WEEK 02

사이버 공격의 이해

학습목표

I. 사이버 공격자와 공격의 이해
II. 공격 유형의 분류
III. 다양한 공격 기법들

학습목차

1. 사이버 공격자와 공격의 이해
2. 공격 유형의 분류
3. 다양한 공격기법들

1. 사이버 공격자와 공격의 이해

1.1 공격자

1.2 공격 유형의 이해

1.1 공격자

- 해커(hacker)
- 크래커(cracker)
- 프래커(phreaker)

[출처] 그림 위키백과

1.1 공격자

◆ 해커(hacker)

- ❖ 해커는 컴퓨터 및 네트워크, 보안에 관한 전문가라 할 수 있으며, 뛰어난 프로그램 개발자이기도 함
- ❖ 해커의 요건들과는 달리 흔히 모든 공격자들을 해커라고 부르기도 함
- ❖ 해커 역시 선의의 해커와 악의적인 해커로 나뉘어지며, 이러한 해커의 구분기준은 의지에 따라 순간 임의적으로 달라질 수 있기 때문에 선의의 해커를 '보안전문가'라고도 구분 지어 부르기도 함
- ❖ 선의의 해커는 도덕적인 윤리의식을 갖추어야 하며, 공익을 위한 취약점발견을 위주로 하며, 방어를 목적으로 함

[출처] 정보보호개론 사이텍미디어

1.1 공격자

◆ 해커(hacker)

- ❖ 선한 윤리적 해커(ethical hacker)나 보안 연구자(security reseacher)를 화이트 햇(white hat) 해커라고 하며, 악한 해커나 크래커(cracker)를 블랙 햇 (black hat) 해커라고 부르는데, 이것은 미국 서부영화의 중흥기 시절 주인공이 흰색 카우보이 모자를, 악당들이 검은색 카우보이 모자를 쓰는 것에서 보고 유래
- ❖ 해커라는 용어에는 좋은 뜻과 나쁜 뜻을 동시에 포함하고 있기 때문에, 대체적으로 문맥이나 상황에 따라 파악해야 함
- ❖ 악한 짓을 하기는 하나, 곧 자기가 했음을 인정하고 자백하거나 때론 그 문제점이나 대처법을 담당자들에 알려주기도 하는 선악이 공존하는 중간적 존재의 해커를 흰색과 검은색의 중간색인 회색에서 유래한 그레이 햇(gray hat) 해커라고 표현하기도 함

[출처] 위키백과

1.1 공격자

◆ 크래커(cracker)

- ❖ 컴퓨터에 대한 지식은 있지만, 지식 그 자체보다는 파괴적인 행위에 목표를 두고 있으며, 이러한 목표를 위한 지식을 습득
- ❖ 도덕성이 결여되어 있고, 정보를 파괴하거나 시스템을 마비시키는데 주력하며, 취득한 정보를 매매하기도 함
- ❖ 크래커는 주로 프로그램의 시리얼번호 및 라이선스 보호장치를 무용지물로 만들기도 함

[출처] 위키백과

1.1 공격자

◆ 프래커(phreaker)

❖ 전화통신이 통신체계의 핵심이었을 때, 장거리 전화의 무료통화를 위해 전화요금을 타인에게 부과하도록 하는 불법적인 행위를 "phreaking"이라 함

❖ 이러한 프래킹의 공격 행위자를 "phreaker"라 함

[출처] 위키백과

1.2 공격의 이해

◆ 대표적인 공격 유형

- ❖ 방해(interrupt)
- ❖ 가로채기(intercept)
- ❖ 위조(fabrication)
- ❖ 변조(modification)

[출처] 정보보호개론 사이텍미디어

1.2 공격의 이해

◆ 방해(interrupt)

- ❖ "방해 공격(interrupt attack)"은 사용자간의 정상적인 네트워킹을 방해하여 데이터를 중간에 목적지 주소까지 전송되지 못하게 차단하는 공격
- ❖ 대표적인 예로 서비스 거부 공격(Denial of Services)이 있음
- ❖ 두 통신자 간의 정상적인 통신의 "방해(interruption)"를 의미

