층)

8 5 · 6 · 7계층 (세션 · 표현 · 응용 계층)

- **세션 · 표현 · 응용 계층은 일반적으로 운영체제 및 응용프로그램 단위에서 통합되어 구현**
  - 5계층 (세션 계층) : 세션의 생성, 유지, 종료 등 세션을 관리하는 계층
  - 6계층 (표현 계층) : 데이터 압축, 암호화, 변환, 부호화 등 데이터 형식 및 변환에 대한 계층
  - 7계층 (응용 계층) : 사용자 인터페이스, 네트워크 서비스에 대한 계층
- **세션 · 표현 · 응용 계층은 사용자가 사용하는 응용프로그램에서 처리하는 메시지에 관한 계층**



OSI 참조 모형 (OSI 7계층)

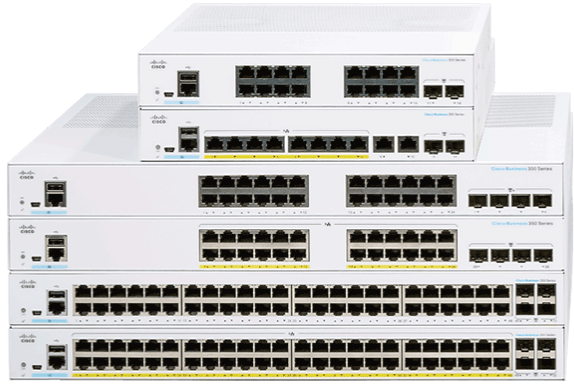
9 주요 네트워크 장비

- **라우터 (Router)**
  - 서로 다른 네트워크 간 출발지에서 목적지까지의 경로를 결정하는 장치로,
    라우터를 기준으로 네트워크 경계 구분
  - 단독으로 존재하는 소규모의 독립적인 네트워크(단독망, 폐쇄망, 독립망 등)에서는 일반적으로 미사용
  - 라우터는 최적의 경로를 결정하기 위해 응답시간을 기준으로 하는 경로 정보를 활용하며,
    인접한 다른 라우터와의 통신을 위해 미리 구성한 라우팅 테이블을 활용
  - 3계층(네트워크 계층) 장치

OSI 참조 모형 (OSI 7계층)

9 주요 네트워크 장비

- **허브 (Hub) / 스위치 (Switch)**
  - 다수의 컴퓨터 및 네트워크 장비 등을 연결하여 네트워크 단위를 구성하거나 거리를 연장하는 장치
  - 회선을 분배하고 자료/정보를 전달하는 기능을 수행
  - 독립적인 네트워크의 최소 단위를 구성하기 위해 사용하나,
    라우터처럼 네트워크 영역을 나누거나 경계를 구분하는 것은 아님.



OSI 참조 모형 (OSI 7계층)

9 주요 네트워크 장비

- **허브 (Hub) / 스위치 (Switch)**

허브	스위치

- 연결된 장치에 대한 정보를 보유하지 않아 **연결된 모든 장치에 자료/정보 전달**
  - 한정된 네트워크 자원을 연결된 장치들이 일률적으로 나누어 사용하므로 통신량 급증 시 병목 현상 발생
- **1계층**(물리 계층) 장치

OSI 참조 모형 (OSI 7계층)

9 주요 네트워크 장비

- **허브 (Hub) / 스위치 (Switch)**

허브	스위치

- 연결된 장치에 대한 정보를 보유하고 있어 **장치를 특정하여 효율적으로 자료 전달**
  - * 근래에는 허브보다 스위치를 보편적으로 사용
- 전통적인 스위치는 **2계층**(데이터링크 계층) 장치
- **일부 라우팅 기능**을 포함한 L3 스위치는 **3계층**(네트워크 계층) 장치
- 부하를 분산시키는 **로드 밸런싱 기능**을 갖춘 L4 스위치는 **4계층**(전송 계층) 장치
  - * 기간망 등 규모가 큰 네트워크에서 사용

9 주요 네트워크 장비

▪ 모뎀 (Modem)

- 아날로그 신호와 디지털 신호를 상호 변환하는 변복조장치

전화 모뎀	• 흔히 **팩시밀리**에 장착 • 전화음성과 동일한 형태의 신호를 발생시켜 **전화선을 통해 전송하는 방식**으로 동작 * 속도가 매우 느리고 다른 전화 통화 중일 때에는 동시에 사용 불가
디지털 모뎀	• 데이터 통신을 위해 전화선을 사용하더라도 **주파수 대역을 달리하여 별도의 통신채널을 발생시키는 방식**으로 동작하여 **고속 통신을 제공** * DSL(Digital Subscriber Line) : 디지털 가입자 회선
무선 이동통신 모뎀	• **3G, 4G(LTE), 5G** 등 무선 이동통신을 위한 디지털 모뎀

OSI 참조 모형 (OSI 7계층)

9 주요 네트워크 장비

- **리피터 (Repeater)**
  - 중계기라고도 하며, 원거리 전송 과정에서 약화되는 신호를 원래 강도의 신호로 증폭(복원)하는 장치
  - 1계층(물리 계층) 장치
- **무선 AP (Wireless Access Point)**
  - Wi-Fi 등 무선 근거리통신(WLAN) 환경의 보편화로 널리 사용되는 장치
  - 2계층(데이터링크 계층) 장치
- **네트워크 카드 (Network Interface Controller)**
  - 네트워크 장비에 컴퓨터 등 장치를 연결하기 위해 네트워크 환경을 부여하는 장치

III

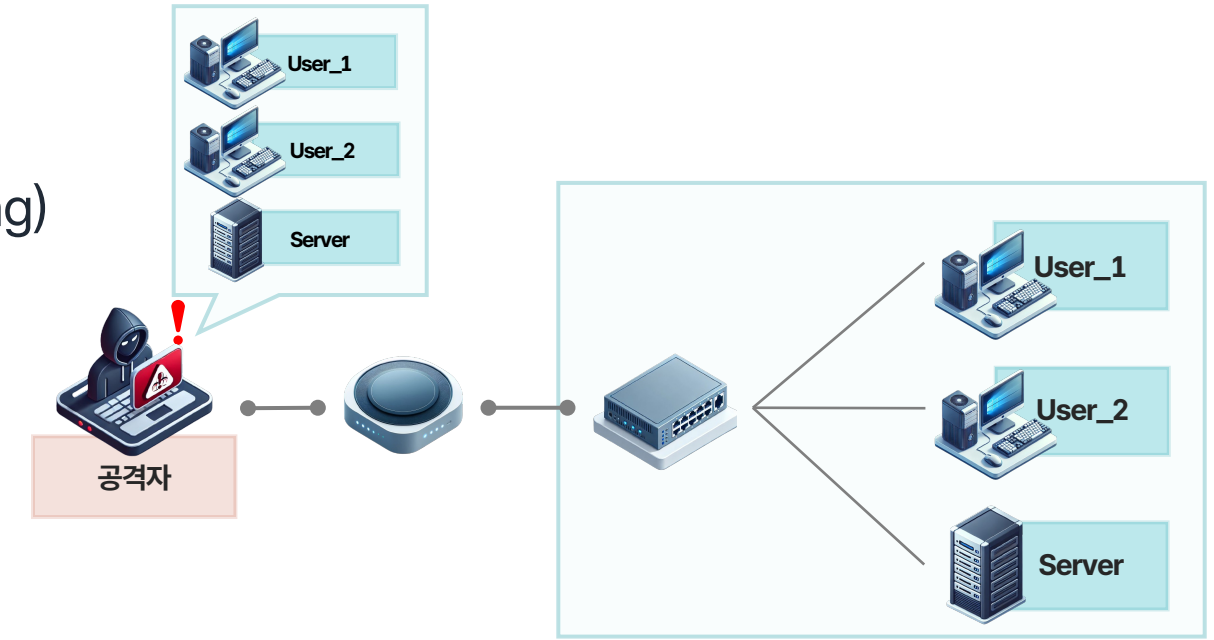
주요 네트워크 공격 기법

(Scanning, Sniffing & Spoofing, DoS & DDoS)

1 스캐닝 (Scanning)

- **공격자가 공격대상의 네트워크나 시스템 정보를 탐색하는 행위**
  - 수집 대상 : 실행 중인 TCP/UDP 서비스들, 시스템 및 운영체제 정보, 그 외 다양한 정보 등
  - 수집 목적 : 공격자가 공격목표로 하는 네트워크나 시스템의 자세한 정보(IP, OS, Port 및 Version 등)를 수집하기 위함

- **스캐닝의 종류**
  - 활성 호스트 스캐닝(Active Host Scanning)
  - 포트 스캐닝 (Port Scanning)
  - 취약점 스캐닝 (Vulnerability Scanning)

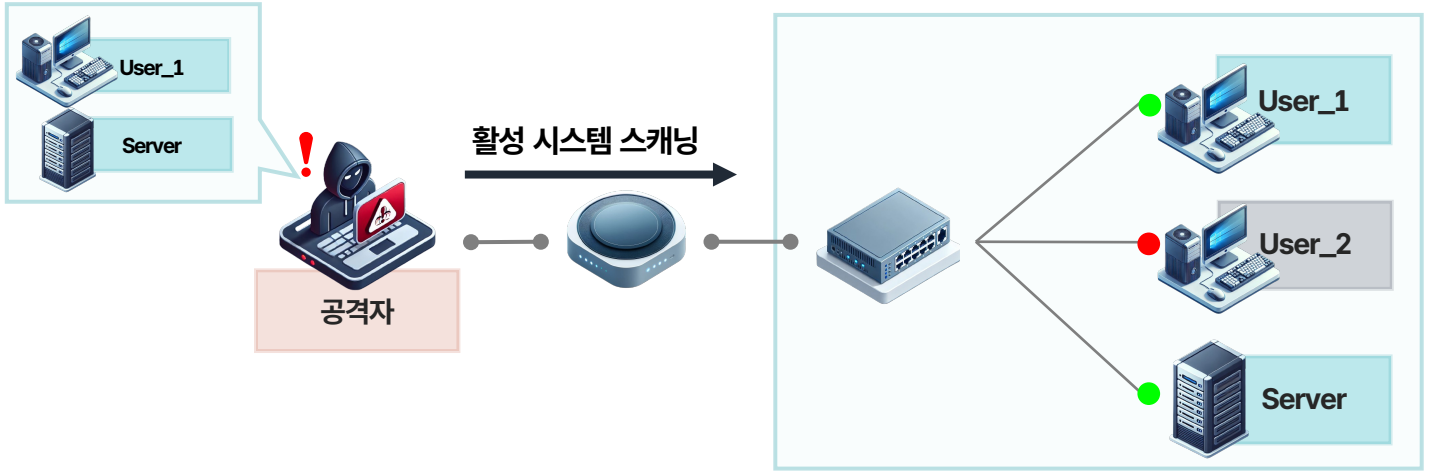


주요 네트워크 공격 기법

1 스캐닝 (Scanning)

