네크워크 보안

〔강평 및 해설 : 임재선 교수〕

총 평

2019년 국가직 9급 네트워크 보안의 전반적인 난이도는 중간이라고 할 수 있겠다. 네트워크 분야에서 무선통신보안 분야와 해킹과 대책을 묻는 문제가 다수 출제되었다.

네트워크 분야에서 망 관리 분야(SNMP)와 인터넷 문제는 많이 나오는 문제이므로 어려움 없이 풀었을 것이다. 그러나 전자서명과 해킹 대책을 묻는 문제는 좀 어렵게 느낄 수 있는 있겠지만 이런 문제일수록 핵심 키워드에 집중하는 방식으로 기출문제를 연습했다면 답을 찾을 수 있는 문제였다.

어려웠을 것으로 생각되는 문제는 서브넷을 묻는 문제였는데 원리면 알면 쉬운 문제였다.

무선통신 보안 문제는 지식을 묻는 문제가 있었는데 외우기 어려워서 힘들었을 것으로 생각한다.

네트워크 보안은 기출문제에서 방화벽과 해킹과 그 대책에서 다수 출제되었다. 기출문제를 중심으로 꾸준히 공부하면서 새로운 경향에 맞춰 이슈를 추가해 나가는 것이 고득점의 길이라 생각한다.

문 1. 네트워크 관리자가 원격으로 네트워크 장비를 모니터링하고 환경 설정을 수행하고자 할 때, 네트워크 구성 요소에 의해 유지되는 변숫값을 조회하거나 변경할 수 있도록 고안된 프로토콜은?

① FTP
② NFS
③ SNMP
④ SMTP

해설

③ SNMP(Simple Network Management Protocol)

TCP/IP 프로토콜 그룹을 이용하여 인터넷에서 장치를 관리하기 위한 서비스의 기반 프로토콜이다. 이것은 인터넷을 감시하고 관리하기 위한 기본적인 운영을 제공한다. 이것은 상호 동작하는 프로토콜을 사용함으로써 이루어지는데, 최상위 레벨에서의 관리는 SMI(Structure of Management Information)와 MIB(Management Information Base)를 통해 이루어진다.

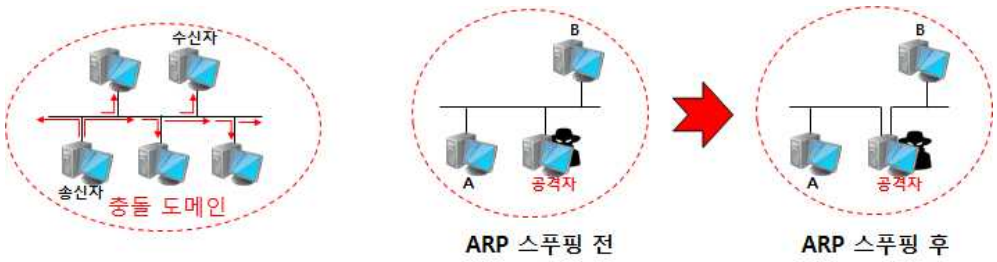
정답 3

문 2. 근거리 통신망에서 공격대상의 MAC 주소를 공격자의 컴퓨터 MAC 주소로 변경하여 공격대상이 전송하는 모든 데이터를 가로챌 수 있는 공격기법은?

① 스위치 재밍
② IP 스푸핑
③ DNS 스푸핑
④ ARP 스푸핑

해설

④ ARP Spoofing(ARP 스푸핑): IP와 상관없이 2계층에서 MAC주소를 속이는 기술이다.



정답 4

문 3. 라우터 외부로 나가는 패킷의 소스 IP만을 검사하여 필터링하는 것으로, 라우터 내부의 네트워크에서 소스 IP를 위조하여 다른 네트워크를 공격하는 형태의 공격을 차단하는 필터링 기법은?

① ingress 필터링
② egress 필터링
③ black hole 필터링
④ null routing을 이용한 필터링

해설

② 이그레스 필터링(Egress Filtering)

이그레스 필더링은 인그레스 필터링과는 달리 라우터 외부로 나가는 패킷을 체크해 필터링하는 것으로, 내부에서 출발지(소스) IP를 위조해 다른 네트워크를 공격하는 형태를 차단할 수 있는 필터링이다.