[출처] 정보보호개론 사이텍미디어

1.2 공격의 이해

◆ 가로채기(intercept)

- ❖ "가로채기(interception)" 공격은 공격자가 통신의 일부를 엿듣는 공격 형태로서 통신상에서 사용자 계정이나 패스워드를 획득
- ❖ 가로채기 공격 유형의 대표적인 기법으로 "스니핑(sniffing)" 공격이 있음

[출처] 정보보호개론 사이텍미디어

1.2 공격의 이해

◆ 위조(fabrication) 및 변조(modification)

- ❖ "전송 데이터의 "위조(fabrication)"와 "변조(modification)"는 두 통신자를 속이는 방법
- ❖ 특정 공격 대상자의 데이터 및 개인 정보를 훔쳐내기 위해 사용
- ❖ 네트워크상에 어떠한 보안 시스템이 설치되어 있지 않을 경우, 통신자들은 감지하기 힘들고, 상대 통신자가 인가된 통신자 인지의 여부조차 확인하기 어려움

[출처] 정보보호개론 사이텍미디어

1. 사이버 공격자와 공격의 이해

1교시 수업을 마치겠습니다.

2. 공격 유형의 분류

2.1 공격 유형의 분류

2.1 공격 유형의 분류

◆ 공격 유형에 따른 분류

- ❖ 의지에 따른 분류
- ❖ 위치에 따른 분류
- ❖ 공격의 체계성에 따른 분류

[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 의지에 따른 분류 (1/3)

❖ 공격 유형을 공격자의 의지 및 공격 위치, 공격의 체계성 등으로 분류해 볼 수 있다. 이러한 공격유형들은 공격 목표의 분석 및 대응방안을 구축하는데 매우 중요한 요소가 된다.

- 소극적 공격(passive attack)
- 적극적 공격(active attack)

[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 의지에 따른 분류 (1/3)

❖ 소극적 공격(passive attack)

- 일반적인 공격 형태로 특정한 공격 목표가 없으며, 공격 목표에 대해서도 적극적인 데이터 파괴 및 변조의 목적을 갖지 않음

- 일반적으로 트래픽 상의 데이터를 훔쳐보는 정도의 공격으로 공격자의 고의성이 없어 위험도가 비교적 낮은 공격들이 이에 속함

[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 의지에 따른 분류 (2/3)

❖ 적극적 공격(active attack) (1/2)

- 소극적 공격과는 달리 목표에 대한 특정 목적을 가지고 데이터의 파괴 및 변조를 취하는 공격을 의미
- 시스템 다운이나 사용 불가 등을 유발시킬 수 있음
- 혼합 공격 방법이 사용되어 각각의 공격방법들을 모두 적극적 공격이라고 정하기는 어렵지만, 공격 목표가 뚜렷하기 때문에 매우 치명적
- 악의적인 해커들에 의해 수행되는 만큼 전문적이며, 네트워크 지식과 관련 취약점까지도 알고 있기 때문에 이에 대한 대응이 어려움

[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 의지에 따른 분류 (3/3)

❖ 적극적 공격(active attack) (2/2)

- 의지에 따른 공격은 공격 결과를 참고하여 공격 의지를 추측해야 하는 단점이 있음
- 대부분의 공격의 경우 소극적인 공격을 차지하지만, 해킹 기술을 습득하려는 자들로 인해 시도되는 경우가 대부분을 차지 함.
- 적극적인 공격은 특정 목적을 갖고 있기 때문에 이는 사이버 범죄에 해당할 수 있어 형사처벌도 가능할 수 있음