▪ 활성 호스트 스캐닝 (Active Host Scanning)

- 현재 동작 중인 컴퓨팅 장치(호스트)를 찾기 위한 스캐닝 기법
  - ICMP(Internet Control Message Protocol)를 이용한 ping 통신을 통해 동작 여부 확인
  - 대상 네트워크의 구조와 공격 대상을 찾는 방법으로 직접적인 공격 영향 없음
- 종류
  - ICMP Echo ping
  - ARPing
  - TCP/UDP ping
- 대표적인 도구
  - Nmap
  - ARPing

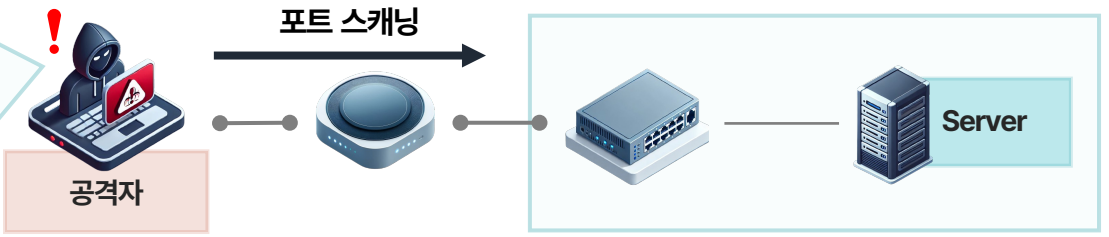


1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

- 호스트에서 실행 중인 서비스를 찾기 위한 스캐닝 기법
  - * 서비스 실행 시 통신을 위한 포트가 필요하며, 공격자는 해당 서비스의 취약점을 목표로 공격을 시작함
- 종류
  - * TCP Port Scanning
  - * UDP Port Scanning

Server	
포트번호	서비스명
22	SSH
25	SMTP
80	HTTP
443	HTTPS
...	...

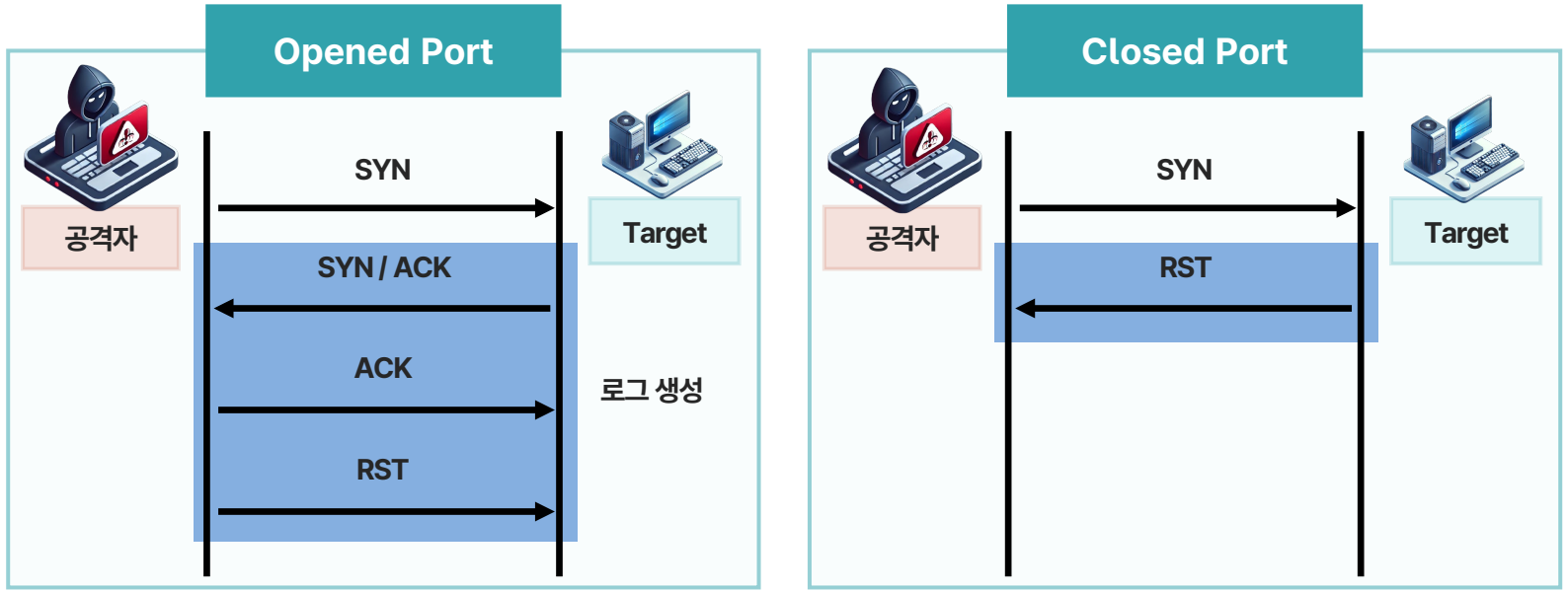


1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

① TCP Connect Scanning

- TCP 연결을 맺어서 포트의 활성화 여부를 판단하는 방법
  - 포트가 열린 경우, 신뢰성 있는 연결(3-Way Handshake)을 수행하며 연결 기록(로그)을 남김

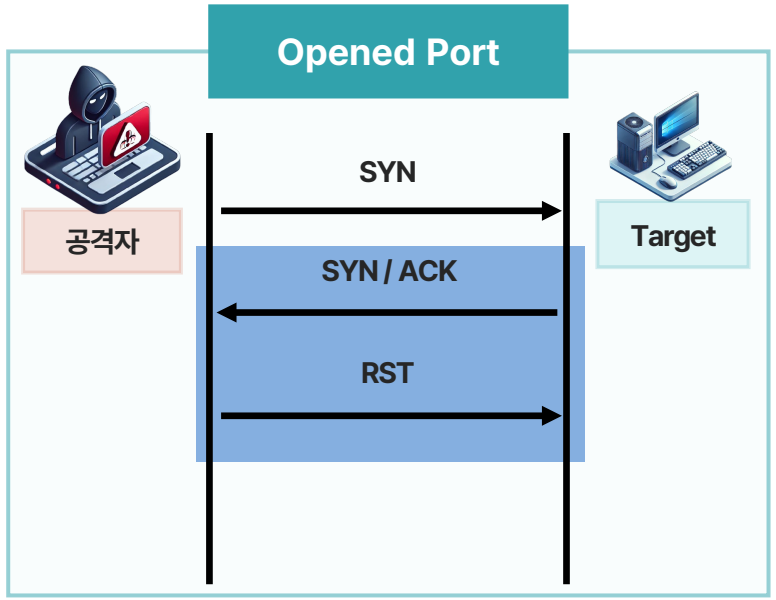


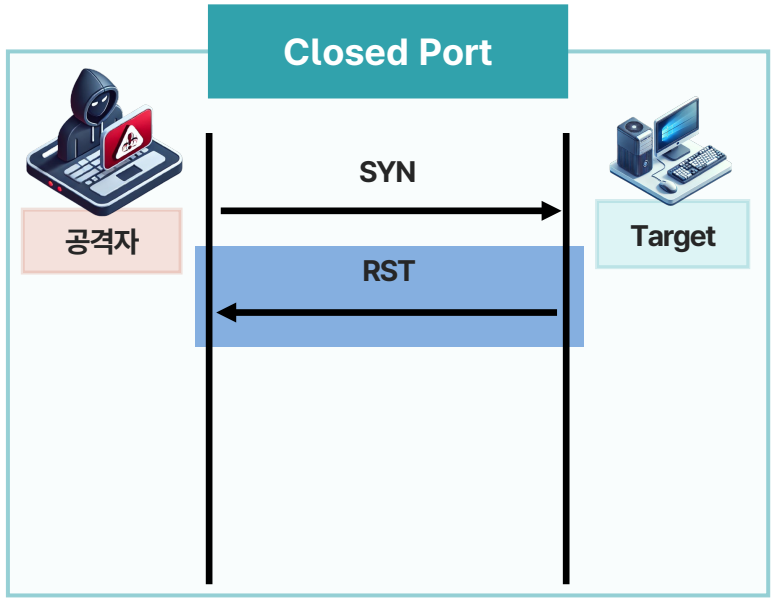
1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

② SYN Stealth(Half Open) Scanning

- TCP 연결을 완전히 하지 않고 포트의 활성화 여부를 판단하는 방법
  - 포트가 열린 경우, 연결 중간(3-Way Handshake 2단계)에 끊으며 연결 기록(로그)을 남기지 않음.



