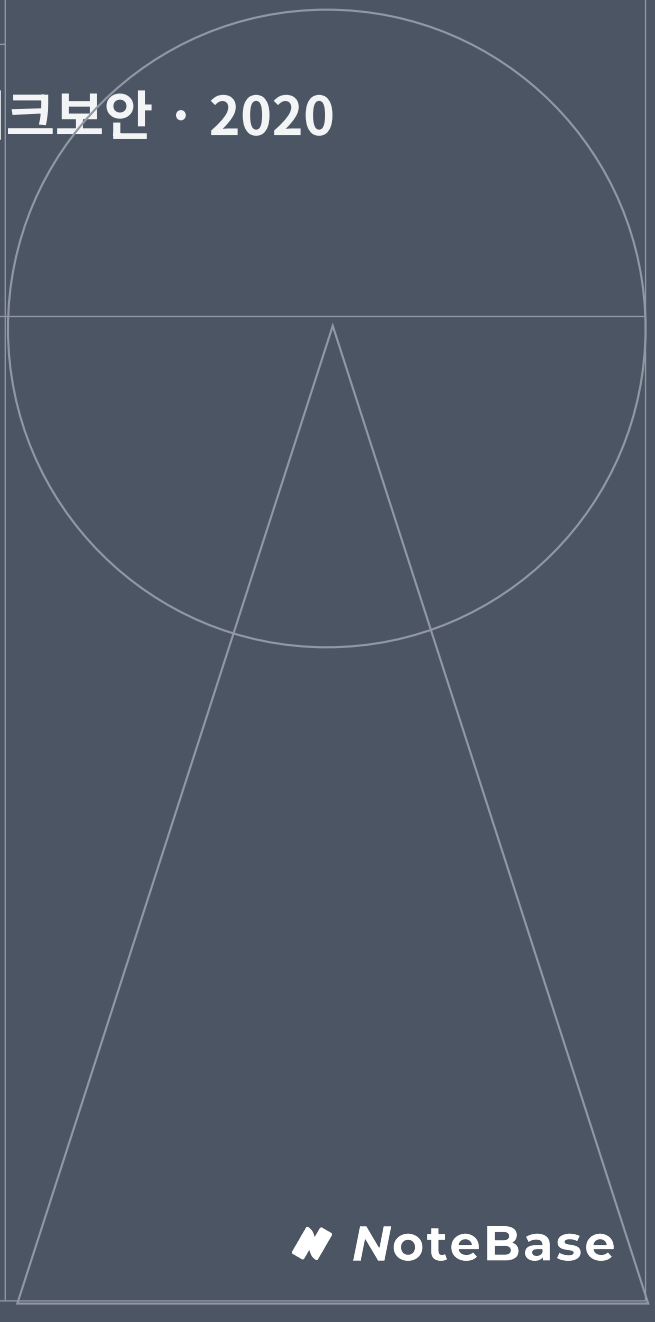
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2020



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2020

공무원/국가직/9급 · 네트워크보안 · 2020

문 1. 전송 과정에서 발생한 데이터 오류를 검출하고 검출된 오류를 정정할 수 있는 것은?

① BCD 코드

② 단일 패리티 비트

③ 해밍(Hamming) 코드

④ 체크섬

정답 3번

간단한 해설

해밍 코드는 여러 패리티 비트의 검사 결과로 오류 위치를 식별하므로 **1비트 오류를 검출하고 정정**할 수 있다.

개념 구분

해밍(Hamming) 코드: 데이터 비트에 여러 패리티 비트를 추가하고, 각 패리티 비트가 서로 다른 비트 묶음을 검사하도록 구성한다. 수신 측은 이 검사 결과를 조합하여 **1비트 오류의 위치를 알아내고**, 해당 비트를 0에서 1로 또는 1에서 0으로 바꾸어 원래 데이터를 복구한다. 따라서 오류 검출뿐 아니라 정정까지 가능한 코드를 묻는 조건에 해당한다.

단일 패리티 비트·체크섬: 단일 패리티 비트는 비트열에서 1의 개수가 정해진 홀수 또는 짝수 조건을 만족하는지 검사한다. 체크섬은 데이터로 계산한 검사값을 수신 측에서 다시 계산한 값과 대조한다. 이들은 오류 검출에 쓰이지만, **검사 결과만으로 잘못된 비트의 위치를 특정하여 정정하는 방식은 아니다**.

BCD 코드: 십진수의 각 자리를 4비트로 표현하는 코드이다. 수를 표현하기 위한 방식으로, 전송 오류를 찾아 정정하기 위한 코드가 아니다.

NoteBase

문 2. 방화벽과 침입탐지시스템의 장점을 결합한 네트워크 보안 장비로, 트래픽 모니터링과 유해 트래픽 차단을 목적으로 하는 것은?

① Honey Pot

② IPS

③ NAC

④ DMZ

정답 2번

간단한 해설

IPS(침입방지시스템)는 트래픽을 감시·분석하여 침입을 탐지하고, **유해 트래픽을 직접 차단**한다. 탐지 기능에 차단 기능을 결합했다는 점이 핵심이다.