물론 대규모의 네트워크를 운용하는 곳에서 적용하는 데 무리가 있지만 사용 네트워크 범위가 고정돼 있는 경우 또는 네트워크 말단에서 적용하는 것이 좋다.

정답 2

문 4. 전자금융거래상에서 사용되는 접속정보 및 거래정보, 단말기정보 등을 종합적으로 분석하여 의심되는 거래를 탐지하고 이상금융거래를 차단하는 시스템으로, 일반적인 보안 프로그램에서 방지하지 못하는 전자금융사기의 이상거래를 탐지하고 조치할 수 있는 기법은?

① STP
② ARIA
③ SARA
④ FDS

해설

④ FDS(Fraud Detection System: 이상 금융거래 탐지시스템)

이상 금융거래 탐지시스템 또는 부정사용 방지시스템이라고 불리는 FDS는 전자금융거래 시 단말기 정보와 접속정보, 거래정보 등을 수집·분석해 의심스러운 거래나 평소와 다른 금융 거래가 발생하면 이를 차단한다.

정답 4

문 5. 사설 네트워크 용도로 사용되는 사설 IPv4 주소에 해당하는 것은?

① 10.10.20.300
② 168.10.40.11
③ 172.16.10.20
④ 192.10.20.30

해설

사설 IP : 인터넷에서 공인된 IP 주소를 사용하지 않고, 사적인 용도로 임의 사용하는 IP 주소
- A클래스: 10.0.0.0~10.255.255.255
- B클래스: 172.16.0.0~172.31.255.255
- C클래스: 192.168.0.0~192.168.255.255

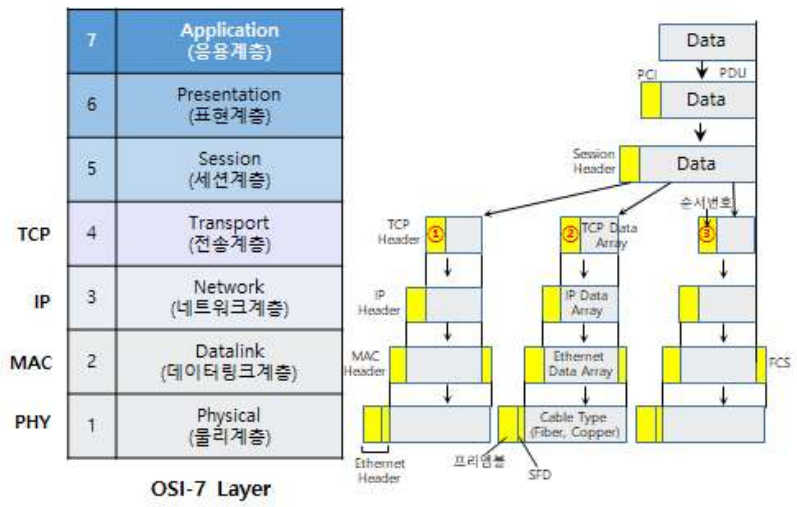
정답 3

문 6. URL(Uniform Resource Locator)이 웹페이지를 정의하는 데 사용하는 식별자가 아닌 것은?

① Protocol
② Sequence Number
③ Host
④ Pat

해설

② Sequence Number : 송신된 데이터의 순서 번호



정답 2

문 7. OSI(Open Systems Interconnection) 참조 모델과 TCP/IP 프로토콜에 대한 설명으로 옳지 않은 것은?

① OSI 참조 모델은 국제 표준 기구인 ISO가 만든 모델이며, 서로 다른 컴퓨터 간의 기능을 여러 계층으로 구분하여 계층 마다 표준화된 서비스와 프로토콜을 규정하였다.

② OSI 참조 모델은 Layer 1인 최상위의 응용 계층부터 Layer 7인 최하위의 물리 계층까지 7개 계층으로 구성된다.

③ 데이터 링크 계층은 물리 계층에서 발생할 수 있는 오류를 발견하는 역할을 한다.

④ 네트워크 계층에서는 출발지부터 목적지까지 여러 링크를 경유하여 패킷을 포워드 할 수 있으며, 이때 IP 주소와 같은 논리 주소가 이용된다.

해설

② OSI 참조 모델은 Layer 1인 최하위의 물리 계층부터 Layer 7인 최상위의 응용 계층까지 7개 계층으로 구성된다.