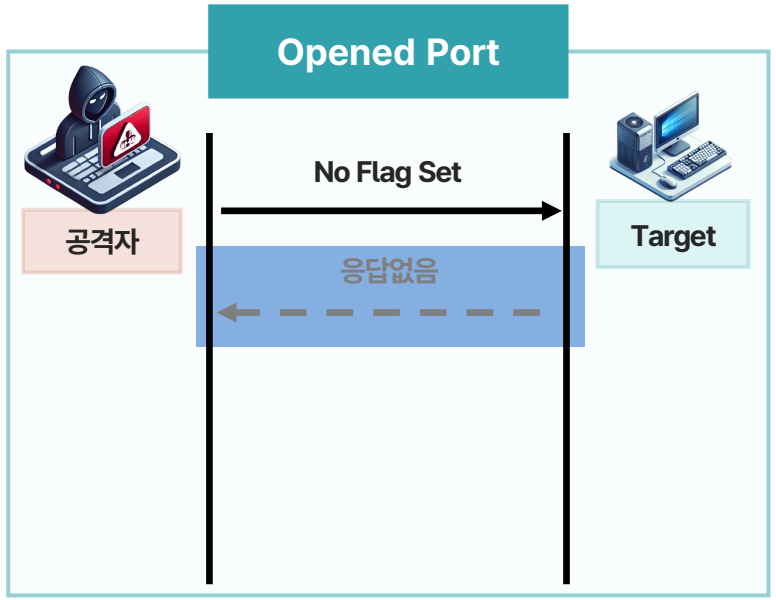


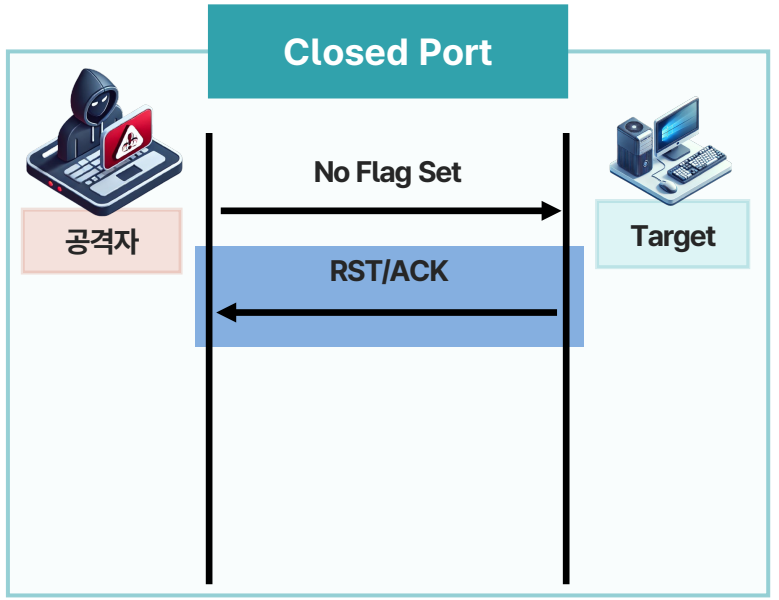
1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

③ SYN Stealth(Half Open) Scanning

- TCP 헤더 내 플래그 값을 설정하지 않고 전송하여 그에 대한 응답으로 포트의 활성화 여부를 판단하는 방법
  - 포트가 열린 경우, 목표대상은 요청을 알 수 없어 응답을 하지 않음



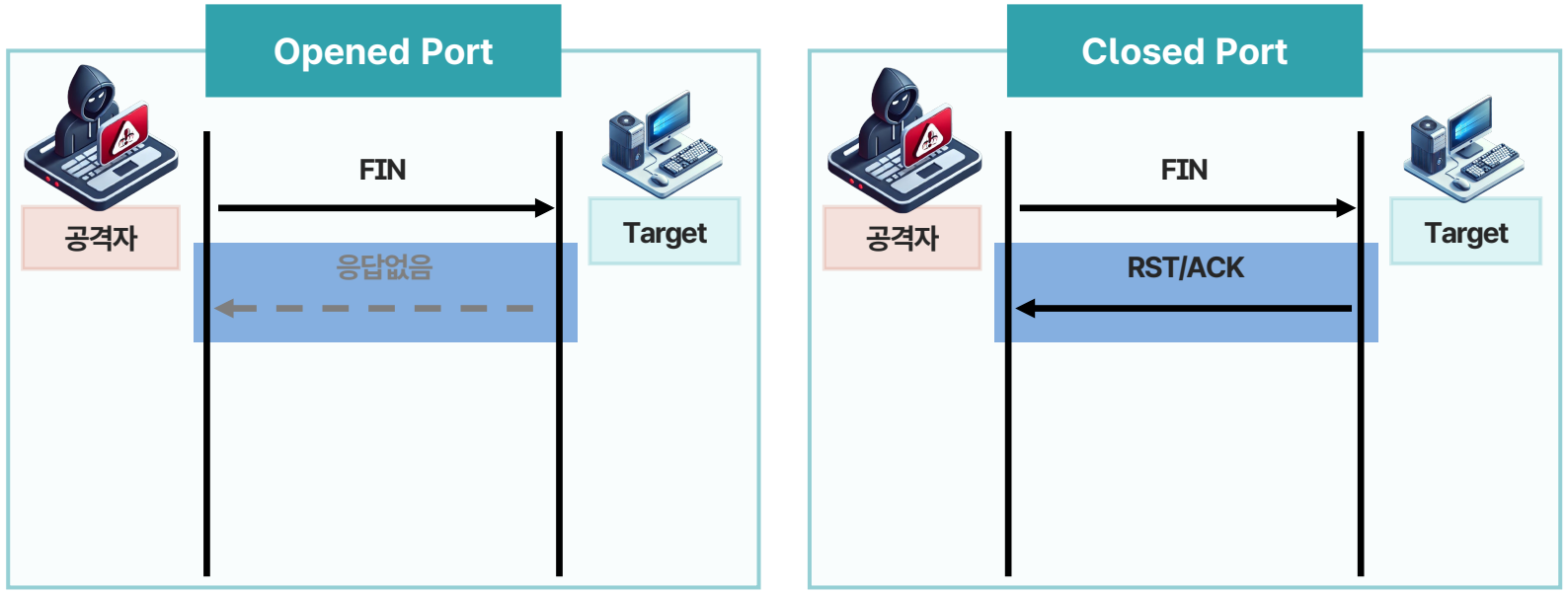


1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

④ FIN Scanning

- TCP 헤더 내 FIN 플래그를 설정하여 전송하고 그에 대한 응답으로 포트의 활성화 여부를 판단하는 방법
  - 포트가 열린 경우, 목표대상은 연결을 수행한 적이 없기에 응답을 하지 않음

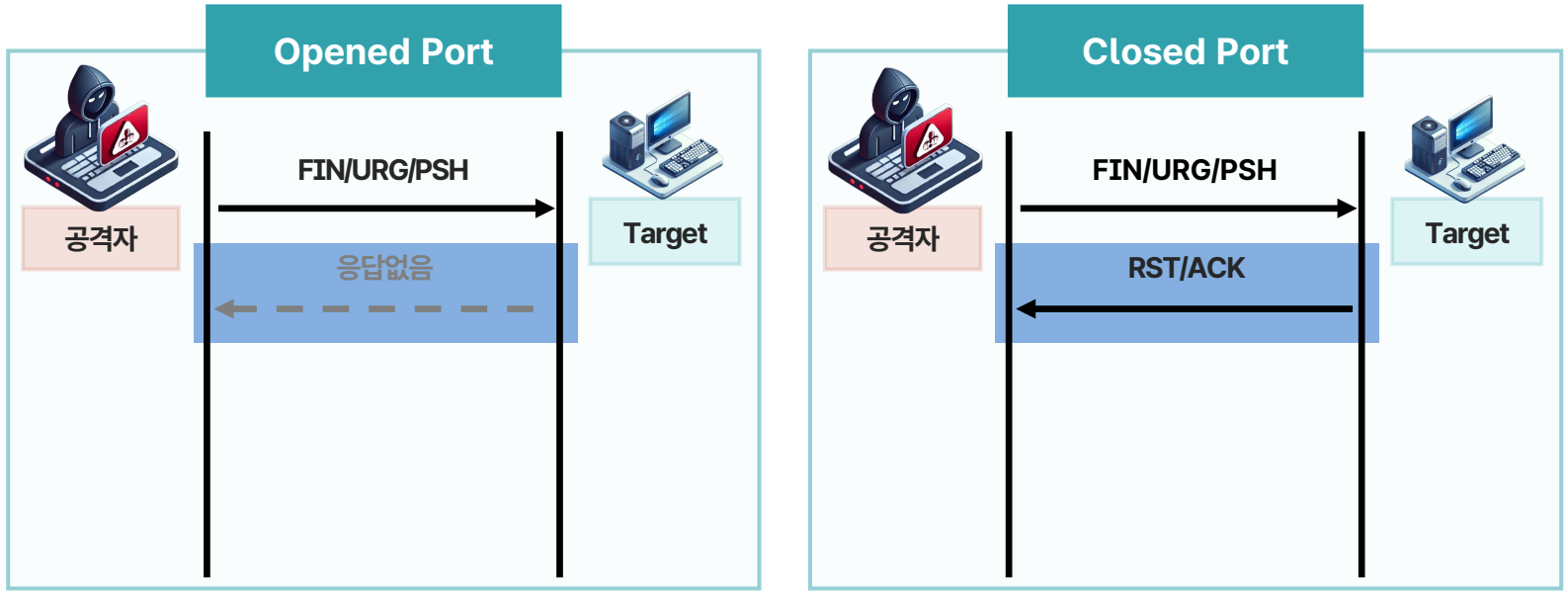


1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

⑤ X-MAS Scanning

- TCP 헤더 내 일부 또는 모든 플래그를 설정하여 전송하고 그에 대한 응답으로 포트의 활성화 여부를 판단하는 방법
  - 포트가 열린 경우, 목표대상은 요청에 대한 정확한 응답을 하기 어렵게 때문에 아무 응답을 하지 않음