개념 구분

IPS(침입방지시스템): 네트워크 트래픽을 분석하여 공격을 탐지하고, 유해한 패킷을 폐기하는 등의 방법으로 침입을 차단한다. 일반적으로 트래픽이 통과하는 경로에 설치하므로 탐지한 공격에 직접 대응할 수 있다. IDS(침입탐지시스템)가 주로 탐지·경보에 초점을 두는 데 비해, IPS는 **탐지와 능동적 차단**을 함께 수행한다. 이것이 문제에서 방화벽과 침입탐지시스템의 장점을 결합했다고 표현한 이유이다.

Honey Pot(허니팟): 공격자를 유인하는 시스템을 마련하여 공격 행위를 관찰·분석한다. 핵심 목적은 **공격 유인과 정보 수집**이다.

NAC(네트워크 접근제어): 접속하려는 사용자·단말을 식별하고 보안 상태 등을 검사하여 **네트워크 접속 허용 여부**를 통제한다.

DMZ(비무장지대): 외부에 공개하는 서버 등을 내부망과 분리하여 배치하는 **네트워크 구간**이다. 트래픽을 탐지·차단하는 보안 장비의 명칭과 구별한다.

NoteBase

문 3. 다음에서 설명하는 SSL 프로토콜은?

메시지의 무결성과 기밀성을 제공하기 위하여, 클라이언트와 서버 간 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증 코드 생성 및 암호화 과정 등을 수행한다.

① Alert Protocol
② Record Protocol
③ Handshake Protocol
④ Change Cipher Spec Protocol

정답 2번

간단한 해설

메시지를 단편화하고, 합의된 방식에 따라 압축·MAC 생성·암호화를 수행하는 것은 **Record Protocol**이다. MAC은 메시지 변조를 검출하여 무결성을, 암호화는 내용을 숨겨 기밀성을 제공한다.

NoteBase

구성 요소별 해설

SSL에서 Record Protocol은 메시지를 보호하여 운반하는 기반이고, Alert·Handshake·Change Cipher Spec Protocol의 메시지도 이 기반을 통해 전달된다. 각 구성 프로토콜은 다음과 같이 역할이 나뉜다.

① Alert Protocol: **오류와 연결 종료를 알리는** 프로토콜이다. 메시지 인증 실패 같은 오류의 종류와 심각도를 전달하며, 정상 종료 때도 종료 알림을 보낸다. 메시지 자체를 단편화하고 암호화하는 처리 절차를 담당하는 것은 아니다.

② Record Protocol: 전송할 메시지를 다룰 수 있는 크기로 단편화하고, 압축한 뒤 MAC을 생성·덧붙이고 암호화하여 전송한다. 압축은 합의된 방식에 따르며 생략될 수 있다. **MAC으로 변조 여부를 검출하고 암호화로 내용을 보호**하므로, 제시문의 무결성과 기밀성 제공에 대응한다.

③ Handshake Protocol: 통신에 사용할 프로토콜 버전과 암호 알고리즘 등 **보안 매개변수를 협상**하고, 필요한 인증과 키 교환을 수행한다. 여기서 마련한 보안 설정을 Record Protocol이 메시지 보호에 사용한다.

④ Change Cipher Spec Protocol: **이후 레코드부터 새로 합의한 암호 설정과 키를 적용**한다는 사실을 상대에게 알린다. Handshake Protocol에서 설정을 협상하는 것과 구별되며, 메시지를 단편화하거나 MAC을 계산하는 처리 자체를 뜻하지 않는다.

제시문의 '단편화, 압축, 메시지 인증 코드 생성 및 암호화'는 전송 메시지를 보호하는 처리이므로 ② Record Protocol에 해당한다.

NoteBase

문 4. IPsec의 SA(Security Association)을 생성하기 위한 키 관리 방식은?

① EAPOL

② OSPF

③ DKIM

④ IKE

정답 4번

간단한 해설

IPsec에서 통신 상대를 인증하고 **SA와 키를 협상·관리**하는 프로토콜은 IKE(Internet Key Exchange)이다.

개념 구분

SA(Security Association)는 IPsec으로 통신을 보호할 때 사용할 알고리즘과 키 등 보안 정보를 정한 관계이다. 양쪽이 서로 다른 키나 알고리즘을 사용하면 보호된 데이터를 정상적으로 처리할 수 없으므로, 통신에 앞서 필요한 정보를 맞춰야 한다. **IKE(Internet Key Exchange)**는 통신 상대를 인증하고 키와 보안 매개변수를 협상하여 IPsec SA를 생성·관리하는 역할을 한다.

EAPOL은 IEEE 802.1X에서 LAN을 통해 인증 관련 메시지를 전달하는 데 사용된다. 따라서 인증과 관련이 있다는 점만으로 **IPsec SA를 생성하는 키 관리 프로토콜**과 혼동하면 안 된다. OSPF는 라우팅 프로토콜이고, DKIM은 전자우편에 도메인 기반 전자서명을 적용하는 방식이므로 문제에서 묻는 역할과 다르다.

NoteBase

문 5. 163.152.175.62/26이 클래스 없는 주소(classless address)로 주어졌다. 해당 IP 주소가 속한 네트워크에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. /26에서의 26은 prefix의 길이를 의미한다.
ㄴ. 네트워크 내의 주소 개수는 128개이다.
ㄷ. 네트워크 마스크는 255.255.255.128이다.
ㄹ. 네트워크에는 주소 163.152.175.15/26이 포함된다.