정답 2

문 8. 다음 중 HTTPS가 사용될 때 통신 간에 암호화되는 요소에 해당하는 것은?

① 요청되는 문서의 URL

② IP 헤더의 TTL 필드

③ TCP 헤더의 플래그 비트들

④ 탐색엔진

해설

HTTPS는 HTTP와 동일한 프로토콜이나 보안 전송 방식인 SSL을 사용하여 네트워크를 통한 모든 데이터의 무결성과 프라이버시를 보호 받는다.

HTTPS 사용 시 암호화되는 통신요소

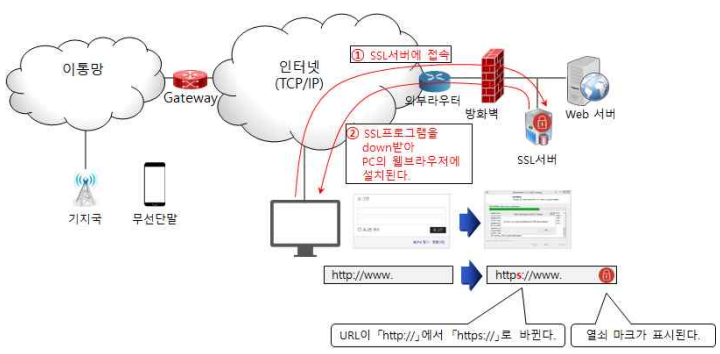
요청문서 URL

문서 내용

브라우저 양식 내용

브라우저가 서버에게 보낸 쿠키와 서버가 브라우저로 보낸 쿠키

HTTP 헤더 내용



정답 1

문 9. HTTP 메시지의 header 정보를 조작하여 서버가 header 정보를 완전히 수신할 때까지 연결을 유지하도록 하여 서버의 가용량을 소비시킴으로써 다른 사용자의 정상적인 서비스를 방해하는 공격은?

① Slowloris 공격
② HTTP CC 공격
③ HTTP GET Flooding 공격
④ Slow HTTP POST 공격

해설

① Slowloris 공격 : 겉으로 보기엔 정상적이지만 느린 속도를 가진 트래픽을 이용한 DoS공격으로 여러 세션을 길게 유지하여 연결 가능한 세션 수를 초과 시켜 정상 연결을 할 수 없도록 하는 공격이다.

정답 1

문 10. 다음 ㉠ ~ ㉣에 들어갈 용어를 바르게 연결한 것은?

가상 사설망이라 불리는 (㉠) 기법은 접근 제어를 위해 보안서비스와 터널링 기술이 요구된다. 터널링 프로토콜로 MS에서 개발한 (㉡) 기법과 시스코에서 개발한 (㉢) 기법이 있으며, 이 둘을 결합한 형태로 (㉣) 기법이 있다.

	㉠	㉡	㉢	㉣
①	VPN	PPTP	L2TP	L2F
②	VPN	PPTP	L2F	L2TP
③	PPTP	VPN	L2TP	L2F
④	PPTP	VPN	L2F	L2TP

해설

VPN(Virtual Private Network)

일반적으로 안전하지 않은 공용 네트워크를 이용하여 사설 네트워크를 구성하는 기술로써, 전용선을 이용한 사설 네트워크에 비해 저렴한 비용으로 안전한 망을 구성할 수 있다.

PPTP, L2F, L2TP는 2계층에서 동작하는 터널링 기술이다.

정답 2

문 11. 데이터링크의 효율성을 위해서 다수의 디바이스가 단일 링크를 공유하여 전송해 주는 기술은?

① 변조
② 부호화
③ 암호화
④ 다중화

해설

다중화(Multiplexing): 다수의 프로세스로부터 메시지를 받아들여 각각의 프로세스마다 할당받은 포트번호를 UDP 헤더에 덧붙여서 IP계층으로 전달한다. 또는 하나의 호스트에 있는 여러 개의 프로세스로부터 전송되는 사용자 데이터그램을 처리하기 위해 다중화 한다.

역다중화(Demultiplexing): 수신한 데이터그램의 오류를 검사하여 오류가 없으면 UDP 헤더의 수신 측 포트번호 필드값을 통해 적절한 상위 프로세스로 메시지를 전달한다.

정답 4

문 12. 부인 봉쇄(non-repudiation) 기능을 제공하는 기법은?