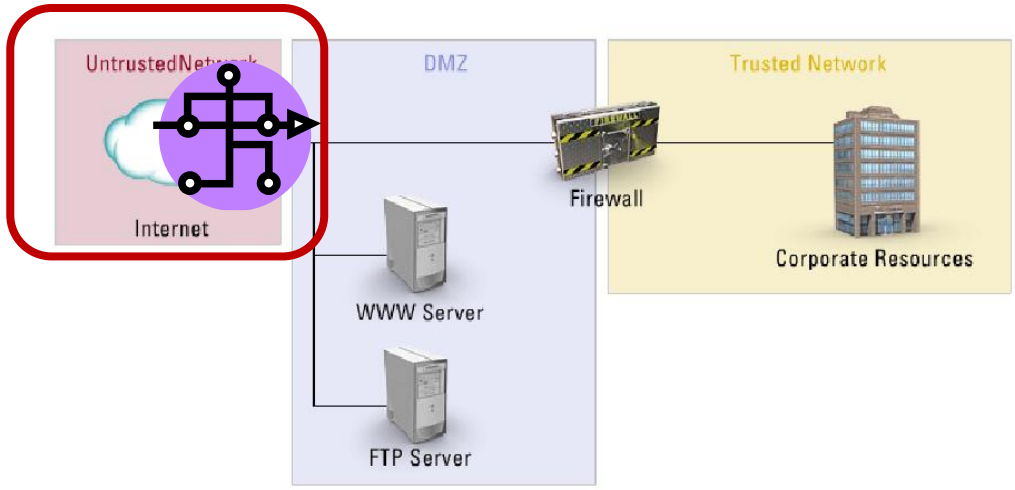
[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 위치에 따른 분류 (1/3)

❖ 외부 공격(external attack) :

- 신뢰된 네트워크(trusted network) 환경에서 외부로부터 허가되지 않은 장치나 장비를 이용해 내부 네트워크를 공격하는 것을 의미



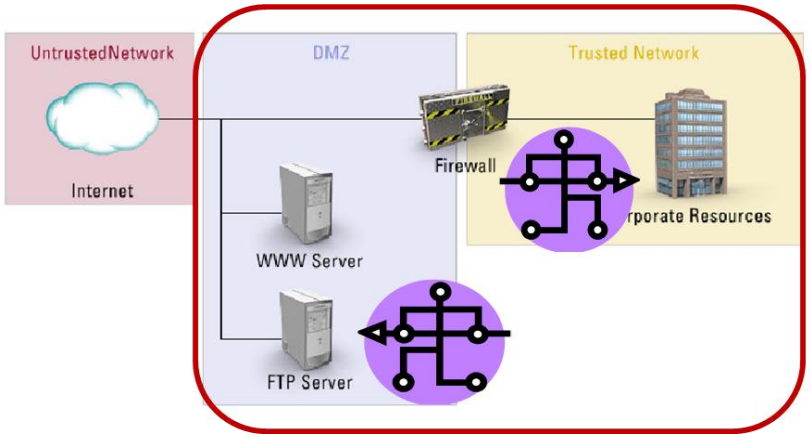
[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 위치에 따른 분류 (2/3)

❖ 내부 공격(inner attack) :

- 보안 영역(DMZ) 내에서는 신뢰하지 못하는 통신이 가능하여, 이를 이용한 보안영역 내에서의 공격을 '내부 공격(internal attack)'이라 함
- 내부 공격을 수행할 경우의 성공률은 약 70% 이상 되며, 대부분이 내부자 공격들로 발생빈도가 매우 높음