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 2번

간단한 해설

/26은 IPv4 주소의 앞 **26비트가 네트워크 접두부**라는 뜻이다. 나머지 6비트로 64개의 주소를 나타내므로, 주어진 주소가 속한 네트워크의 범위는 **163.152.175.0~163.152.175.63**이며 163.152.175.15도 여기에 포함된다.

보기별 해설

ㄱ. O: CIDR 표기의 /26은 32비트 IPv4 주소에서 **앞 26비트가 네트워크 접두부**임을 뜻한다. 같은 네트워크에 속한 주소들은 이 접두부를 공유하고, 뒤의 6비트로 네트워크 내부의 주소를 구분한다.

ㄴ. X: 주소를 구분하는 비트가 32 − 26 = 6개이고 각 비트는 0 또는 1이므로, 전체 주소 수는 $2^{32-26} = 2^6 = 64$개이다. 따라서 128개가 아니라 **64개**이다. 이는 네트워크 주소와 브로드캐스트 주소를 포함한 전체 주소 수이다.

ㄷ. X: 네트워크 마스크는 접두부에 해당하는 앞 26비트를 1로, 나머지 6비트를 0으로 채운다. 앞의 세 옥텟은 모두 255이고, 마지막 옥텟은 이진수 11000000이므로 128 + 64 = 192이다. 따라서 마스크는 **255.255.255.192**이다. 보기의 255.255.255.128은 앞 25비트가 1인 /25 마스크이다.

ㄹ. O: /26의 주소 블록은 64개 단위로 나뉘므로 마지막 옥텟의 범위는 0~63, 64~127, 128~191, 192~255이다. 주어진 주소의 마지막 옥텟 62는 0~63에 속하므로 네트워크 주소는 163.152.175.0/26이다. 163.152.175.15/26도 **같은 0~63 범위**에 있으므로 이 네트워크에 포함된다.

옳은 보기는 ㄱ, ㄹ이므로 ②의 조합과 일치한다.

NoteBase

문 6. 다음은 SSL 프로토콜에서 쌍방이 응용 데이터를 전송하기 전에, 인증 및 키 합의를 위하여 교환한 메시지의 일부를 나타낸 것이다. 메시지가 발생하는 순서를 바르게 나열한 것은? (단, 순서 중간에 다른 메시지가 포함될 수 있음)

ㄱ. Client_Key_Exchange
ㄴ. Certificate
ㄷ. Change_Cipher_Spec

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

정답 3번

간단한 해설

인증서로 상대방의 공개키를 확인한 뒤 키 생성에 필요한 정보를 전달한다. **Change_Cipher_Spec**은 키를 교환하는 메시지가 아니라, 준비된 암호 방식과 키를 **이후 레코드에 적용한다는 전환 신호**이므로 키 교환보다 뒤에 온다.

올바른 순서

ㄴ → ㄱ → ㄷ

ㄴ. Certificate: 인증서를 전달하여 공개키와 그 소유자의 신원을 확인할 근거를 제공한다. 서버 인증서는 Client_Key_Exchange보다 먼저 전달되며, 서버가 요청하여 클라이언트 인증서를 보내는 경우에도 그 인증서가 먼저 온다. 이렇게 **인증에 필요한 공개키 정보를 먼저 제공**한 뒤 키 교환을 진행한다.

ㄱ. Client_Key_Exchange: 클라이언트가 선택된 키 교환 방식에 따라 **공유 비밀을 마련하는 데 필요한 정보**를 서버로 보낸다. 예를 들어 RSA 방식에서는 프리마스터 시크릿을 서버의 공개키로 암호화하여 전달한다. 양쪽은 이를 바탕으로 통신에 사용할 키를 준비하므로, 새 키를 적용하는 전환 신호보다 이 메시지가 먼저 와야 한다.

ㄷ. Change_Cipher_Spec: 이후 보내는 레코드부터 **새로 합의한 암호 방식과 키를 적용**한다고 알린다. 키 교환을 통해 필요한 키를 준비한 뒤에 이 전환이 이루어진다. 이어지는 Finished 메시지는 새 암호 설정으로 보호되며, 양쪽의 Finished 교환까지 마치면 응용 데이터를 주고받는다.

NoteBase

문 7. IEEE 802.11i의 키 관리에 대한 다음 설명에서 (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

AAAK라고도 불리는 MSK는 IEEE 802.1X 프로토콜에 의해 인증 단계에서 생성된다. 인증의 마지막 과정이 끝나고 나면 AP(Access Point)와 STA(클라이언트 스테이션)는 (가)를 공유하게 된다. (가)로부터 AP와 STA 간의 통신에 사용할 (나)가 만들어지는데, (나)의 일부인 (다)가 사용자의 무선 데이터 패킷의 암호화에 사용된다.

① (가): PMK, (나): PTK, (다): TK
② (가): PMK, (나): TK, (다): PTK
③ (가): PTK, (나): PMK, (다): TK
④ (가): PTK, (나): TK, (다): PMK

정답 1번

간단한 해설

PMK는 통신용 키를 만드는 기반이고, 여기서 유도한 PTK는 여러 용도의 키를 묶은 것이다. 사용자 데이터의 암호화에는 **PTK의 구성 요소인 TK**를 사용한다.