① 디지털 서명
② 트래픽 패딩
③ 접근 제어
④ CRC

해설

① 전자서명(디지털 서명: Digital Signature)

수신자는 수신 받은 원본에서 해시값을 구한 다음 수신 받은 해시값과 비교하여 일치하면 그 문서는 변경되지 않은 것이다(무결성 확보).

이때 송신자는 그 해시값에 부인방지 기능을 부여하기 위해 공개키 방법을 사용한다.

정답 1

문 13. 공중 무선랜의 공격에 대한 대응 기법이 아닌 것은?
① 폐쇄 시스템 운영
② MAC 주소 인증
③ SSID 설정을 통한 접속 제한
④ WEP/WPA 키 크래킹

해설

WEP/WPA(무선랜 보안) : 무선 랜에서의 프라이버시 강화를 위하여 IEEE 802.11에서 WEP를 정의하였으나, 이 표준에서 무결성 보장과 키 사용의 심각한 약점이 발견되었다. Wi-Fi Alliance에서 이를 개선할 목적으로 IEEE 802.11i의 초안에 기초한 중간 조치로 WPA를 공표하였고, 이후 IEEE 802.11i 전체 표준을 따르는 새로운 보안대책으로 WPA2가 등장하게 되었다.

정답 4

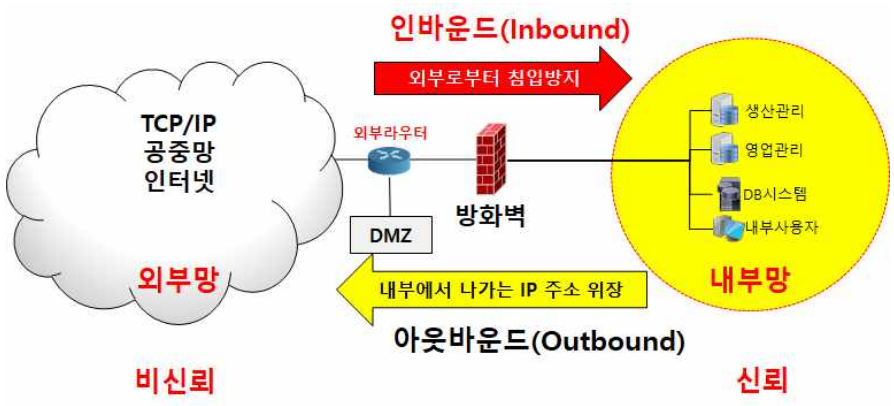
문 14. 방화벽 내에서 내부 사설 IP 주소를 가진 클라이언트가 외부로 접속하는 단계를 순서대로 바르게 나열한 것은?

ㄱ. 원격지 서버가 방화벽이 보낸 패킷에 대한 응답 패킷을 보낸다.
ㄴ. 클라이언트는 내부 IP 주소를 출발지 주소로, 접속하고자 하는 외부 IP 주소를 목적지 주소로 하는 패킷을 생성하여 방화벽으로 보낸다.
ㄷ. 방화벽은 Normal NAT 규칙에 따라 패킷의 출발지 주소를 미리 설정되어 있는 방화벽 IP 주소로 바꾸어 원격지 서버에 전송한다.
ㄹ. 방화벽은 Normal NAT 규칙에 따라 목적지 주소를 처음 접속을 시도한 클라이언트의 내부 IP 주소로 바꾼 후, 클라이언트로 전송한다.

① ㄴ → ㄷ → ㄱ → ㄹ
② ㄴ → ㄹ → ㄱ → ㄷ
③ ㄷ → ㄱ → ㄴ → ㄹ
④ ㄷ → ㄹ → ㄴ → ㄱ

해설

방화벽은 내부 네트워크와 인터넷의 경계점에 게이트웨이 형태로 설치되는 시스템으로, 내부 네트워크와 외부 네트워크 사이에 설치해 상호간에 미치는 영향을 최소화시키는 특별한 목적을 수행하는 시스템 이다.