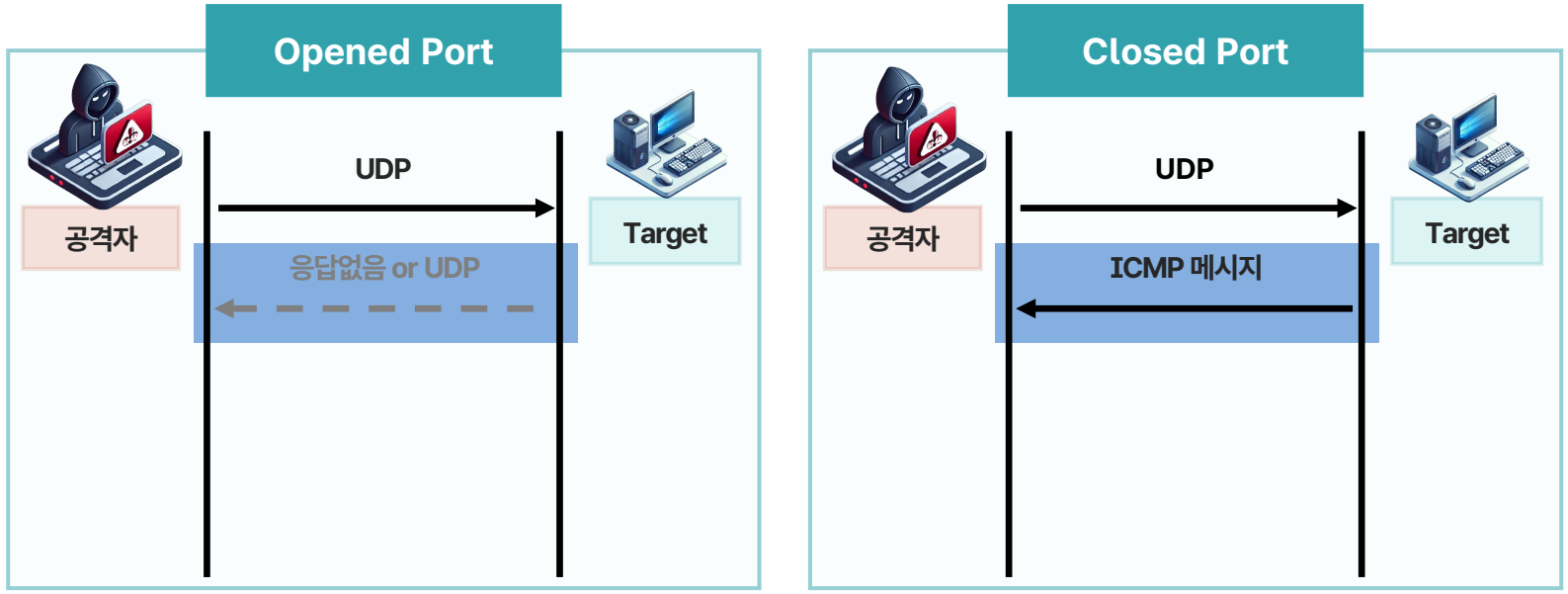


1 스캐닝 (Scanning)

▪ 포트 스캐닝 (Port Scanning)

⑥ UDP Port Scanning

- ICMP Unreachable 메시지를 이용하여 UDP 포트의 활성화 여부를 판단하는 방법
  - 포트가 열린 경우, UDP 응답이 오거나 별도 응답 없음(정책 차단)
  - 포트가 닫힌 경우, ICMP 메시지 응답(Type 3 : Destination Unreachable, Code 3 : Port Unreachable)



1 스캐닝 (Scanning)

▪ 취약점 스캐닝 (Vulnerability Scanning)

- Nmap을 이용한 취약점 스캐닝
  - * nmap –sV –script vuln {네트워크 대역 | 호스트 IP} : 열린 포트를 스캔하고 vuln 스크립트를 이용해 취약점 스캔

