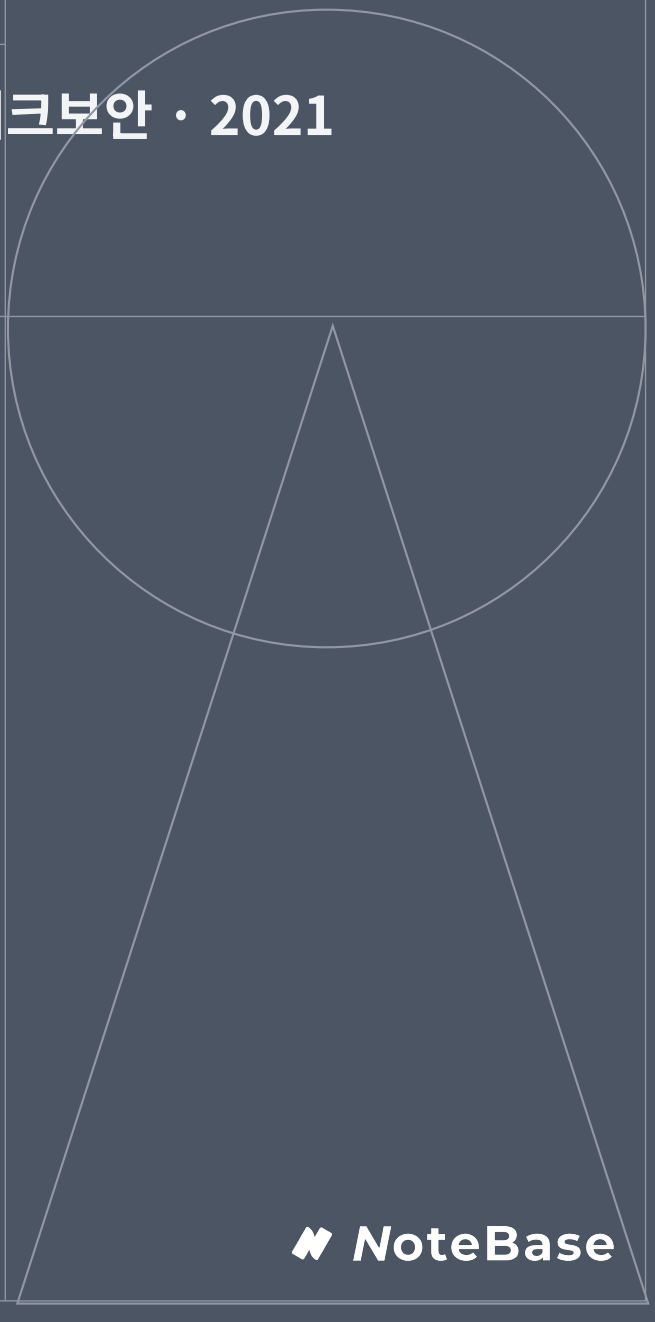
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2021



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2021

공무원/국가직/9급 · 네트워크보안 · 2021

문 1. IPv6의 특성으로 옳지 않은 것은?

① 32Bit에서 128Bit로 확장된 주소 공간

② IP 주소의 동적 할당

③ 인증 및 보안 기능 지원

④ 헤더를 고정길이에서 가변길이로 변경

정답 4번

간단한 해설

IPv6의 기본 헤더는 가변길이가 아니라 **40바이트 고정길이**이다. 선택적인 정보는 기본 헤더 뒤에 붙이는 **확장 헤더**로 처리한다.

선지별 해설

① O: IPv4의 주소 길이는 32비트이고 IPv6는 **128비트**이다. 주소를 나타내는 비트 수가 늘어나므로 표현할 수 있는 주소의 수가 크게 증가한다.

② O: IPv6는 **주소 자동 설정과 동적 할당**을 지원한다. SLAAC 방식에서는 호스트가 라우터가 알려 준 네트워크 접두사와 인터페이스 식별자를 이용해 주소를 구성하고, DHCPv6 방식에서는 서버로부터 주소를 할당받을 수 있다.

③ O: IPv6는 IPsec을 이용한 **인증·무결성·기밀성 보호**를 지원한다. 인증은 통신 상대나 데이터 출처를 확인하고, 무결성 보호는 데이터 변조를 탐지하며, 기밀성 보호는 암호화로 내용을 숨긴다. 다만 IPv6를 사용한다는 사실만으로 모든 통신에 이러한 보호가 자동 적용되는 것은 아니다.

④ X: IPv4 헤더는 옵션의 유무와 길이에 따라 가변길이이지만, IPv6의 기본 헤더는 **40바이트 고정길이**이다. 필요한 선택 정보는 기본 헤더 뒤의 확장 헤더에 담는다. 확장 헤더가 추가되어도 기본 헤더 자체의 길이는 변하지 않으므로, 선지의 '고정길이에서 가변길이로 변경'은 '가변길이에서 고정길이 기본 헤더로 변경'으로 고쳐야 한다.

NoteBase

문 2. 다음에서 설명하는 통신규약은?

◯ IETF에서 만든 공개키암호화 표준을 따름
◯ PGP에 비해 보안성이 높지만 사용이 어려움
◯ 전자우편 사용 시 전송하기 전에 자동으로 암호화하여
전송 도중 유출되어도 편지의 내용을 알 수 없음

① PPTP
② DNS
③ SNMP
④ PEM

정답 4번

간단한 해설

PEM은 IETF에서 표준화한 전자우편 보안 통신규약이다. 공개키 기반의 키 관리와 전자우편 암호화를 통해 **전송 중 메일 내용의 기밀성**을 보호한다.