정답 1

문 15. 스니핑을 수행하는 스니퍼(sniffer)를 탐지하는 방법에 대한 설명으로 옳지 않은 것은?
① 로컬 네트워크에 존재하지 않는 주소로 위장하여 ping(ICMP Echo Request)을 보냈을 때, ICMP Echo Reply를 받으면 해당 호스트는 스니퍼임을 추측할 수 있다.
② FIN 패킷을 보냈을 때, RST 패킷을 받으면 해당 호스트는 스니퍼임을 추측할 수 있다.
③ 특정 호스트에서 promiscuous mode의 설정 여부를 확인하면 스니퍼임을 추측할 수 있다.
④ ARP 트래픽을 모니터링하는 ARP watch를 이용하여 스니퍼임을 추측할 수 있다.

해설

다음은 'promiscuous mode'로 설정된 시스템을 탐지하는 방법에 대하여 설명한다. 아래의 대부분의 방법들은 주로 로컬 네트워크 내에서 탐지가능한 방법이다.
- ping을 이용하는 방법
- ARP를 이용하는 방법
- DNS 방법

- 유인(decoy) 방법
- host method

정답 2

문 16. IPSec에 대한 설명으로 옳지 않은 것은?

① IPSec을 침입차단시스템이나 라우터에서 구현할 경우 경계를 통과하는 모든 트래픽에 적용할 수 있는 강한 보안성을 제공 하기 때문에 회사나 작업그룹 사이의 트래픽 보안을 위해 특별한 처리를 할 필요가 없다.

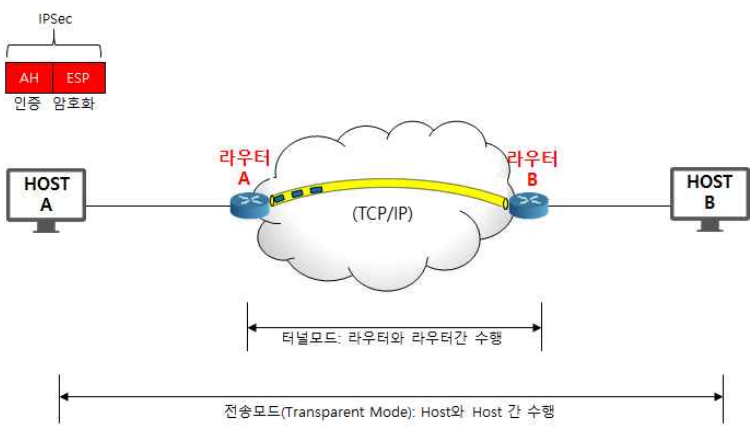
② IPSec은 전송계층(TCP와 UDP)의 아래에 있으며 응용 프로그램에는 투명하다. 침입차단시스템이나 라우터에서 IPSec이 작동되고 있을 때는 서버 시스템과 사용자 시스템의 소프트웨어를 바꿀 필요가 없다.

③ 만약 외부로부터의 모든 트래픽이 IP를 사용해야만 한다면 침입차단시스템에서의 IPSec은 우회하는 트래픽을 차단할 수 없으며, 개별적인 사용자가 보안이 필요하다면 IPSec은그 사용자에게 보안을 제공할 수 없다.

④ IPSec은 종단 사용자에게 투명하게 할 수 있다. 따라서 번거롭게 사용자에게 보안 메커니즘을 훈련시키거나, 개별 기반으로 키를 발급하거나, 사용자가 근무를 그만두고 떠날 때 키를 취소할 필요가 없다.

해설

IPSec은 인터넷에서 이용되고 있는 IP프로토콜은 패킷교환망에서 단순히 데이터의 신뢰성 있는 전송만을 염두에 두고 개발한 것이기 때문에 IP spoofing이나 IP sniffing과 같은 보안 허점이 생겨나게 되었는데, 이를 해결하기 위한 방안으로 등장했다.



정답 3

문 17. 전송계층에 적용되는 SSL(또는 TLS) 보안 프로토콜에 대한 설명으로 옳은 것은?

① Authentication Header 프로토콜은 발신지 호스트를 인증하고 페이로드의 무결성을 보장하기 위하여 설계되었다.

② Alert 프로토콜은 암호화 또는 암호화/인증의 결합을 제공하기 위해 사용되는 캡슐화 헤드와 트레일러로 구성된다.

③ Change Cipher Spec 프로토콜은 연결에서 사용될 암호화 그룹을 갱신하는 프로토콜이다.