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script vuln 192.168.0.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-29 16:51 PST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is di
sabled. Try using --system-dns or specify valid servers with --dns-server
s
Nmap scan report for 192.168.0.2
Host is up (0.000088s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workg
roup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-
010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsof
t SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guid
ance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.asp
x
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.17 seconds
```

2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

- **스니핑은 네트워크 트래픽을 도청(eavesdropping)하는 공격**
  - 사전적 의미 : 코를 킁킁거리다, 냄새를 맡다 등
  - 대상 몰래 도청만 하므로 피해 여부를 인지하거나 탐지하기 어려움

- **허브 환경과는 달리 스위치 환경에서 스니핑을 하기 위해서는 스푸핑 등을 유발시키는 선행 공격 필요**
  - 스위치 재밍 (Switch Jamming)
  - ARP 스푸핑 (ARP Spoofing)
  - ARP 리다이렉트 (ARP Redirect)
  - ICMP 리다이렉트 (ICMP Redirect)

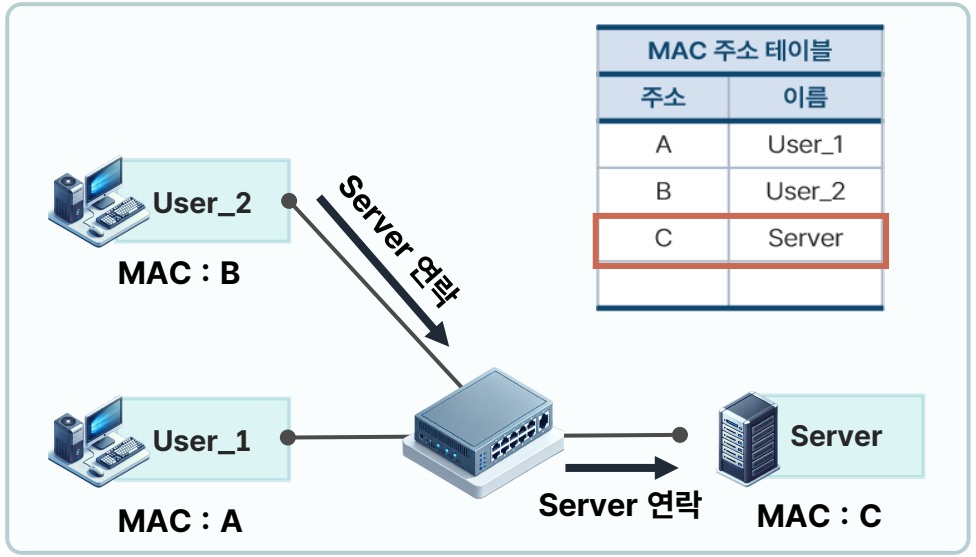
2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

▪ 스위치 대상 선행 공격

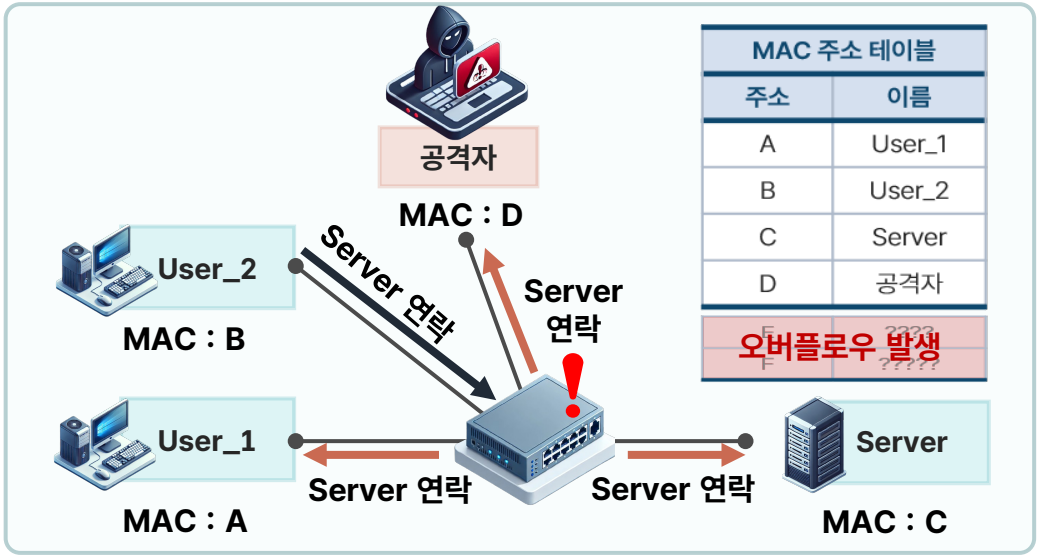
① 스위치 재밍 (Switch Jamming)

- 스위치에서 관리하는 MAC 주소 테이블의 버퍼를 오버플로우(Overflow) 시켜 스위치가 더미 허브*처럼 동작하게 만드는 기법

* 신호 증폭의 역할을 수행하는 장비로 네트워크 내 모든 대상에게 데이터를 전송하는 브로드캐스트(Broadcast) 수행



스위치재밍 전 패킷흐름



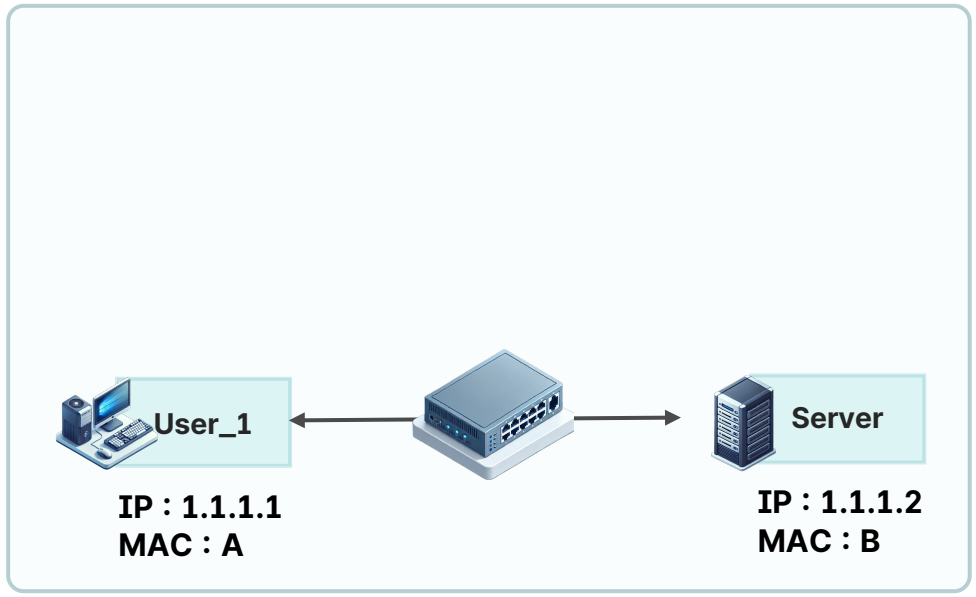
스위치재밍 후 패킷흐름

2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