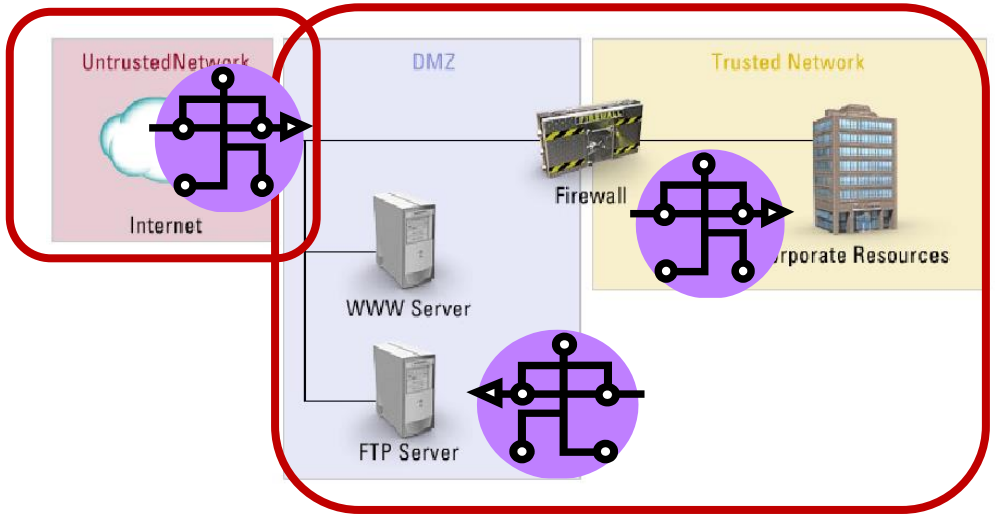
[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 위치에 따른 분류 (3/3)

❖ 흔한 사이버 공격의 대부분은 내부로부터 이뤄지고 있으며,

❖ 외부로부터의 공격은 그 빈도가 낮지만, 위험성이 매우 높음



[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 공격의 체계성에 따른 분류 (1/2)

❖ 조직적 공격(structured attack)

- 공격에 대한 충분한 지식과 경험을 가진 자가 침해 방법, 결정, 관련 지식, 자금, 시간, 장비 등의 치밀한 준비와 수행을 미리 계획하여 공격을 수행 하는 공격을 의미

❖ 비조직적 공격(unstructured attack)

- 충분한 지식과 경험을 갖지 못한 자들의 공격 형태로 해킹 툴이나 유틸리티를 사용하여 공격하는 형태를 의미
- 단순한 툴 사용이나 네트워크 및 법적인 책임에 대해 무지한 공격들이 이에 해당되며, 대부분 이런 공격들은 미성년자 또는 단순 호기심에 의해 이뤄짐

[출처] 정보보호개론 사이텍미디어

2.1 공격 유형의 분류

◆ 공격의 체계성에 따른 분류 (2/2)

❖ 대부분의 국내 사이버 공격의 대부분은 비조직적으로 개인에 의해서 이뤄지는 경우가 다수이며, 조직적인 공격의 경우에는 대부분이 국외 서버를 이용한 외부 공격이 이뤄짐

❖ 조직적인 공격은 특정 목적을 갖고 있기 때문에 공격의 위험성이 매우 높음

[출처] 정보보호개론 사이텍미디어

2. 공격 유형의 분류

2교시 수업을 마치겠습니다.

3. 다양한 공격기법들

3.1 다양한 공격기법들

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ Session Hijacking

- 공격자가 서버와 클라이언트 간 통신을 가로채어 원하는 작업을 수행하여 정보를 유출하는 공격기술

❖ Spam Mail

- 사용자의 의사와는 무관하게 사용자에게 무차별적으로 메일을 전송하여, 대량의 광고 및 기타 상업적 목적으로 발송되는 메일

❖ Sniffing

- 네트워크상에 흘러가는 패킷에서 원하는 정보를 알아내는 해킹 기술로서 이는 네트워크의 한 호스트에서 실행되어 그 주위의 패킷을 엿보는 공격기술

[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 스푸핑 공격(Spoofing)(1/2)