④ Handshake 프로토콜은 응용데이터가 전송된 후에 사용되며, 서버와 클라이언트 간의 상호인증, 그리고 암호와 MAC 알고리즘을 협상하지만, 보안 프로토콜로 송신되는 데이터를 보호하기 위한 암호화 키들은 협상하지 않는다.

해설

① Record Protocol

전송계층을 지나기 전에 애플리케이션 데이터를 암호화 한다(상위계층에서 수신된 메시지를 전달하는 역할을 담당).

② Alert Protocol

다양한 에러 메시지를 전달한다.

③ Change Cipher Spec Protocol(암호사양 변경 프로토콜)

방금 협상된 cipher(암호) 규격과 암호키 이용, 추후 레코드의 메시지 보호할 것을 명령한다.

SSL Protocol 중 가장 단순한 Protocol로 Hand Shake Protocol에서 협의된 암호 알고리즘, 키 교환 알고리즘, MAC 암호화, HASH 알고리즘이 사용될 것을 클라이언트와 웹서버에게 공지한다.

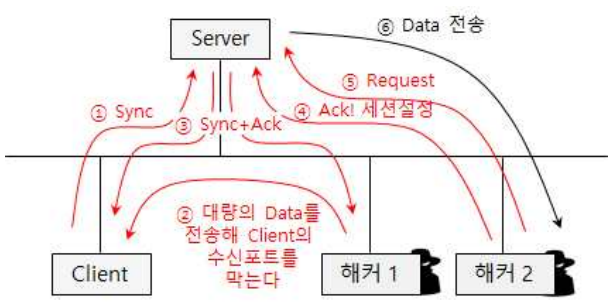
④ Handshake Protocol은 세션정보와 연결정보를 공유하기 위해 이용되는 프로토콜이다.

정답 3

문 18. TCP session hijacking 공격에 대한 설명으로 옳지 않은 것은?
① 이 공격 기법에 대한 대응 방안으로 데이터를 암호화하여 전송하는 방식을 사용한다.
② 이 공격은 클라이언트와 서버가 통신할 때 사용되는 TCP의 sequence number를 이용한 공격이다.
③ 이 공격을 성공적으로 수행하기 위해서는 ARP 스푸핑과 같은 추가적인 공격 기술이 필요하다.
④ 세션 성립은 일반적으로 인증 성립을 의미하며, 인증이 성립된 후에는 이 공격을 막을 수 있다.

해설

Session Hijacking 공격
세션 하이재킹 공격이란 이미 인증을 받아 세션을 생성 및 유지하고 있는 연결을 여러 가지 방법으로 빼앗는 공격을 총칭이다.
Session Hijacking Attack은 세션을 가로채 인증을 우회하는 공격이다.



정답 4

문 19. 네트워크 공격 기법에 대한 설명으로 옳지 않은 것은?
① 서비스 거부 공격은 대상 시스템의 서비스를 중단시키기 위해 공격하는 기법이다.
② 중간자 공격(man-in-the middle attack)은 두 컴퓨터의 통신 중간에 위치하는 공격 기법이다.
③ DDoS 공격은 일반적으로 공격을 증폭시키는 중간자가 사용되는 공격 기법이다.
④ CSRF 공격은 메일 서버를 요청하지 않은 이메일로 공격하는 기법이다.

해설

④ 사이트 간 요청 위조(CSRF: Cross Site Request Forgery)
특정 사용자를 대상으로 하지 않고, 불특정 다수를 대상으로 로그인 된 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록, 송금 등)를 하게 만드는 공격이다.

정답 4

문 20. 203.230.15.0과 같은 IPv4의 C 클래스 네트워크를 30개의 서브넷으로 나누고, 각각의 서브넷에는 5개의 호스트를 연결하려고 한다. 30개의 서브넷 대부분에서 사용되는 서브넷 마스크는?
① 255.255.255.224
② 255.255.255.240
③ 255.255.255.248
④ 255.255.255.252

해설

서브넷팅의 장점은 관리의 효율성을 위해 하나의 큰 네트워크를 몇 개의 작은 논리적인 네트워크로 분할하여 사용하는 방식으로, 적절한 서브넷팅을 통해 IP주소의 낭비를 막아 IP손실을 줄일 수 있다.

2^5 즉 32에서 스위치용과 broadcase용 제외하면 30개의 host를 연결가능 즉 128+64+32+16+8 = 248

정답 3