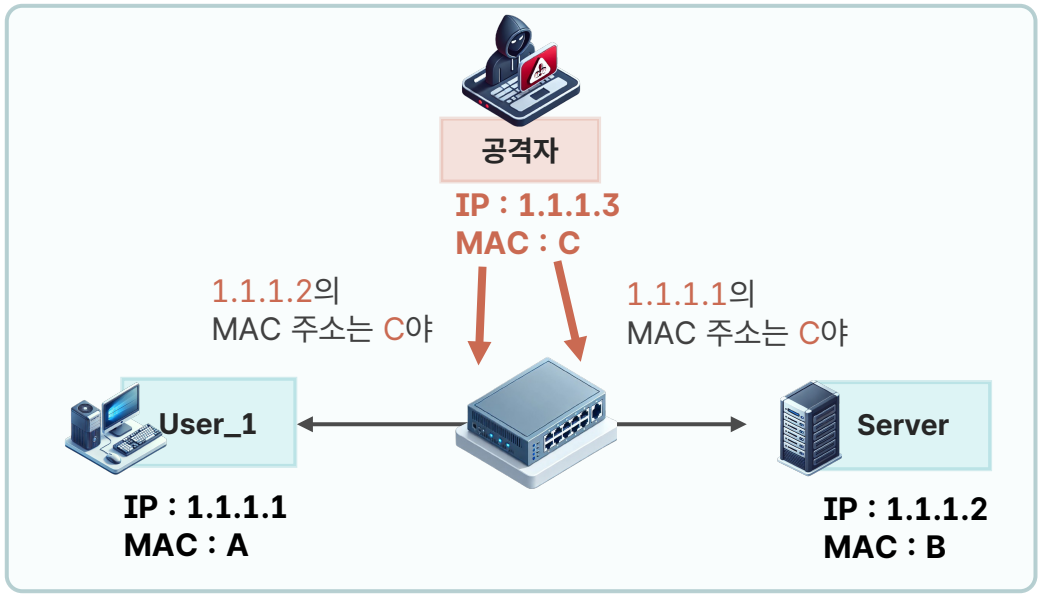
▪ 스위치 대상 선행 공격

② ARP 스푸핑 (ARP Spoofing)

- 공격자가 통신 대상자인 것처럼 MAC 주소를 위조하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법



ARP 스푸핑 전 패킷 흐름



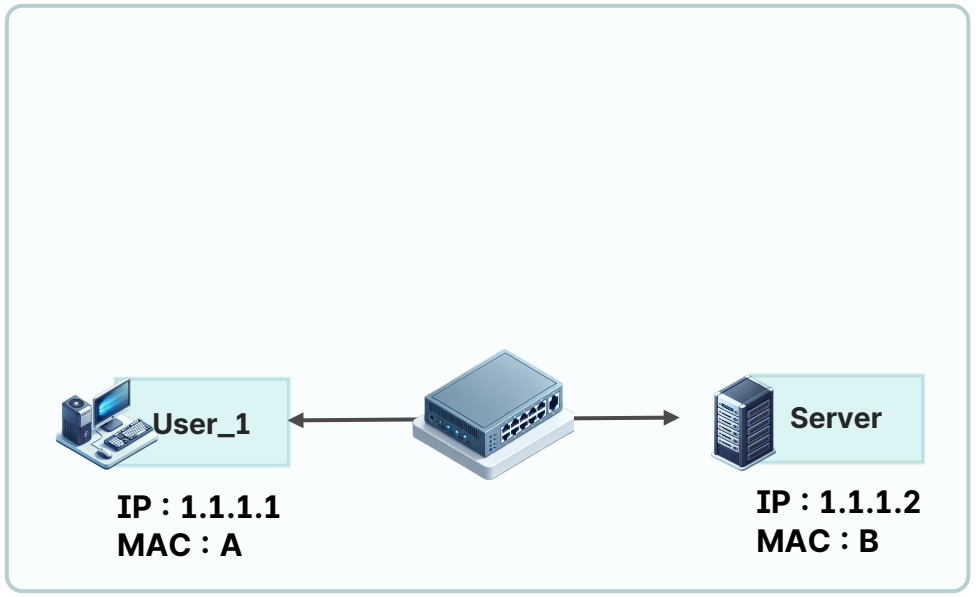
ARP 스푸핑 패킷 흐름

2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

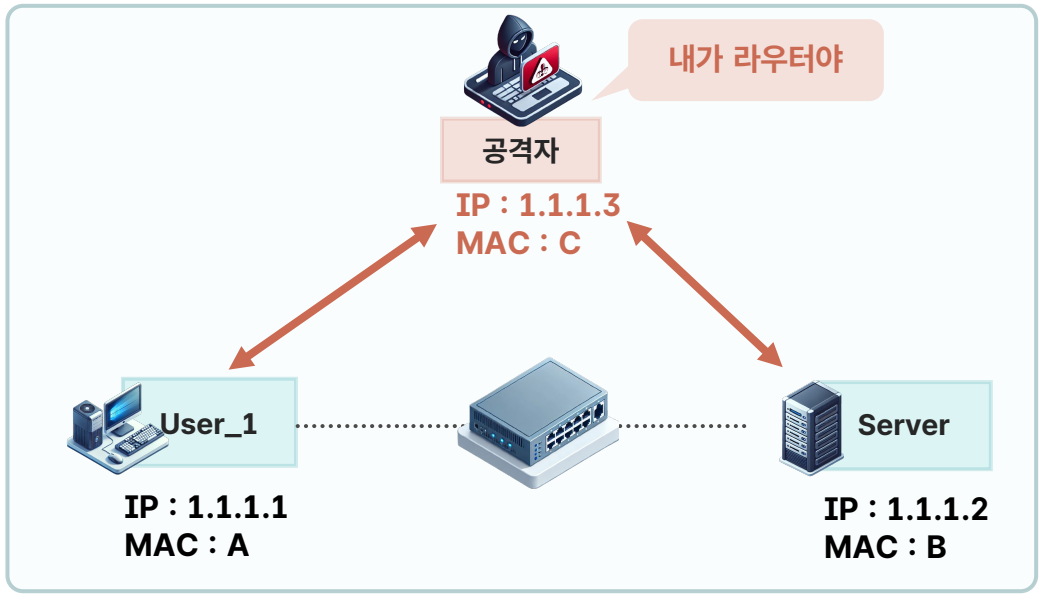
▪ 스위치 대상 선행 공격

③ ARP 리다이렉트 (ARP Redirect)

- 공격자가 라우터인 것처럼 MAC 주소를 위조하여 데이터 패킷을 중간에서 가로채는 중간자 공격 기법



ARP 리다이렉트 전 패킷 흐름



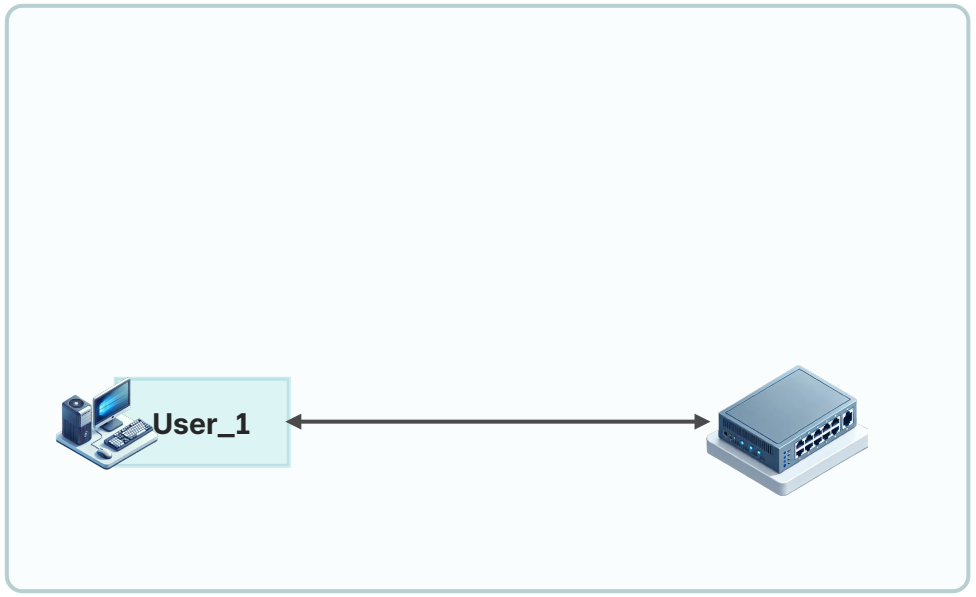
ARP 리다이렉트 후 패킷 흐름

2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

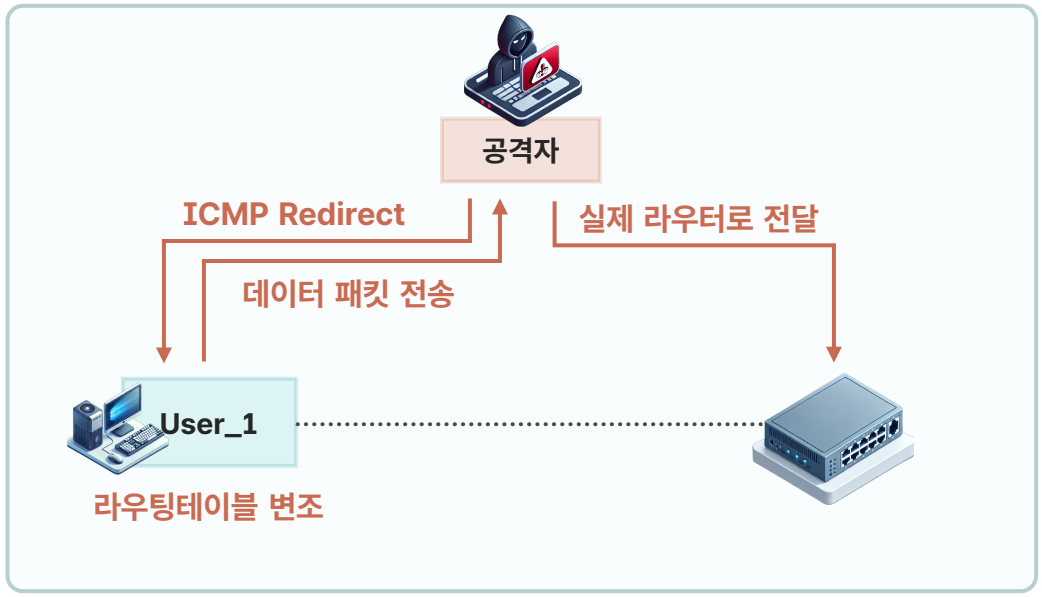
▪ 스위치 대상 선행 공격

④ ICMP 리다이렉트 (ICMP Redirect)

- ICMP 리다이렉트 메시지를 이용하여 라우팅 경로를 재설정하도록 하여 데이터 패킷을 가로채는 공격 기법



ICMP 리다이렉트 전 패킷 흐름

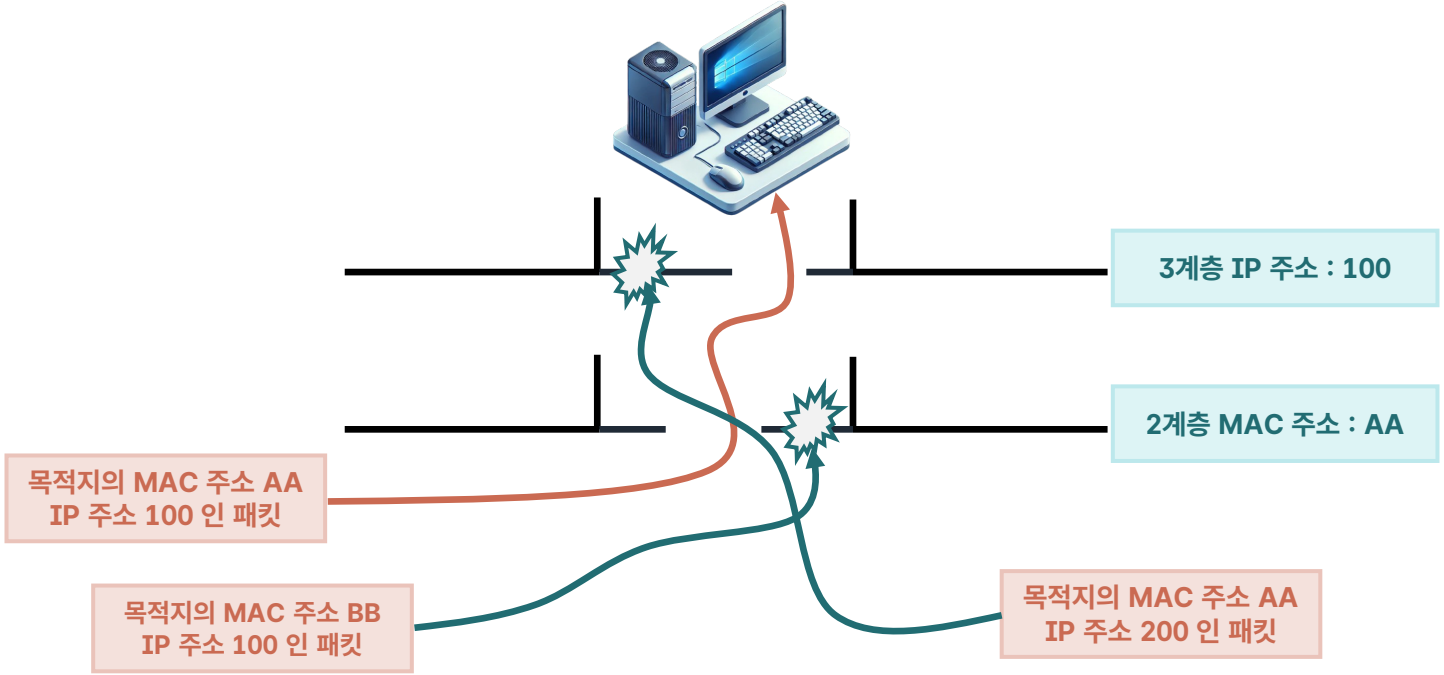


ICMP 리다이렉트 후 패킷 흐름

2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

▪ NIC 모드 변경을 통한 스니핑

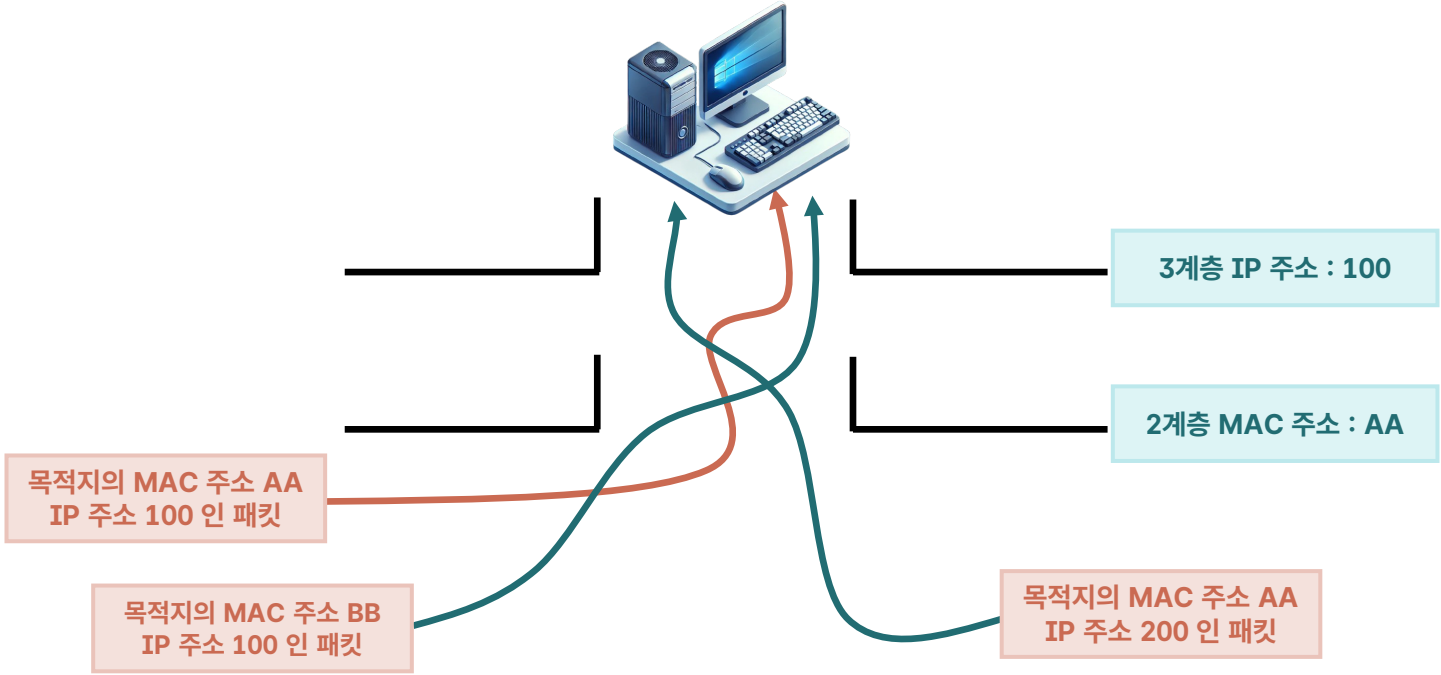
- 기본 모드에서는 들어온 패킷 데이터의 2계층 주소(MAC)와 3계층 주소(IP)를 확인하여 필터링 수행
  - * 패킷의 IP, MAC 주소를 확인하여 버퍼에 저장할 지 여부를 결정하며 자신의 것과 일치하지 않으면 무시함



2 스니핑 (Sniffing) · 스푸핑 (Spoofing)

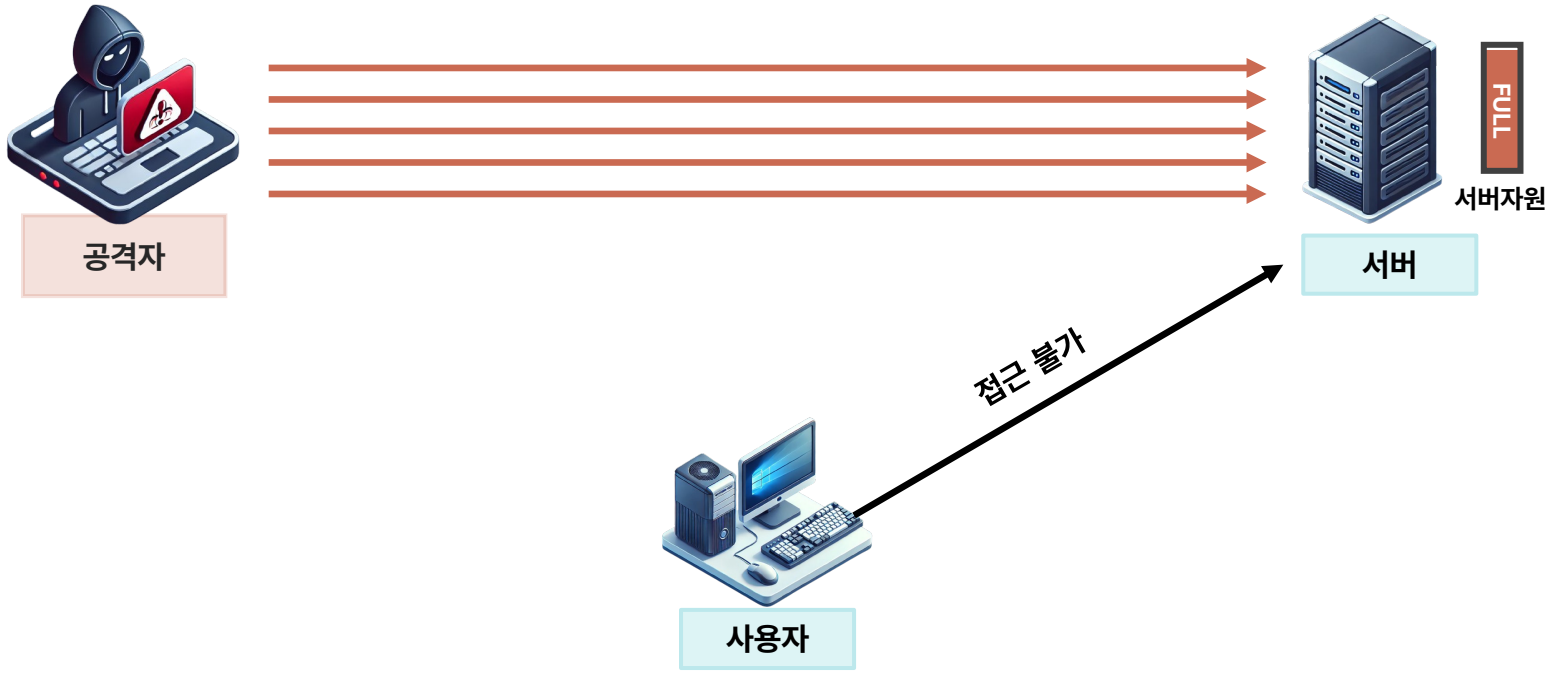
▪ NIC 모드 변경을 통한 스니핑

- 프로미스큐어스 모드는 들어온 패킷 데이터의 모든 필터링(2계층, 3계층)을 해제함으로써 네트워크 감시 목적으로 사용할 수 있는 모드



3 DoS & DDoS

- **DoS (Denial of Service)**
  - 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 함으로써 가용성을 고갈시키는 공격

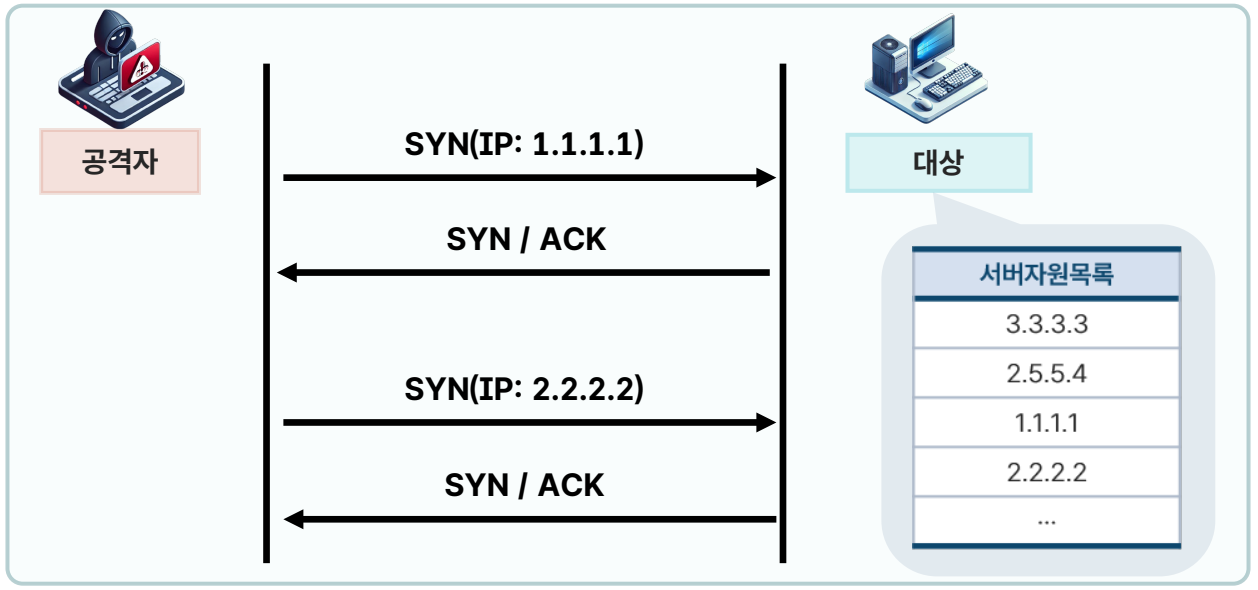


3 DoS & DDoS

▪ DoS (Denial of Service)

① TCP SYN Flooding