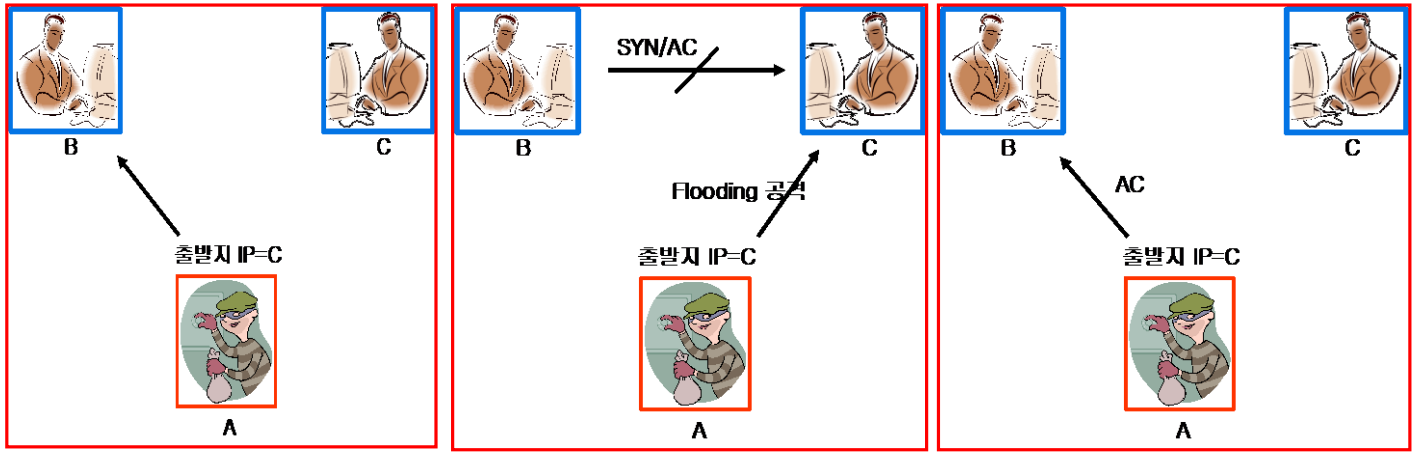
- IP 주소를 속이는 공격방법으로 마치 시스템의 접속 권한을 갖고 있는 것처럼 위장하여 공격하는 방법
- 공격 대상이 신뢰할 수 있는 시스템으로 가장하여 공격 대상에 접근하는 것(1995년 캐빈 미트닉이 샌디에고 슈퍼컴퓨터를 해킹하는데 사용한 방법으로 이후 널리 알려지게 되었음.)

[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 스푸핑 공격(Spoofing)(2/2)



[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 스푸핑 공격(Spoofing) 상세(1/4)

- 스푸핑 공격에는 IP 뿐만 아니라 물리주소(MAC), 도메인 네임 스푸핑 등이 있음
- 이와 같은 스푸핑을 종류로 구분해볼 때, 이를 'IP스푸핑', 'ARP 스푸핑', 'DNS 스푸핑' 이라고 함

[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 스푸핑 공격(Spoofing) 상세(2/4)

- ARP 스푸핑은 MAC 주소를 속여 랜에서의 통신 흐름을 왜곡시키는 공격
- 공격 대상 컴퓨터와 서버 사이의 트래픽을 공격자의 컴퓨터로 우회시켜 패스워드 정보 등 원하는 정보를 획득 할 수 있음

[출처] 위키백과

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 스푸핑 공격(Spoofing) 상세(3/4)

- IP 스푸핑은 IP 자체의 보안 취약성을 악용한 것으로 자신의 IP주소를 속여서 접속하는 공격
- IP 스푸핑을 통해 서비스 거부 공격(DoS)도 수행 가능하며 공격 대상 컴퓨터와 서버 사이의 연결된 세션을 끊을 수도 있음
- 이 문제를 해결하기 위해, 우리는 종단 인증(end point authentication), 즉 메시지가 실제로 와야 할 곳으로부터 온 것인지를 확신할 수 있는 방법이 필요

[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 스푸핑 공격(Spoofing) 상세(4/4)

- DNS 프로토콜은 인터넷 연결 시 도메인 주소를 실제 IP 주소로 대응시켜 주는 프로토콜
- 정상적인 접속에서는 사용자가 접속하고자 하는 사이트에 대한 IP 주소를 DNS 서버에서 받아와야 함
- 공격자가 DNS 서버를 장악하거나 사용자와 DNS 사이의 트래픽을 스니핑하여 공격자가 설정한 임의의 IP 주소를 사용자에게 보내 원하는 사이트로 이동시키는 것과 같은 공격이 DNS 스푸핑 임