공통 해설

PEM(Privacy Enhanced Mail)은 전자우편에 암호화와 인증 기능을 제공하기 위한 통신규약이다. IETF의 PEM 표준은 메시지 보호 절차와 공개키 인증서에 기반한 키 관리 체계를 규정한다. 따라서 지문의 '공개키암호화 표준'과 '전자우편을 전송하기 전에 암호화'한다는 단서는 PEM에 대응한다.

공개키 기반 방식에서는 메일 본문을 대칭키로 암호화하고, 그 대칭키를 **수신자의 공개키로 암호화**하여 함께 보낸다. 수신자는 자신의 개인키로 대칭키를 복원한 뒤 메일 본문을 복호화한다. 이 때문에 전송 도중 암호문을 가로채더라도 복호화에 필요한 키가 없으면 내용을 읽을 수 없다. 수신자의 공개키가 실제 수신자의 것인지 확인하기 위해 인증서를 검증하는 절차도 필요하다.

NoteBase

문 3. 무선 LAN에서 사용하는 인증 프로토콜은?

① RIP

② EAP

③ BGP

④ SIP

정답 2번

간단한 해설

EAP는 여러 인증 방식을 지원하는 **확장 인증 프로토콜**로, 무선 LAN에서 접속하려는 사용자를 인증하는 데 사용된다.

개념 구분

EAP(Extensible Authentication Protocol)는 여러 인증 방식을 지원하는 인증 프레임워크이다. IEEE 802.1X 기반 무선 LAN 인증에 사용되며, 인증에 필요한 요청과 응답을 주고받는 공통 틀을 제공한다. 즉, 하나의 고정된 인증 알고리즘이 아니라 **다양한 인증 방식을 수용하는 구조**이다.

RIP와 BGP는 **경로 정보를 교환하는 라우팅 프로토콜**이다. 네트워크 접속자의 신원을 확인하는 EAP와 달리, 패킷을 전달할 경로를 정하는 데 사용된다.

SIP는 음성·영상 통신 등의 **세션을 설정·변경·종료하는 신호 프로토콜**이다. 무선 LAN 접속 인증을 위한 EAP와는 목적이 다르다.

NoteBase

문 4. Land 공격의 출발지 주소와 목적지 주소로 옳은 것은?

① 출발지 주소: 192.168.0.1, 목적지 주소: 192.168.0.1

② 출발지 주소: 192.168.0.1, 목적지 주소: 192.168.0.200

③ 출발지 주소: 192.168.0.5, 목적지 주소: 192.168.0.1

④ 출발지 주소: 192.168.0.5, 목적지 주소: 192.168.0.200

정답 1번

간단한 해설

Land 공격은 패킷의 **출발지 주소와 목적지 주소를 피해 호스트의 동일한 IP 주소**로 설정한다. 두 주소가 모두 192.168.0.1인 경우가 이 특징에 해당한다.

핵심 풀이

Land 공격은 피해 호스트의 IP 주소를 출발지와 목적지에 똑같이 넣은 TCP SYN 패킷을 보내 취약한 호스트의 정상적인 통신 처리를 방해하는 서비스 거부 공격이다. 공격자가 실제 사용하는 주소를 출발지에 쓰는 것이 아니라, **피해 호스트 자신의 주소로 출발지를 위조**한다.

①에서는 출발지와 목적지가 모두 192.168.0.1이므로 피해 호스트가 자기 자신에게 연결을 요청하는 형태가 된다. 반면 ②·③·④는 모두 출발지와 목적지 주소가 서로 다르다. 주소의 앞부분이 같다는 점이 아니라 **두 IP 주소 전체가 동일하다는 점**이 이 문항의 구별 기준이다.

NoteBase

문 5. 다음에서 설명하는 보안 기술은?

◯ 외부 네트워크로부터의 공격 탐지에 중점을 두는 전사적 보안 관리(ESM) 기능에 내부의 정보 유출 탐지 영역까지 담당
◯ ESM와 상호보완적인 관계로 다양한 정보시스템에 대한 로그 관리 및 분석이 강화되고 빅데이터 기술이 접목되어 정보시스템 전반에 대한 신속한 위협탐지가 가능한 지능형 로그 관리 플랫폼

① DLP
② NAC
③ SIEM
④ DRM

정답 3번

간단한 해설

다양한 정보시스템의 **로그를 통합 관리·분석**하여 보안 위협을 탐지하는 기술은 SIEM이다. 빅데이터 기술을 접목한 지능형 로그 분석 플랫폼이라는 설명이 결정적인 단서이다.

공통 해설

SIEM(Security Information and Event Management, 보안 정보 및 이벤트 관리)은 서버·네트워크 장비·보안 장비 등에서 발생하는 로그와 보안 이벤트를 수집하고 통합 분석하는 기술이다. 개별 장비의 기록을 따로 보는 데 그치지 않고 **여러 기록 사이의 연관성을 분석**하여 공격이나 이상 행위의 징후를 찾아낸다.