빈칸별 해설

(가) PMK(Pairwise Master Key): IEEE 802.1X 인증으로 얻은 MSK를 바탕으로 마련되는 마스터 키이다. 인증을 마치면 AP와 STA가 이를 공유하며, **후속 통신용 키를 유도하는 기반**으로 사용한다.

(나) PTK(Pairwise Transient Key): AP와 STA가 4-way handshake 과정에서 PMK, 양쪽의 MAC 주소와 난수인 nonce를 이용하여 유도하는 키 묶음이다. 따라서 지문의 '(가)로부터 AP와 STA 간의 통신에 사용할' 키는 PTK이다. PTK에는 **사용자 데이터 보호용 키와 키 교환 보호용 키**가 포함된다.

(다) TK(Temporal Key): PTK에 포함된 키 중 AP와 STA 사이의 사용자 데이터 패킷을 암호화하는 데 사용하는 키이다. 지문의 **'(나)의 일부'**라는 조건은 TK가 PTK의 구성 요소임을 뜻한다. PMK는 PTK를 만드는 기반이므로 이 자리에 들어가지 않는다.

(가)는 PMK, (나)는 PTK, (다)는 TK이므로 ①의 연결과 일치한다.

NoteBase

문 8. 방화벽 유형의 하나인 응용 레벨 게이트웨이에 대한 설명으로 옳은 것은?

① 외부 네트워크와 내부 네트워크 간의 직접적인 패킷 교환을 허용한다.

② OSI 참조 모델의 응용 계층에서 동작하며 여러 응용 서비스에 대하여 하나의 프록시로 구현된다.

③ 단순 패킷 필터링 방식에 패킷들의 상태 정보를 관리하는 기능이 추가된 것이다.

④ 응용 프로그램 수준의 트래픽을 기록하고 감시하기가 용이하며, 추가로 사용자 인증과 같은 부가 서비스를 지원할 수 있다.

정답 4번

간단한 해설

응용 레벨 게이트웨이는 **응용 프로토콜의 내용을 해석**하므로 서비스별 요청을 자세히 기록하고 감시할 수 있다. 프록시가 통신을 중개하는 과정에서 **사용자 인증**을 요구하는 부가 기능도 제공할 수 있다.

선지별 해설

① X: 응용 레벨 게이트웨이는 내부 호스트와 외부 호스트 사이의 직접 통신을 허용하는 대신 **프록시를 통해 통신을 중개**한다. 클라이언트와 프록시 사이의 연결, 프록시와 목적지 서버 사이의 연결을 각각 맺으므로 두 호스트가 직접 패킷을 주고받는 구조가 아니다.

② X: OSI 참조 모델의 응용 계층에서 동작한다는 부분은 맞지만, 여러 응용 서비스를 하나의 공통 프록시로 처리한다는 부분이 틀리다. 응용 프로토콜의 명령과 데이터 형식을 이해해야 하므로 **응용 서비스별 프록시 기능**이 필요하다. 예를 들어 HTTP와 FTP는 프로토콜이 다르므로 각각에 맞는 프록시 기능으로 처리한다. 이 기능들이 하나의 장비에 함께 구현될 수는 있다.

③ X: 패킷 필터링에 연결 상태를 추적하는 기능을 추가한 것은 **상태 기반 검사 방식**이다. 상태 기반 검사는 연결 상태 정보를 유지하여 해당 패킷이 허용된 연결에 속하는지 판단한다. 응용 레벨 게이트웨이는 프록시가 응용 프로토콜의 내용을 해석하고 통신을 중개한다는 점에서 구별된다.

④ O: 응용 레벨 게이트웨이는 IP 주소와 포트 번호뿐 아니라 응용 프로토콜의 명령이나 요청 내용도 확인할 수 있다. 따라서 **응용 서비스 수준의 상세한 기록과 감시**가 가능하며, 통신을 중개하면서 사용자 이름과 비밀번호 등으로 사용자를 인증하도록 구성할 수도 있다.

NoteBase

문 9. TCP RFC 793을 준수하는 시스템의 닫혀 있는 포트에 대하여 TCP FIN, NULL, Xmas 스캔을 한 경우 시스템의 반응으로 옳은 것은?

① ICMP 도달 불가능 오류 메시지

② 아무 응답 없음

③ RST

④ RST + ACK

정답 3번

간단한 해설

닫힌 TCP 포트는 FIN·NULL·Xmas 탐지 패킷에 **RST 리셋 응답**을 보낸다. 여기서 RST는 응답의 종류를 가리키며, 실제 패킷에 ACK 플래그가 함께 설정되지 않는다는 뜻은 아니다.

핵심 풀이

FIN 스캔은 FIN만, NULL 스캔은 아무 플래그도 설정하지 않고, Xmas 스캔은 FIN·PSH·URG를 설정한 TCP 패킷을 보낸다. 세 방식 모두 **SYN·RST·ACK가 설정되지 않은** 패킷을 사용한다.

RFC 793을 따르는 닫힌 포트는 RST가 없는 탐지 패킷을 받으면 리셋 응답을 보낸다. 반면 열린 포트의 LISTEN 상태에서는 이들 탐지 패킷을 버리므로 응답하지 않는다. 따라서 이 스캔의 기본 구분은 **닫힌 포트의 RST 응답과 열린 포트의 무응답**이다. Nmap은 ICMP 도달 불가능 오류가 돌아오면 해당 오류 유형에 따라 필터링된 상태로 분류한다.