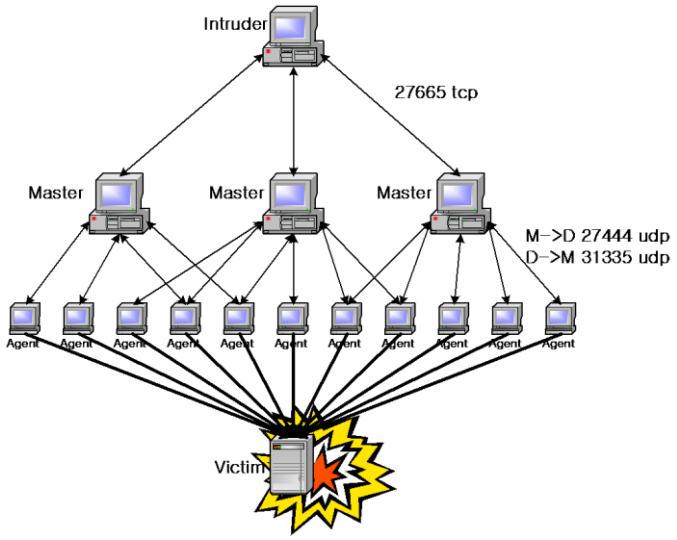
[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ DoS와 DDoS 공격(Denial of service)

- 다중 작업을 지원하는 운영체제에서 발생할 수 있는 공격
- 희생시스템에 서비스를 마비시켜 이를 이용자에게 정상적인 서비스를 제공하지 못하도록 하는 공격(Denial of Service)기술



[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 다양한 공격기법들

❖ 컴퓨터 바이러스(Computer Virus)

- 컴퓨터 시스템의 부트 영역, 메모리 영역, 파일 영역 등에 기생하면서 자기 증식 및 복제가 가능하고, 특정한 공격 목표를 갖고 있으며, 인위적으로 제작한 파괴성을 가진 컴퓨터 프로그램

❖ 웜(Worm)

- 바이러스와 달리 감염 대상을 갖지 않으며, 복제 기능이 없고, 바이러스보다 전파력과 파괴력이 강하여 가장 위험한 유형의 프로그램

[출처] 정보보호개론 사이텍미디어

3.1 다양한 공격기법들

◆ 일상생활의 공격 사례

- ❖ 아이디 & 패스워드
- ❖ 주민번호(게임, 핸드폰 등 명의도용)의 수집
- ❖ 주소 및 전화번호를 악용한 사기
- ❖ 피싱(계좌번호 & 비밀번호) & 보이스 피싱
- ❖ 웹 서버의 접속지연
- ❖ 이 메일의 유출 및 스팸 메일 수신
- ❖ 무단 텔레마케팅
- ❖ 홍보용 우편물
- ❖ 명의 도용 휴대폰 및 계좌개설

[출처] 정보보호개론 사이텍미디어

학습평가

1. (　　)공격은 사용자간의 정상적인 네트워킹을 방해하여 데이터를 중간에 목적지 주소까지 전송되지 못하게 차단하는 공격을 말한다.

2. 의지에 따른 공격 유형의 분류 중 (　　)은 일반적인 공격 형태로 특정한 공격 목표가 없으며, 공격 목표에 대해서도 적극적인 데이터 파괴 및 변조의 목적을 갖지 않는다.

3. (　　) 다중 작업을 지원하는 운영체제에서 발생할 수 있는 공격으로 희생시스템에 서비스를 마비시켜 이를 이용자에게 정상적인 서비스를 제공하지 못하도록 하는 공격기술이다.

[출처] 출처내용 (12포인트, 자간 -1, 단락간격 앞 4, 아래쪽 맞춤)

요약

- ❖ 해커와 크래커의 구분
- ❖ 공격의 분류
- ❖ 공격 유형의 이해
- ❖ 공격기법들의 이해

이번 시간

02주차 사이버 공격의 이해

다음 시간

03주차 사이버 공격 대응

3. 다양한 공격기법들

3교시 수업을 마치겠습니다.