지문의 '다양한 정보시스템에 대한 로그 관리 및 분석', '빅데이터 기술의 접목', '정보시스템 전반에 대한 신속한 위협탐지'는 이러한 SIEM의 기능을 설명한다. 대량의 로그를 분석하여 외부 공격뿐 아니라 내부 정보 유출의 징후도 탐지할 수 있다는 의미이다. 따라서 '내부의 정보 유출 탐지'라는 일부 표현만으로 기술을 특정하기보다, **정보시스템 전반의 로그를 통합 분석하는 플랫폼**이라는 공통 기준으로 식별한다.

NoteBase

문 6. 포트 스캔에 대한 설명으로 옳지 않은 것은?

① TCP stealth 스캔은 정상적인 3-way handshake를 완성하지 않아 로그를 남기지 않는다.

② XMAS 스캔은 NULL 스캔과 반대로 모든 플래그를 설정하여 패킷을 전송한다.

③ NULL 스캔은 어떠한 플래그도 설정하지 않고 NULL 상태로 패킷을 전송한다.

④ UDP 포트 스캔은 3-way handshake 절차를 거쳐 수행한다.

정답 4번

간단한 해설

UDP는 **연결 설정 절차가 없는 비연결형 프로토콜**이므로 3-way handshake를 수행하지 않는다. UDP 포트 스캔은 대상 포트에 UDP 패킷을 보내고, UDP 응답이나 ICMP 오류 등의 반응으로 상태를 판단한다.

선지별 해설

① O: TCP 스텔스 스캔은 정상적인 TCP 연결을 완성하지 않고 포트 상태를 알아낸다. 대표적인 SYN 스캔은 SYN을 보낸 뒤 SYN/ACK을 받으면 마지막 ACK 대신 RST로 연결 시도를 중단한다. 선지의 '로그를 남기지 않는다'는 **연결이 성립한 뒤 남기는 응용 서비스의 접속 로그를 피한다**는 취지이다. 방화벽이나 침입탐지시스템까지 탐지·기록할 수 없다는 뜻은 아니다.

② O: XMAS 스캔을 SYN·ACK·RST·FIN·PSH·URG 등 TCP 제어 플래그를 모두 켜는 방식으로 설명하는 용례에서는, 플래그를 모두 끄는 NULL 스캔과 반대가 된다. 다만 **XMAS라는 명칭이 항상 모든 플래그의 설정을 뜻하지는 않는다**. 대표적인 Nmap의 XMAS 스캔은 FIN·PSH·URG 세 플래그를 켜며, SYN·ACK·RST는 켜지 않는다. 이 문항의 표현과 Nmap의 구체적인 설정을 구별해야 한다.

③ O: NULL 스캔은 **TCP 제어 플래그를 모두 0으로 설정**한 패킷을 보낸다. NULL은 데이터를 전혀 보내지 않는다는 뜻이 아니라, TCP 헤더의 플래그가 설정되지 않았다는 뜻이다. 이 방식에 예상대로 반응하는 시스템에서는 닫힌 포트가 RST를 반환하지만, 응답이 없을 때는 열린 포트와 필터링된 포트를 확실히 구별할 수 없다.

④ X: 3-way handshake는 TCP에서 SYN → SYN/ACK → ACK를 교환하여 연결을 설정하는 절차이다. UDP는 비연결형이므로 **3-way handshake 없이 UDP 패킷을 전송**하여 포트를 검사한다. 대상 서비스의 UDP 응답은 포트가 열려 있음을 나타내며, ICMP '포트 도달 불가' 오류는 닫힌 포트임을 나타낸다. 응답이 없다는 사실만으로는 포트가 열려 있는지, 방화벽 등이 패킷을 차단했는지 확정할 수 없다.

NoteBase

문 7. Brute Force Attack에 대한 설명으로 옳지 않은 것은?

① 특정 단어 또는 문자 조합으로 성공할 때까지 대입을 시도해 원하는 계정 정보를 얻는다.

② 공격이 가능한 서비스는 Telnet, FTP 등이 있다.

③ 공격을 막는 방법에는 포트 변경, 패스워드 변경, 필터링 툴 사용 등이 있다.

④ 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격한다.

정답 4번

간단한 해설

④의 악성 스크립트가 웹 페이지를 통해 방문자의 브라우저에서 실행되는 방식은 **크로스 사이트 스크립팅(XSS)**이다. 무차별 대입 공격은 **비밀번호 후보를 반복해서 대입**하여 인증정보를 알아내는 방식이다.

선지별 해설

① O: 무차별 대입 공격은 단어나 문자 조합으로 만든 비밀번호 후보를 반복해서 대입하여 인증에 성공하는 값을 찾는다. 핵심은 **후보를 바꾸며 인증을 계속 시도**하는 데 있다. 단어 목록을 중심으로 후보를 고르는 방식은 사전 공격으로 구분하기도 한다.

② O: Telnet과 FTP는 사용자 이름과 비밀번호로 인증하는 서비스를 제공하므로, 공격자가 로그인 요청을 반복하며 비밀번호를 추측할 수 있다. 무차별 대입 공격은 웹 로그인에만 한정되지 않고 **반복적인 인증 시도가 가능한 서비스**를 대상으로 할 수 있다.

③ O: 포트 변경은 기본 포트를 겨냥한 자동화된 접속 시도를 줄이고, 추측하기 어려운 긴 비밀번호로 변경하면 후보 탐색에 필요한 시간이 늘어난다. 필터링 도구는 반복해서 인증에 실패하는 접속을 탐지하여 차단할 수 있다. 다만 **포트 변경만으로 공격을 막을 수는 없으므로**, 비밀번호 강화와 접속 제한을 함께 적용해야 한다.