③의 'RST'는 이 리셋 응답의 통칭으로 이해할 수 있다. 다만 RFC 793의 CLOSED 상태 처리 규칙은 수신 패킷에 ACK가 없으면 응답에 **RST와 ACK를 함께 설정**하도록 한다. FIN·NULL·Xmas 탐지 패킷에는 ACK가 없으므로 실제 응답의 플래그 조합은 ④의 'RST + ACK'에 해당한다. 따라서 RST라는 응답 종류와 실제 플래그 조합을 구별해야 하며, ③을 설명하면서 ④의 조합이 RFC에 어긋난다고 단정해서는 안 된다.

NoteBase

문 10. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?

① 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.

② 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.

③ TCP/IP 프로토콜을 사용하는 인터넷에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.

④ MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.

정답 4번

간단한 해설

④는 MIB와 SMI의 역할을 바꾸어 설명했다. 객체의 명명·자료형·부호화에 관한 일반 규칙은 **SMI**가 정의하고, **MIB**는 그 규칙에 따라 정의된 관리 객체들의 집합이다.

선지별 해설

① O: 관리자는 **GetRequest로 관리 객체의 값을 조회**한다. 에이전트는 요청받은 객체의 값을 읽어 응답 메시지로 돌려준다. 관리자는 이를 통해 장치의 상태 정보를 얻는다.

② O: 에이전트는 장애 등 중요한 사건이 발생하면 **관리자의 조회 요청 없이 Trap을 전송**할 수 있다. 예를 들어 통신 링크의 장애를 Trap으로 알리면 관리자는 다음 조회 시점까지 기다리지 않고 상황을 파악할 수 있다.

③ O: SNMP는 TCP/IP 네트워크의 장치를 관리하는 응용 계층 프로토콜이며, 일반적으로 UDP를 사용한다. **UDP 161번은 에이전트의 관리 요청 수신**에, **UDP 162번은 관리자의 Trap 수신**에 사용된다. TCP/IP 기반이라는 말이 SNMP의 전송 계층 프로토콜도 TCP라는 뜻은 아니다.

④ X: 객체의 이름을 부여하고 자료형과 부호화 방식의 일반 규칙을 정의하는 것은 **SMI(Structure of Management Information)**이다. MIB(Management Information Base)는 SMI의 규칙에 따라 정의된 관리 객체들을 모아 놓은 논리적인 정보 저장소이다. 즉, SMI는 관리 정보를 어떤 형식으로 정의할지를 정하고, MIB는 장치 상태나 통신 통계 등 어떤 관리 객체를 다룰지를 구체화한다.

NoteBase

문 11. IPv4 헤더의 필드 중, IP 패킷이 방문할 수 있는 최대 라우터 수를 제한하기 위한 것은?

① Time To Live

② Fragment Offset

③ Header Checksum

④ Flags

정답 1번

간단한 해설

Time To Live(TTL)는 라우터를 거칠 때마다 **최소 1씩 감소**하며, 0이 되면 패킷이 폐기된다. 이 방식으로 통과할 수 있는 라우터 수를 제한하여 패킷이 무한히 순환하는 것을 막는다.

핵심 풀이

Time To Live(TTL): 송신자가 설정한 값이 라우터에서 패킷을 전달할 때마다 최소 1씩 감소한다. TTL이 0이 되면 패킷을 더 전달하지 않고 폐기하므로, **라우터를 거칠 수 있는 횟수의 상한**을 정한다. 라우팅 루프가 발생해도 패킷이 계속 순환하지 못하게 하는 장치이다.

Fragment Offset·Flags: Fragment Offset은 단편화된 데이터가 원래 데이터에서 차지하는 위치를 나타낸다. Flags의 DF는 단편화 금지를, MF는 뒤에 단편이 더 있는지를 나타낸다. 이들은 **단편화와 재조립**에 관련된 필드이다.

Header Checksum: IPv4 헤더의 오류를 검출하기 위한 검사값이다. **헤더의 오류 검출**이 목적이며, 라우터 통과 횟수를 제한하는 값은 아니다.

NoteBase

문 12. TCP 포트 번호 143을 사용하는 메일 접속 프로토콜로, 사용자가 폴더를 생성하고 폴더에 메시지를 할당하는 기능을 제공하는 것은?

① HTTP

② SMTP

③ POP3

④ IMAP

정답 4번

간단한 해설

IMAP은 **TCP 143번 포트**를 사용하는 메일 접속 프로토콜로, 서버의 메일함에 폴더를 만들고 메시지를 폴더별로 관리할 수 있다.

핵심 풀이

IMAP: 사용자가 메일 서버에 접속하여 서버에 저장된 메시지와 메일함을 관리하는 프로토콜이다. TCP 143번 포트를 사용하며, **서버에 폴더를 생성하고 메시지를 폴더에 배치**할 수 있다. 예를 들어 서버에 '업무' 폴더를 만든 뒤 수신한 업무 메일을 그 폴더로 옮길 수 있다. 포트 번호와 폴더 관리 기능이라는 두 단서가 모두 IMAP에 해당한다.

POP3와의 구분: POP3도 메일 서버에서 메시지를 가져오는 프로토콜이지만, **서버의 여러 폴더를 생성·관리하는 기능은 제공하지 않는다**. 따라서 단순히 메일을 받는다는 공통점보다 서버에서 폴더별로 메시지를 관리한다는 기능이 두 프로토콜을 구별하는 기준이다.