- **SYN 요청을 지속적으로 보내는 네트워크 계층 공격**
  - 반개방(half-open) 공격이라고 불리며, TCP의 3-Way HandShake를 이용한 공격
  - 네트워크에서 서비스를 제공하는 시스템은 동시 사용자 수가 한정되어 있어 해당 공격을 통해 서버 자원을 소모시킴

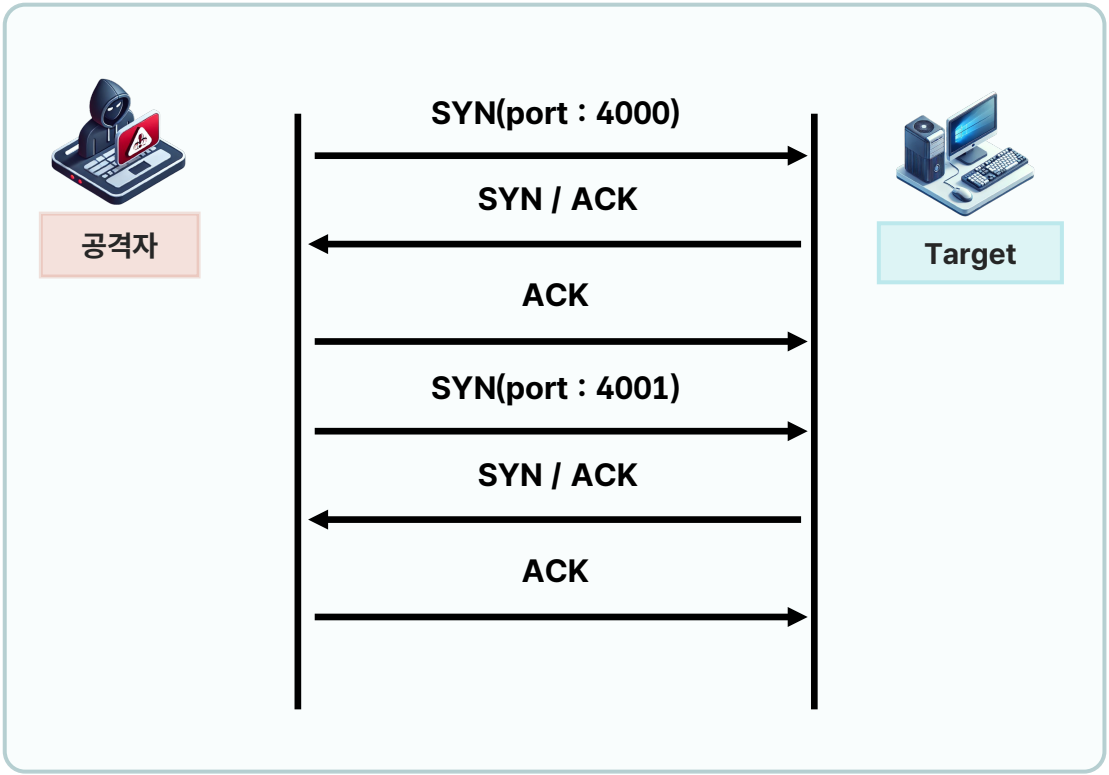


3 DoS & DDoS

- **DoS (Denial of Service)**

② TCP Connection Flooding

- **TCP의 세션을 이용한 공격**
  - 한 개의 IP가 다양한 포트로 SYN 패킷을 전송
  - 클라이언트는 서버와 3 Way-Handshake를 통해 세션을 연결하게 됨
  - 세션 연결이 가득차면 더 이상 연결이 불가능 함

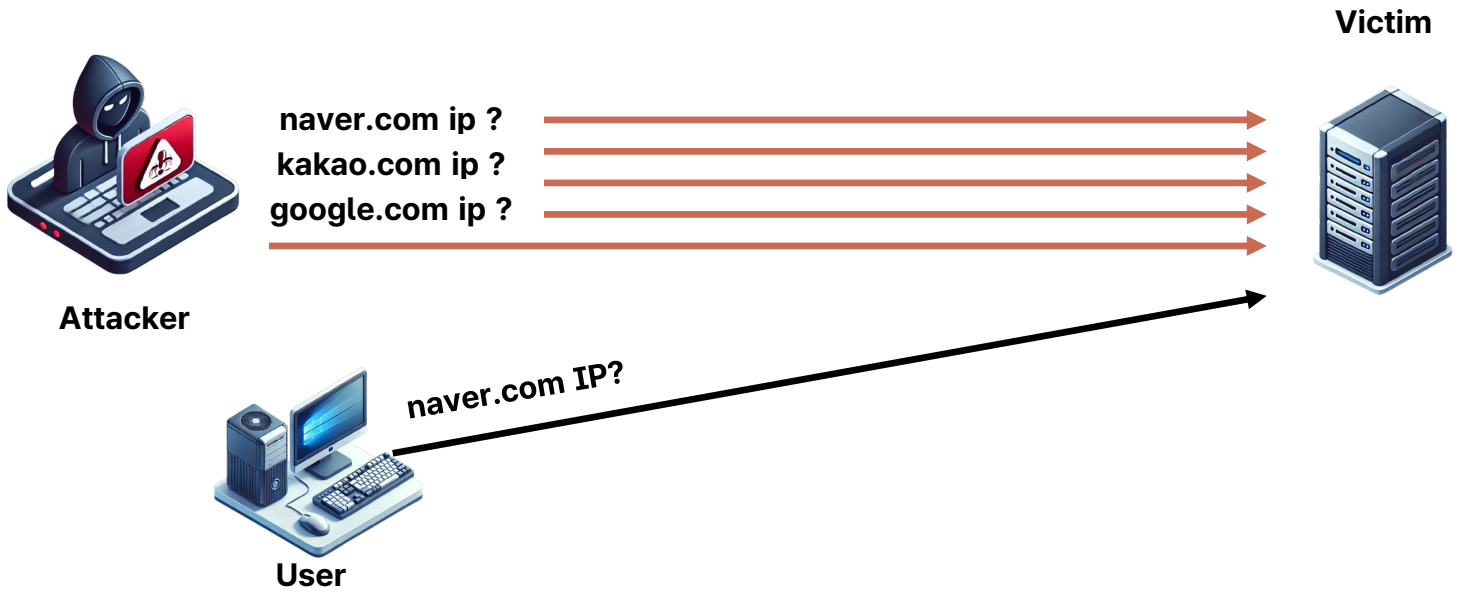


3 DoS & DDoS

- **DoS (Denial of Service)**

③ DNS Query Flooding

- DNS Query 요청 패킷을 대량으로 서버에 전송하여 DNS의 정상적인 서비스 방해
- 대량의 Query를 발생시켜 서버가 더 이상 DNS 응답을 하지 못하도록 함

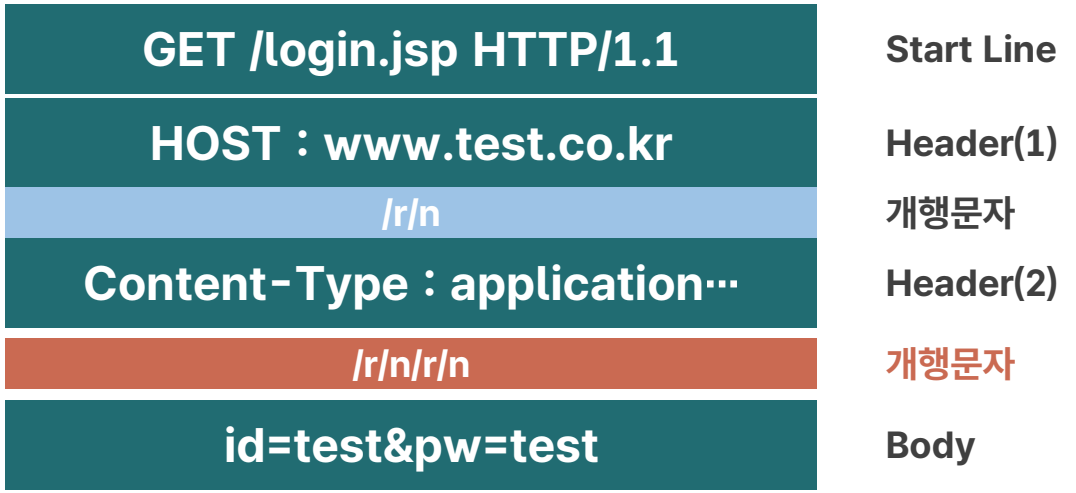


3 DoS & DDoS

- **DoS (Denial of Service)**

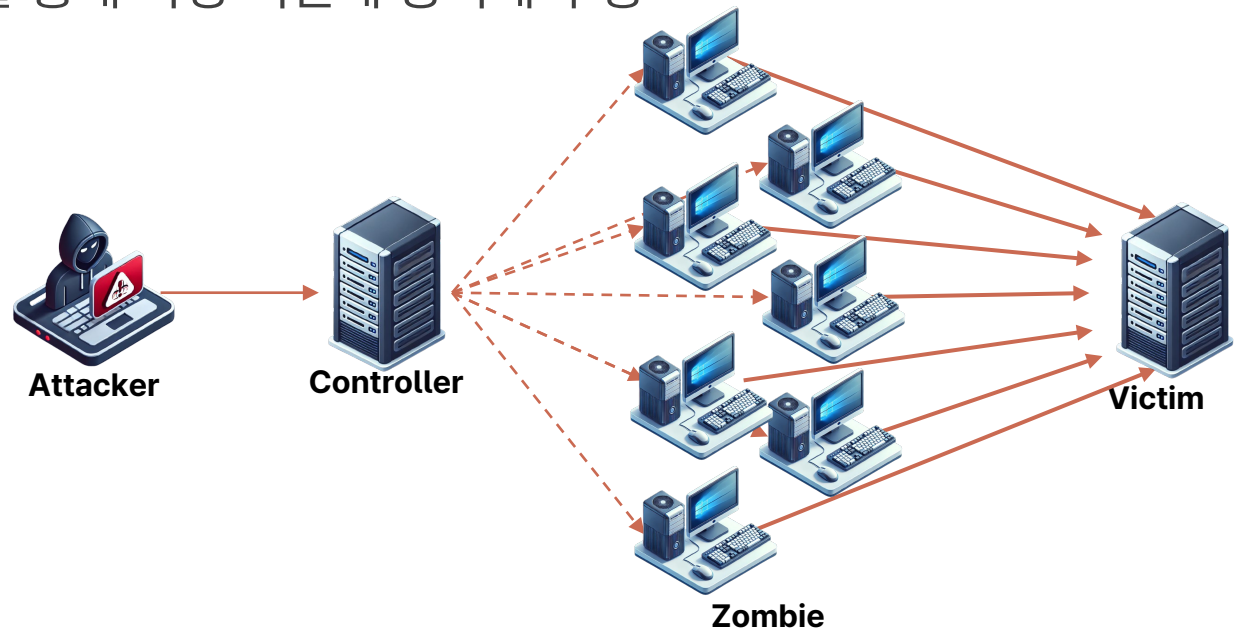
④ Slow HTTP Header DoS (Slowloris)

- HTTP Header 정보를 비정상적으로 조작하여 웹서버가 온전한 Header 정보가 올 때 까지 기다리도록 함
- HTTP에선 헤더의 끝을 /r/n라는 문자로 구분하게 되는데 공격자는 마지막 개행 문자를 보내지 않음



3 DoS & DDoS

- **DDoS (Distributed DoS)**
  - 분산 서비스 거부 공격은 여러 대의 공격자를 분산적으로 배치해 동시에 DoS공격을 실시
  - 악성 코드를 이용하여 일반 사용자의 PC를 감염시켜 좀비 PC로 만든 다음 C&C(명령 제어) 서버의 제어를 통해 특정 시간에 동시에 수행



요약 정리

- 지금까지 학습한 내용을 정리해보겠습니다.

요약정리

▪ 네트워크 보호의 필요성

• 보안관제시스템

– 통합 보안관제시스템이라고도 하며, 보안관제 업무를 원활하게 수행할 수 있도록 수집, 분석, 가시화/시각화 등의 기능을 통합적으로 제공

* **수집 :** 정보시스템 및 정보통신망과 정보보호시스템에 보관된 보안 정보 및 이벤트 기록을 모아서 보관하는 기능
* **분석 :** 수집된 보안 정보 및 이벤트 기록을 분석하는 기능
* **가시화/시각화 :** 수집 및 분석된 결과를 보안관제사가 쉽게 이해할 수 있게 그림, 그래프, 애니메이션 등의 형태로 표현하는 기능

– 보안관제시스템 도입 시 보안관제사는 개별 정보보호시스템을 각각 들여다볼 필요없이 보안관제시스템만 보면 되므로 업무 효율이 향상되는 효과

• 네트워크 보호