④ X: 웹 페이지에 삽입된 악성 스크립트가 방문자의 브라우저에서 실행되는 것은 **크로스 사이트 스크립팅(XSS)**에 해당한다. 브라우저가 해당 사이트의 코드로 받아들여 실행하기 때문에, 스크립트는 사용자의 세션 정보를 탈취하거나 페이지 내용을 바꾸는 데 악용될 수 있다. 무차별 대입 공격은 스크립트 실행이 아니라 비밀번호 후보를 반복적으로 대입하여 인증정보를 찾는 공격이다.

NoteBase

문 8. HMAC(Hashed MAC)에 대한 설명으로 옳지 않은 것은?

① RFC2004에서 정의된 HMAC은 수정 없이 이용 가능한 해시 함수를 사용하면 소프트웨어 구현이 어렵다.

② IP 보안을 위한 필수 구현 MAC으로 선택되어 TLS나 SET에서 사용된다.

③ 더 빠르고 안전 해시함수가 있거나 필요하다면 기존의 해시 함수를 쉽게 바꿀 수 있다.

④ 심각하게 기능 저하를 유발하지 않고 해시함수의 원래 성능을 유지하도록 한다.

정답 1번

간단한 해설

HMAC은 기존 해시 함수를 **수정 없이 재사용**할 수 있어 소프트웨어로 구현하기 쉽다. HMAC을 정의한 문서도 선지의 RFC2004가 아니라 **RFC 2104**이다.

선지별 해설

① X: HMAC은 비밀키와 해시 함수를 결합하여 메시지의 무결성과 출처를 확인하는 메시지 인증 코드이다. 기존 해시 함수의 코드를 **수정하지 않고 이용할 수 있어 소프트웨어 구현이 쉽다**. 이미 구현된 해시 함수에 키와 메시지를 조합하여 입력하므로 해시 함수 자체를 새로 만들 필요가 없다. 또한 HMAC을 정의한 문서는 RFC 2104이며, RFC 2004는 IP 최소 캡슐화를 다루는 문서이다.

② O: HMAC은 IPsec의 인증 알고리즘으로 채택되었으며, 기존 IPsec 표준은 HMAC-MD5와 HMAC-SHA-1을 필수 구현 알고리즘으로 규정하였다. TLS의 HMAC 기반 암호군과 전자상거래 보안 프로토콜인 SET에서도 사용된다. 여기서 **필수 구현**은 해당 알고리즘을 지원해야 한다는 뜻이며, 모든 통신에서 반드시 그 알고리즘을 사용해야 한다는 뜻은 아니다.

③ O: HMAC은 특정 해시 함수 하나에 고정된 구조가 아니다. 더 빠르거나 더 안전한 해시 함수가 필요하면 **기반 해시 함수를 교체**할 수 있도록 설계되었다. 다만 송신자와 수신자는 사용할 해시 함수에 합의해야 같은 인증 값을 계산하고 검증할 수 있다.

④ O: HMAC의 설계 목표에는 **해시 함수의 성능을 크게 떨어뜨리지 않는 것**이 포함된다. 기존 해시 연산을 활용하면서 키 처리 등에 필요한 연산을 추가하는 구조이다. 따라서 원래 성능을 유지한다는 설명은 해시 함수만 단독으로 실행할 때와 처리 시간이 완전히 같다는 의미는 아니다.

NoteBase

문 9. 매체 접근 기법 중에서 유선망에서 사용되며, 호스트가 채널의 상태를 감지하여 충돌을 피하는 데이터 전송 방안은?

① Token Bus

② Carrier Sense Multiple Access with Collision Detection

③ Token Ring

④ Carrier Sense Multiple Access with Collision Avoidance

정답 2번

간단한 해설

유선 공유매체에서 채널의 사용 여부를 확인하고, 전송 중 발생한 충돌을 검출해 재전송하는 방식은 **CSMA/CD**이다. 전송 전 채널 감지는 충돌 가능성을 줄이지만 충돌을 완전히 막지는 못한다.

공통 해설

CSMA/CD(Carrier Sense Multiple Access with Collision Detection)는 전통적인 공유매체 이더넷의 반이중 통신에서 사용하는 매체 접근 기법이다. 여러 호스트가 같은 매체를 이용하므로, 데이터를 보내기 전에 반송파를 감지하여 다른 호스트가 전송 중인지 확인한다. 채널이 사용 중이면 기다리고, 비어 있으면 전송한다.

신호가 전파되는 데 시간이 걸리므로 두 호스트가 모두 채널이 비었다고 판단하여 거의 동시에 전송할 수 있다. 이때 충돌을 검출하면 전송을 중단하고 무작위 대기 시간을 거쳐 재전송한다. 즉, **전송 전 채널 감지와 전송 중 충돌 검출**을 함께 사용하는 방식이다. 문제의 '충돌을 피하는'은 채널 감지로 충돌 가능성을 줄인다는 뜻으로 이해해야 하며, 충돌이 전혀 발생하지 않는다는 뜻은 아니다.