NoteBase

문 13. ICMP Echo Request 패킷을 브로드캐스트 주소로 전송하여 많은 양의 응답 패킷이 공격 대상으로 전송되게 하는 서비스 거부 공격은?

① Ping of Death

② SYN Flooding

③ Smurf

④ Land

정답 3번

간단한 해설

브로드캐스트로 전달된 ICMP 요청에 여러 호스트가 응답하도록 하여 트래픽을 증폭시키는 공격이 **Smurf**이다. 요청의 출발지 IP 주소를 공격 대상의 주소로 위조하므로 응답이 공격 대상에 집중된다.

핵심 풀이

Smurf: 공격자는 ICMP Echo Request의 **출발지 IP 주소를 공격 대상의 주소로 위조**하고, 목적지는 브로드캐스트 주소로 지정한다. 브로드캐스트는 해당 네트워크의 여러 호스트에 패킷을 전달하는 방식이다. 이 요청에 응답하는 호스트들은 출발지로 표시된 공격 대상에게 ICMP Echo Reply를 보낸다. 따라서 하나의 요청이 여러 응답을 유발하고, 응답 트래픽이 공격 대상에 집중되어 통신 자원이 소모된다.

Ping of Death와의 구분: Ping of Death는 분할된 IP 패킷을 재조립했을 때 허용 크기를 넘도록 만들어 취약한 시스템의 처리 오류를 유발하는 공격이다. 문제의 단서는 패킷의 비정상적인 크기가 아니라 **브로드캐스트를 통한 다수 호스트의 응답 증폭**이므로 Smurf에 해당한다.

NoteBase

문 14. IPsec 터널 모드를 사용하는 VPN(Virtual Private Network)에 대한 설명으로 옳지 않은 것은?

① 인터넷과 같은 공중망을 이용하여 사설망의 효과를 얻기 위한 기술이다.

② 내부 네트워크의 호스트는 보안 게이트웨이를 거쳐서 통신함으로써 자신의 본래 IP 주소를 외부 네트워크에 노출하지 않는다.

③ 내부 IPv4 패킷의 전체를 암호화하고 선택적으로 인증할 수 있다.

④ IPv6의 경우에는 New IP Header를 사용하지 않고, 본래 헤더를 그대로 사용한다.

정답 4번

간단한 해설

터널 모드는 IPv4와 IPv6 모두 원래 IP 패킷을 통째로 감싸고 **새 외부 IP 헤더**를 붙인다. 원래 헤더를 바깥쪽 헤더로 유지하는 것은 전송 모드의 특징이다.

선지별 해설

① O: VPN은 인터넷 같은 공중망 위에 논리적인 전용 통신 경로를 만들어 사설망처럼 이용하는 기술이다. IPsec 터널 모드는 패킷을 캡슐화하고 암호화·인증 등의 보안 기능을 적용하여 떨어진 내부 네트워크 사이의 통신을 보호할 수 있다.

② O: 보안 게이트웨이 사이에서 ESP 암호화를 적용하면 내부 호스트의 원래 IP 주소가 담긴 헤더도 암호화된다. 외부망에서 전달에 사용하는 것은 **게이트웨이 주소가 담긴 새 외부 IP 헤더**이므로, 내부 호스트의 본래 IP 주소가 외부에 드러나지 않는다.

③ O: ESP를 터널 모드로 사용하면 **원래 IPv4 헤더와 데이터를 포함한 내부 패킷 전체**를 암호화할 수 있다. 인증 기능도 선택하여 적용할 수 있으며, 이를 통해 보호 대상 데이터의 변조 여부와 송신 출처를 확인한다. 새로 붙인 외부 IP 헤더는 내부 패킷의 암호화 범위에 포함되지 않는다.

④ X: IPv6에서도 터널 모드는 **새 외부 IP 헤더를 추가**한다. 원래 IPv6 헤더는 내부 패킷의 일부로 캡슐화되고, 새 외부 헤더는 터널 양 끝 사이에서 패킷을 전달하는 데 쓰인다. 원래 IP 헤더를 바깥쪽에 유지하면서 그 뒤에 ESP를 삽입하는 것은 전송 모드이다.

NoteBase

문 15. 커버로스 버전 4의 메시지 교환 중, 클라이언트(C)가 서버(V)의 서비스를 얻기 위해 티켓발행서버(TGS)에게 보내는 메시지에 포함되지 않는 것은?

① C가 인증서버(AS)로부터 받은 티켓

② V의 식별자

③ C와 V가 사용할 공유비밀키

④ C와 TGS의 세션키로 암호화된 타임스탬프

정답 3번

간단한 해설

C와 V가 사용할 공유비밀키는 **TGS가 서비스 티켓을 발급하면서 생성해 C에게 전달**한다. 따라서 C가 TGS에 서비스 티켓을 요청하는 메시지에는 이 키가 포함되지 않는다.

핵심 풀이

C → TGS 요청: C는 AS에서 받은 티켓발급티켓(TGT), 서비스를 이용하려는 V의 식별자, 인증자를 보낸다. TGT는 TGS에 자신의 인증 사실을 제시하는 데 쓰이고, V의 식별자는 어느 서버의 서비스 티켓을 발급받을지 지정한다. 인증자는 C의 식별자·네트워크 주소·타임스탬프 등을 **C와 TGS가 이미 공유하는 세션키**로 암호화한 것이다. 타임스탬프는 요청의 최신성을 확인하는 데 쓰인다.