– 침해사고로 이어지기 전에, 사이버 공격이 들어오는 경계 또는 통로에서 침해시도를 탐지하여 차단하는 것

요약정리

- **OSI 참조 모형** (OSI 7계층)
  - **정보시스템과 네트워크**
    - 오늘날 통신 기술의 발달, 정보시스템의 복잡도 증가, 처리 자료/정보의 단위 용량 증가로 인해 대부분의 정보시스템은 네트워크 형태로 구성
  - **OSI 참조 모형** (OSI 7계층)
    - 각 통신장치 개발사들이 참조할 수 있도록 자료/정보의 전달 구조를 국제적인 표준 모형으로 정한 것
    - 7개의 계층으로 구성
      - 1계층 (물리) – 2계층 (데이터링크) – 3계층 (네트워크) – 4계층 (전송) – 5계층 (세션) – 6계층 (표현) – 7계층 (응용)
  - **주요 네트워크 장비**
    - 라우터 : 서로 다른 네트워크 간 출발지에서 목적지까지의 경로를 결정하는 장치
    - 허브/스위치 : 네트워크 단위를 구성하거나 거리를 연장하는 장치로, 회선을 분배하고 자료/정보를 전달
      - 스위치 : 연결된 장치에 대한 정보를 보유하고 있어 장치를 특정하여 효율적으로 자료를 전달하는 특성

요약정리

주요 네트워크 공격 기법

- **스캐닝 (Scanning)**
  - 공격자가 공격 대상을 탐색하기 위한 목적으로 정보를 수집하는 행위
  - 활성 호스트 스캐닝, 포트 스캐닝, 취약점 스캐닝
- **스니핑 (Sniffing)**
  - 네트워크 트래픽을 도청하는 행위
  - 단, 스위치 환경에서 스니핑을 하기 위해서는 스위치에 스푸핑 등 선행 공격 필요
    - **스푸핑 (Spoofing) :** 공격자가 통신 대상자 또는 네트워크 장비인 것처럼 가장하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법
- **DoS (Denial of Service)**
  - 시스템을 악의적으로 공격하여 해당 시스템의 자원을 부족하게 하여 가용성을 고갈시키는 공격
  - **DDoS (Distributed DoS) :** 대량으로 발생되는 DoS를 특별히 구분

참고문헌

- 정보통신기반보호법 (법률)
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (법률)
- 사이버안보 업무규정 (대통령령)
- 국가사이버안전관리규정 (대통령훈령)
- 국가 정보보안 기본지침 (국가정보원 지침)
- 보안관제학, 2014, 안성진 등 공저, 이한미디어
- 2023 국가정보보호백서, 2023, 국가정보원 등 관계기관 합동
- 국가사이버안보센터 웹 사이트, http://www.ncsc.go.kr
- 한국인터넷진흥원 웹 사이트, http://www.kisa.or.kr
- KISA 보호나라 & KrCERT/CC 웹 사이트, http://www.krcert.or.kr
- 중국 해킹그룹, 국내 12개 학술기관 해킹, MBC뉴스(2023.01.25), https://www.youtube.com/watch?v=oSnkr3uvk5s

수고하셨습니다