Token Bus와 Token Ring은 토큰이라는 전송 권한을 가진 호스트가 데이터를 보내는 방식이므로, 채널 감지로 전송 여부를 결정한다는 설명과 다르다. CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)는 주로 무선 LAN에서 사용하며, 채널 감지와 대기 절차로 충돌 가능성을 줄이는 데 중점을 둔다. 이 문항에서는 '유선망'이라는 조건과 함께 읽어 CSMA/CD를 식별한다.

NoteBase

문 10. VLAN에 대한 설명으로 옳지 않은 것은?

① 물리적 장치의 이동이나 분리 없이 소프트웨어로 하나의 LAN으로 구현된다.

② 물리적인 세그먼트가 아닌 논리적인 세그먼트로 분할한다.

③ VLAN 멤버십 구성 정보로는 포트 번호, MAC주소, IP주소 등이 있다.

④ VLAN 표준으로 IEEE 802.3 부위원회에서 IP 태깅을 위한 IP 형식을 정의하는 802.3Q표준을 제정하였다.

정답 4번

간단한 해설

④의 VLAN 표준은 IEEE 802.1에서 제정한 **802.1Q**이다. 이는 IP 패킷 형식이 아니라 **이더넷 프레임에 VLAN 태그를 넣는 방식**을 규정한다.

선지별 해설

① O: VLAN은 물리적 위치와 독립적으로 장치들을 하나의 논리적 LAN으로 묶는 기술이다. 스위치의 VLAN 설정을 바꾸면 **장치를 옮기거나 배선을 분리하지 않고** 소속 LAN을 구성·변경할 수 있다. 선지의 '소프트웨어로 구현'은 이러한 논리적 설정을 뜻한다.

② O: VLAN은 같은 물리적 스위치에 연결된 장치들도 서로 다른 논리적 세그먼트로 나눌 수 있다. 각 VLAN은 **별도의 브로드캐스트 도메인**을 이루므로, 한 VLAN의 브로드캐스트 프레임이 다른 VLAN으로 그대로 전달되지 않는다.

③ O: VLAN 멤버십은 장치나 트래픽이 어느 VLAN에 속하는지를 뜻한다. 구성 방식에 따라 **스위치 포트, MAC 주소, IP 주소·서브넷** 등을 분류 기준으로 사용할 수 있다. 포트 기반은 연결된 포트를, MAC 기반은 장치의 MAC 주소를, IP 기반은 IP 주소나 서브넷을 기준으로 VLAN을 지정한다.

④ X: VLAN을 규정한 표준은 IEEE 802.1 작업반의 **IEEE 802.1Q**이다. VLAN 태깅은 이더넷 프레임에 VLAN 식별 정보가 담긴 태그를 넣어 프레임이 속한 VLAN을 구별하는 방식이다. 따라서 '802.3 부위원회', '802.3Q', 'IP 태깅을 위한 IP 형식'은 각각 IEEE 802.1 작업반, 802.1Q, **VLAN 태깅을 위한 이더넷 프레임 형식**으로 고쳐야 한다.

NoteBase

문 11. OSI 7계층의 응용 계층 프로토콜로 옳지 않은 것은?

① FTP

② TCP

③ HTTP

④ SMTP

정답 2번

간단한 해설

TCP는 응용 프로그램의 데이터를 신뢰성 있게 전달하는 **전송 계층(4계층)** 프로토콜이다. 따라서 응용 계층(7계층) 프로토콜로 분류할 수 없다.

개념 구분

② TCP: **전송 계층(4계층)**에서 응용 프로그램 사이의 데이터 전달을 담당한다. 데이터의 순서를 관리하고 손실된 데이터를 재전송하여 신뢰성 있는 통신을 제공한다. 파일 전송이나 전자우편 전송 같은 서비스 자체의 규칙을 정하는 응용 계층 프로토콜과 구별된다.

① FTP · ③ HTTP · ④ SMTP: 모두 **응용 계층(7계층)** 프로토콜이다. FTP는 파일 전송, HTTP는 웹 자원에 대한 요청과 응답, SMTP는 전자우편 전송의 규칙을 정한다. 예를 들어 FTP로 파일을 보낼 때 파일 전송 명령과 응답은 FTP가 정하고, 그 데이터를 순서대로 신뢰성 있게 전달하는 일은 TCP가 담당한다.

NoteBase

문 12. L2 스위치에 대한 설명으로 옳은 것은?

① OSI 2계층에서 기능을 수행하며, 고유 MAC 정보를 사용하여 통신한다.

② 패킷의 정보를 확인하여 가장 빠른 네트워크 IP 주소 경로를 찾아내 패킷을 전달한다.

③ 서로 다른 프로토콜 통신망 간에도 프로토콜을 변환하여 정보를 주고받을 수 있다.

④ 응용 계층까지 분석해서 높은 수준의 로드밸런싱을 수행한다.

정답 1번

간단한 해설

L2 스위치는 OSI 2계층인 데이터 링크 계층에서 동작하며, **목적지 MAC 주소**와 MAC 주소 테이블을 바탕으로 프레임을 전달한다.

선지별 해설

① O: L2 스위치는 OSI 2계층인 데이터 링크 계층에서 동작한다. 수신 프레임의 출발지 MAC 주소와 수신 포트의 관계를 학습해 MAC 주소 테이블에 저장하고, **목적지 MAC 주소에 대응하는 포트**로 프레임을 전달한다. 따라서 MAC 정보를 이용한다는 설명이 L2 스위치의 기능에 해당한다.