TGS → C 응답: TGS는 TGT와 인증자를 확인한 뒤 **C와 V가 사용할 새로운 공유비밀키**를 생성한다. 이 키를 V용 서비스 티켓 안에 넣고, C도 키를 얻을 수 있도록 키와 서비스 티켓 등을 담은 응답을 C와 TGS의 세션키로 암호화해 돌려준다. 따라서 C와 V의 공유비밀키는 요청 메시지에 실어 보내는 정보가 아니라, 요청을 처리한 TGS로부터 받는 정보이다.

NoteBase

문 16. 사설 주소를 이용하는 내부 네트워크를 인터넷에 연결하는 NAT(Network Address Translation) 라우터에 대한 설명으로 옳지 않은 것은?

① 여러 개의 사설 주소는 내부 통신을 위하여 사용하고, 한 개 이상의 전역 인터넷 주소는 외부 통신을 위하여 사용하도록 해 준다.

② 변환 테이블을 이용하여 내부에서 외부로 전송하고자 하는 모든 패킷의 발신지 주소를 전역 주소로 변환해 준다.

③ 외부 인터넷에서 라우터뿐만 아니라 사설 주소를 사용하는 호스트를 식별할 수 있다.

④ 내부 네트워크 호스트와 외부 서버 프로그램들이 다대다 관계를 가질 수 있도록, 변환 테이블에는 IP 주소 외에 전송 계층의 포트 번호와 같은 추가적인 정보가 포함될 수 있다.

정답 3번

간단한 해설

NAT를 거친 패킷에는 **사설 주소 대신 전역 주소**가 표시되므로, 외부에서 그 주소만 보고 내부 호스트의 사설 주소를 직접 식별할 수는 없다. 내부 호스트에 응답을 전달하는 데 필요한 주소 대응은 NAT 라우터가 관리한다.

선지별 해설

① O: NAT는 내부에서 사용하는 사설 IP 주소를 인터넷에서 사용할 수 있는 전역 IP 주소로 변환한다. 따라서 내부 통신에는 사설 주소를 쓰고, 외부 통신에는 **한 개 이상의 전역 주소**를 이용할 수 있다.

② O: 내부 호스트가 인터넷으로 보내는 패킷은 NAT 라우터를 지나면서 **발신지 사설 주소가 전역 주소로 변환**된다. 라우터는 변환 테이블에 주소의 대응을 관리하고, 돌아오는 응답에서는 목적지 전역 주소를 해당 내부 호스트의 사설 주소로 바꾸어 전달한다.

③ X: 외부로 나간 패킷의 발신지 IP 주소에는 **사설 주소가 아닌 전역 주소**가 들어간다. 따라서 외부에서는 변환된 전역 주소를 볼 수 있을 뿐, 그 주소만으로 내부 호스트의 사설 주소를 직접 식별할 수는 없다. 사설 주소와 전역 주소의 대응을 관리하는 주체는 NAT 라우터이다.

④ O: IP 주소와 함께 TCP·UDP 포트 번호도 변환하는 방식을 NAPT 또는 PAT라고 한다. 변환 테이블에 **IP 주소와 포트 번호의 대응**을 기록하면 여러 내부 호스트가 하나의 전역 주소를 공유하면서도 통신을 구분할 수 있다. 예를 들어 내부 호스트 A와 B의 통신에 서로 다른 외부 포트를 배정하면, 응답이 도착한 포트를 보고 해당 내부 호스트로 전달할 수 있다. 이를 통해 여러 내부 호스트가 여러 외부 서버 프로그램과 동시에 통신할 수 있다.

NoteBase

문 17. ARP에 대한 설명으로 옳지 않은 것은?

① 호스트와 라우터는 IP 주소와 MAC 주소의 매핑 정보를 캐시 테이블에 가지고 있다.

② 캐시 테이블 정보를 공격자 호스트의 MAC 주소로 업데이트하게 하는 ARP 스푸핑 공격을 통해 스니핑이 발생할 수 있다.

③ 한 호스트의 캐시 테이블은 서브넷상의 모든 호스트와 라우터에 대한 엔트리를 가지고 있어야 한다.

④ ARP의 요청은 브로드캐스트되고, 응답은 유니캐스트된다.

정답 3번

간단한 해설

③의 '모든 호스트와 라우터에 대한 엔트리를 가지고 있어야 한다'는 설명이 잘못되었다. ARP 캐시는 **필요에 따라 학습한 IP 주소와 MAC 주소의 대응 관계**를 저장하며, 서브넷의 모든 장비에 대한 정보를 미리 갖출 필요는 없다.

선지별 해설

① O: ARP는 같은 링크에서 IPv4 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 호스트와 라우터는 알아낸 **IP 주소와 MAC 주소의 대응 관계**를 ARP 캐시에 저장하여, 이후 프레임을 보낼 때 다시 사용할 수 있다.