② X: 목적지 IP 주소를 바탕으로 다른 네트워크로 패킷을 전달하는 것은 **라우터나 L3 스위치**의 기능이다. 이들은 OSI 3계층인 네트워크 계층에서 라우팅 정보를 이용해 전달 경로를 결정한다. L2 스위치의 기본 전달 기준은 IP 주소가 아니라 MAC 주소이다. 또한 라우팅의 최적 경로는 사용하는 지표와 정책에 따라 정해지므로 항상 전송 시간이 가장 짧은 경로를 뜻하지는 않는다.

③ X: 서로 다른 프로토콜을 사용하는 통신망 사이에서 **프로토콜을 변환**하여 통신을 가능하게 하는 것은 게이트웨이의 기능이다. L2 스위치는 MAC 주소를 기준으로 프레임을 전달하는 장비로, 이와 같은 상위 프로토콜 변환을 기본 기능으로 수행하지 않는다.

④ X: 응용 계층의 정보를 분석하여 부하를 분산하는 것은 **L7 스위치 또는 응용 계층 로드밸런서**의 기능이다. 예를 들어 HTTP 요청의 URL이나 헤더 정보를 기준으로 요청을 처리할 서버를 선택할 수 있다. L2 스위치는 데이터 링크 계층에서 프레임을 전달하므로 이러한 응용 계층 분석에 따른 부하 분산은 기본 기능에 해당하지 않는다.

NoteBase

문 13. 다음에서 설명하는 네트워크 기반 유틸리티는?

◯ 네트워크 모니터링 및 패킷 분석을 위해 많이 사용
◯ 패킷 수집을 위해 libpcap 라이브러리를 사용
◯ 유닉스 및 윈도우즈 등에서 사용

① ping
② netstat
③ tcpdump
④ traceroute

정답 3번

간단한 해설

tcpdump는 **libpcap을 이용해 패킷을 수집**하고 그 내용을 분석하는 명령행 도구이다. 네트워크에서 실제로 오가는 패킷을 살펴보는 기능이 결정적인 단서이다.

공통 해설

tcpdump는 네트워크 인터페이스에서 패킷을 수집하고, 수집한 패킷의 주소·프로토콜 등 정보를 해석하여 보여주는 명령행 패킷 분석 도구이다. libpcap은 이때 패킷을 수집하는 기능을 제공하는 라이브러리이다. 따라서 제시된 설명은 **libpcap 기반의 패킷 수집·분석 도구인 tcpdump**에 해당한다. 연결 성공 여부, 현재 연결 상태, 목적지까지의 경로를 확인하는 기능만으로는 이러한 패킷 수집·분석 기능을 설명할 수 없다.

유닉스 계열에서 사용되는 tcpdump는 Windows용 이식판인 WinDump로도 제공되었다. WinDump는 WinPcap을 이용하여 패킷을 수집하므로, 지문의 Windows 사용 설명은 이러한 이식 도구까지 포함하는 맥락으로 이해할 수 있다.

NoteBase

문 14. 취약점을 악용해 공격을 수행하는 프로그램뿐만 아니라 공격 수행 절차, 스크립트 등을 의미하는 것은?

① Exploit

② Bell-LaPadula

③ Biba

④ IPSec

정답 1번

간단한 해설

Exploit은 **취약점을 실제 공격에 이용하는 수단이나 방법**을 뜻한다. 실행 프로그램뿐 아니라 공격용 스크립트와 공격 수행 절차도 포함한다.

공통 해설

Exploit은 시스템이나 소프트웨어의 **취약점을 악용하여 공격을 수행하는 코드나 방법**이다. 취약점이 공격에 이용될 수 있는 약점이라면, Exploit은 그 약점을 실제로 이용하는 수단에 해당한다. 따라서 특정 취약점을 이용하는 실행 프로그램뿐 아니라 같은 공격을 수행하는 스크립트나 절차도 Exploit에 포함된다.

문항의 구별 기준은 '취약점을 악용하는 공격 수단·절차를 뜻하는가'이다. Bell-LaPadula와 Biba는 접근 통제를 위한 보안 모델이고, IPSec은 IP 통신을 보호하는 보안 프로토콜 체계이다. 이들은 취약점을 이용하는 공격 수단·절차의 명칭이 아니므로, 제시된 설명은 Exploit에 해당한다.

NoteBase

문 15. SSH에 대한 설명으로 옳은 것은?

① SSH는 TCP 및 UDP 기반의 보안 프로토콜이다.

② SSH 전송계층 프로토콜, SSH 인증 프로토콜, SSH 연결 프로토콜을 포함한다.

③ SSH는 SSH 터널링을 지원하지 않는다.

④ SSH 전송계층 프로토콜은 다수의 기본 SSH 연결을 사용하여 통신채널을 다중화한다.

정답 2번

간단한 해설

SSH는 **전송계층 프로토콜·사용자 인증 프로토콜·연결 프로토콜**로 구성된다. 각각 안전한 전송, 사용자 신원 확인, 논리 채널 관리를 담당한다.

선지별 해설

① X: SSH는 신뢰성 있는 데이터 스트림을 전제로 하며, 일반적으로 **TCP를 기반으로 동작**한다. TCP와 UDP를 모두 기반으로 하는 보안 프로토콜이라는 설명은 부정확하다.

② O: SSH는 전송계층 프로토콜, 사용자 인증 프로토콜, 연결 프로토콜을 포함한다. 전송계층 프로토콜은 서버 인증과 데이터의 기밀성·무결성을 제공하고, 사용자 인증 프로토콜은 **서버에 접속하는 사용자의 신원**을 확인한다. 연결 프로토콜은 이렇게 확보한 안전한 연결에서 여러 논리 채널을 관리한다.

③ X: SSH는 **SSH 터널링을 지원**한다. 포트 포워딩을 이용하면 다른 TCP 응용프로그램의 통신을 SSH의 암호화된 터널로 전달할 수 있다. 따라서 터널링을 지원하지 않는다는 부분을 지원한다는 내용으로 고쳐야 한다.

④ X: 채널 다중화는 전송계층 프로토콜이 아니라 **SSH 연결 프로토콜**의 역할이다. 또한 다수의 기본 SSH 연결을 사용하는 것이 아니라, **하나의 암호화된 연결에 여러 논리 채널**을 다중화한다. 예를 들어 원격 셸과 포트 포워딩을 서로 다른 채널로 처리하면서 하나의 연결을 공유할 수 있다.

NoteBase

문 16. DDoS 공격기법에 해당하지 않는 것은?

① Trin00

② TFN

③ MITM

④ Stacheldraht

정답 3번

간단한 해설

MITM은 통신하는 두 당사자 사이에 끼어들어 데이터를 **가로채거나 변조하는 중간자 공격**이다. 여러 시스템을 동원해 대상의 정상적인 서비스 이용을 방해하는 DDoS와 구별된다.

개념 구분

DDoS: 분산 서비스 거부 공격으로, 여러 시스템이 특정 대상에 공격 트래픽을 보내 네트워크 대역폭이나 서버 자원을 소모시킨다. 정상 사용자가 서비스를 이용하지 못하게 하므로 **가용성**을 침해한다. Trin00, TFN, Stacheldraht는 이러한 분산 공격을 수행하는 대표적인 도구이다.

MITM: Man-in-the-Middle의 약자로, 공격자가 통신 당사자 사이에 개입하여 오가는 데이터를 가로채거나 변조하는 공격이다. 예를 들어 사용자와 서버 사이의 메시지를 중간에서 읽거나 내용을 바꾸어 전달한다. 핵심은 **통신 내용의 가로채기·변조**이므로, 여러 시스템에서 공격 트래픽을 집중시키는 DDoS 공격기법에 해당하지 않는다.

NoteBase

문 17. 다음에서 설명하는 스위치 환경에서의 스니핑은?

◯ 스위치에 저장 용량 이상의 MAC 주소를 보내 스위치 기능을 잃고 더미 허브처럼 동작하게 만드는 방식
◯ 일부 고가 스위치는 MAC 테이블의 캐시와 연산 장치가 쓰는 캐시가 독립적으로 나뉘어 스니핑 공격이 통하지 않는 경우도 있음

① ICMP 리다이렉트

② SPAN 포트 태핑

③ 스위치 재밍

④ ARP 리다이렉트

정답 3번

간단한 해설

대량의 MAC 주소로 **MAC 주소 테이블을 포화**시켜 다른 호스트의 트래픽을 엿보려는 방식이 **스위치 재밍**이다. 목적지 포트를 알 수 없는 프레임이 여러 포트로 전달되는 현상을 이용한다.

공통 해설

스위치는 MAC 주소 테이블에 MAC 주소와 포트의 대응을 저장하고, 목적지 MAC 주소에 해당하는 포트로 프레임을 전달한다. 목적지 주소가 테이블에 없으면 같은 VLAN에서 수신 포트를 제외한 다른 전달 가능한 포트들로 프레임을 내보낸다. 이를 플러딩이라고 한다.

스위치 재밍은 서로 다른 허위 출발지 MAC 주소를 가진 프레임을 대량으로 보내 MAC 주소 테이블의 저장 공간을 소진시키는 공격이다. 정상 주소를 추가로 학습하지 못하면 그 주소로 향하는 프레임이 플러딩되어 공격자의 포트에도 도달할 수 있다. 지문의 '저장 용량 이상의 MAC 주소'와 '더미 허브처럼 동작'은 이처럼 **MAC 테이블 포화로 플러딩을 유도**하는 원리를 가리킨다.

다만 실제 성공 여부는 스위치의 구현 방식과 보호 기능에 따라 달라진다. 지문의 둘째 항목은 공격이 통하지 않는 장비도 있다는 한정 조건이며, 모든 스위치가 테이블 포화만으로 전체 트래픽을 모든 포트에 보내게 된다는 뜻은 아니다.

NoteBase

문 18. IDS(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은?

① IDS는 네트워크기반 및 호스트기반의 침입탐지시스템으로 분류할 수 있다.

② 침입탐지 기법 중 오용탐지기법은 시그니처기반 탐지 또는 지식기반 탐지로 불린다.

③ 네트워크기반 침입탐지시스템은 네트워크 전반에 대한 감시를 할 수 있다.

④ 호스트기반 침입탐지시스템은 시스템의 로그에 대한 탐지보다는 네트워크 패킷을 수집하여 공격을 판단한다.

정답 4번

간단한 해설

호스트기반 IDS는 **해당 호스트의 시스템 로그와 내부 활동**을 분석하여 침입을 탐지한다. 네트워크 패킷을 수집·분석하여 공격을 판단하는 것은 **네트워크기반 IDS**의 대표적인 방식이다.

선지별 해설

① O: IDS는 감시 대상과 수집 자료에 따라 네트워크기반 IDS(NIDS)와 호스트기반 IDS(HIDS)로 분류할 수 있다. NIDS는 **네트워크 트래픽**을, HIDS는 **개별 호스트의 로그와 내부 활동**을 중심으로 침입 여부를 판단한다.

② O: 오용탐지는 **이미 알려진 공격의 패턴**을 저장해 두고 관찰된 활동이 그 패턴과 일치하는지 확인하는 방식이다. 공격 특징을 나타내는 시그니처나 알려진 공격 지식을 이용하므로 시그니처기반 탐지 또는 지식기반 탐지라고 부른다.

③ O: 네트워크기반 IDS는 센서가 수집할 수 있는 구간의 트래픽을 분석하므로 **여러 호스트와 관련된 통신을 함께 감시**할 수 있다. 이처럼 개별 호스트에 국한되지 않는 감시가 가능하다는 뜻이며, 실제 감시 범위는 센서의 배치와 트래픽 수집 범위에 따라 달라진다.

④ X: 호스트기반 IDS의 대표적인 분석 대상은 **시스템 로그·감사 기록·파일 변경·프로세스 활동** 등 해당 호스트의 내부 정보이다. 예를 들어 비정상적인 로그인 기록이나 중요 파일의 변경을 살펴 침입 징후를 찾는다. 선지의 네트워크 패킷 수집·분석 중심 설명은 네트워크기반 IDS의 특징에 해당한다.

NoteBase

문 19. Wireshark에 대한 설명으로 옳지 않은 것은?

① 윈도우즈 운영체제만을 지원한다.

② www.wireshark.org에서 구할 수 있는 프로그램이다.

③ 네트워크 분석도구이다.

④ 트래픽 수집을 위해 WinPcap을 사용한다.

정답 1번

간단한 해설

Wireshark는 Windows뿐 아니라 **Linux·macOS 등 여러 운영체제**에서 사용할 수 있다. 따라서 '윈도우즈 운영체제만을 지원한다'는 설명은 지원 범위를 잘못 한정한 것이다.

선지별 해설

① X: Wireshark는 **여러 운영체제를 지원**하는 네트워크 분석 도구이다. Windows 외에도 Linux·macOS 등에서 사용할 수 있으므로, '윈도우즈 운영체제만을 지원한다'는 표현을 '여러 운영체제를 지원한다'로 고쳐야 한다.

② O: Wireshark는 공식 웹사이트에서 내려받을 수 있는 무료 오픈 소스 프로그램이다. 운영체제에 맞는 설치 파일이나 소스 코드를 제공한다.

③ O: Wireshark는 네트워크에서 오가는 **패킷을 캡처하고 프로토콜별로 분석**하는 도구이다. 수집한 패킷의 헤더와 내용 등을 확인하여 통신 상태를 파악하거나 네트워크 문제의 원인을 조사할 수 있다.

④ O: 구버전 Windows용 Wireshark는 트래픽 수집에 **WinPcap**을 사용했다. WinPcap은 네트워크 인터페이스를 통해 패킷을 캡처하도록 지원하는 라이브러리이다. 다만 Wireshark 3.0부터 Windows 설치 프로그램에는 Npcap이 포함되며, 최신 버전은 Windows에서 패킷을 캡처할 때 Npcap을 사용한다.

NoteBase

문 20. 네트워크 관리기능에 대한 설명으로 옳은 것은?

① 장애 관리 - 네트워크의 동작 및 효율성을 평가하는 기능

② 구성 관리 - 상호 연결 및 네트워크의 정보를 제공하는 기능

③ 성능 관리 - 비정상적인 동작을 발견하고 대처하는 기능

④ 보안 관리 - 자원 사용량과 관련이 있는 네트워크 데이터를 수집하는 기능

정답 2번

간단한 해설

구성 관리는 네트워크를 이루는 장비와 설정, **장비 간 연결 관계**를 파악하고 관리하는 기능이다. 이를 통해 네트워크가 어떻게 구성되어 있는지에 관한 정보를 제공한다.

선지별 해설

① X: 네트워크의 동작 및 효율성을 평가하는 것은 **성능 관리**이다. 처리량, 응답시간, 오류율 등의 지표를 측정·분석하여 네트워크가 얼마나 원활하게 동작하는지 평가한다.

② O: 구성 관리는 네트워크 장비와 소프트웨어의 구성·설정 및 **상호 연결 관계**를 파악하고 관리한다. 어떤 장비가 연결되어 있고 어떻게 설정되어 있는지에 관한 정보를 제공하므로 선지의 설명과 일치한다.

③ X: 비정상적인 동작을 발견하고 대처하는 것은 **장애 관리**이다. 장애를 탐지하고 원인을 진단하여 정상 상태로 복구하는 기능이며, 성능 관리는 네트워크의 동작 및 효율성을 측정·평가하는 기능이다.

④ X: 자원 사용량과 관련된 네트워크 데이터를 수집하는 것은 **회계 관리**이다. 사용자별 자원 사용량을 기록하여 비용 배분이나 과금 등에 활용한다. 보안 관리는 접근 권한을 통제하고 비인가 사용이나 변조로부터 네트워크 자원을 보호하는 기능이다.

NoteBase