② O: ARP 스푸핑은 다른 장비의 IP 주소에 공격자의 MAC 주소가 대응하도록 피해자의 ARP 캐시를 오염시키는 공격이다. 예를 들어 게이트웨이의 IP 주소가 공격자의 MAC 주소에 연결되면, 피해자가 게이트웨이로 보내려던 프레임이 공격자에게 전달된다. 공격자는 이렇게 **자신에게 유도된 트래픽을 가로채어** 스니핑할 수 있다.

③ X: ARP 캐시는 서브넷에 존재하는 모든 장비의 목록이 아니다. 통신에 필요한 MAC 주소가 캐시에 없으면 ARP 요청으로 알아내고, 학습한 대응 관계를 저장하면 된다. 따라서 **모든 호스트와 라우터의 엔트리를 보유할 의무는 없다**. 다른 서브넷으로 보낼 때도 원격 목적지의 MAC 주소가 아니라 같은 링크에 있는 다음 홉 라우터의 MAC 주소를 알아내어 프레임을 보낸다.

④ O: 일반적인 ARP 주소 조회에서 요청자는 대상 IP 주소는 알지만 대상 MAC 주소를 모르므로, 같은 링크의 장비들이 받도록 요청을 **브로드캐스트**한다. 대상 장비는 요청에 포함된 송신자의 MAC 주소를 알 수 있으므로, 자신의 MAC 주소를 담은 응답을 요청자에게 유니캐스트한다.

NoteBase

문 18. TCP의 3-Way Handshaking을 통한 서버와의 연결 설정 과정에서, 연결에 성공한 클라이언트 측의 연결 상태 천이 다이어그램상의 상태 변화의 순서를 바르게 나열한 것은?

① CLOSED → SYN_RCVD → ESTABLISHED

② CLOSED → SYN_SENT → ESTABLISHED

③ LISTEN → SYN_RCVD → ESTABLISHED

④ LISTEN → SYN_SENT → ESTABLISHED

정답 2번

간단한 해설

연결을 먼저 요청하는 클라이언트는 **SYN을 보낸 뒤 SYN_SENT** 상태에서 서버의 응답을 기다린다. 서버의 SYN+ACK를 받고 ACK로 응답하면 연결이 성립하여 ESTABLISHED 상태가 된다.

올바른 순서

CLOSED → SYN_SENT → ESTABLISHED

CLOSED: 아직 TCP 연결이 없는 상태이다. 클라이언트가 서버에 연결을 요청하는 능동 개방을 시작한다. LISTEN은 일반적으로 서버가 **연결 요청을 기다리는** 상태이므로 이 클라이언트의 시작 상태와 구별한다.

SYN_SENT: 클라이언트가 연결 설정을 요청하는 SYN 세그먼트를 보낸 뒤 **서버의 SYN+ACK를 기다리는** 상태이다. 서버는 클라이언트의 SYN을 받아 SYN+ACK를 보내고 SYN_RCVD 상태에서 마지막 ACK를 기다리므로, 양쪽의 대기 상태를 혼동하지 않아야 한다.

ESTABLISHED: 클라이언트가 서버의 SYN+ACK를 정상적으로 받아 자신의 SYN에 대한 확인과 서버의 연결 요청을 확인한 상태이다. 클라이언트는 **마지막 ACK**를 보내고 ESTABLISHED로 전이하여 데이터를 주고받을 수 있다. 서버도 이 ACK를 받으면 ESTABLISHED 상태가 된다.

NoteBase

문 19. IDS의 오용 탐지(misuse detection) 기법에 대한 설명으로 옳은 것은?

① 이미 발견되어 알려진 공격 패턴과 일치하는지를 검사하여 침입을 탐지한다.

② 오탐률이 높지만 새로운 공격 기법을 포함한 광범위한 공격을 탐지할 수 있다.

③ 정상적이고 평균적인 상태의 범주를 벗어나 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생할 경우에 침입 탐지를 알린다.

④ 데이터 마이닝 등을 활용하여 수집한 다양한 정보를 분석하므로 많은 학습 시간이 소요된다.

정답 1번

간단한 해설

오용 탐지는 **이미 알려진 공격 패턴과의 일치 여부**로 침입을 판단한다. 정상 행위에서 벗어났는지를 판단하는 이상 탐지와 구별된다.

선지별 해설

① O: 오용 탐지는 알려진 공격의 특징을 시그니처나 규칙으로 저장하고, 관찰한 패킷이나 로그가 **저장된 공격 패턴과 일치하는지** 검사한다. 따라서 이미 발견된 공격 패턴을 기준으로 침입을 탐지한다는 설명이 맞는다.

② X: 새로운 공격까지 탐지할 수 있지만 정상 행위를 공격으로 잘못 판단할 가능성이 큰 것은 **이상 탐지**의 특성이다. 정상 범위에서 벗어난 행위를 찾기 때문에 알려지지 않은 공격도 탐지할 수 있으나, 드물게 발생하는 정상 행위도 경보를 유발할 수 있다. 오용 탐지는 알려진 패턴에 없는 새로운 공격을 탐지하기 어렵다.

③ X: 정상 상태의 범주에서 크게 벗어나거나 발생 가능성이 낮은 행위에 경보를 내는 것은 이상 탐지의 판단 방식이다. 이때 기준은 **정상 행위와의 차이**이다. 오용 탐지는 정상 상태로부터의 이탈 자체가 아니라 알려진 공격 패턴과의 일치 여부를 기준으로 판단한다.

④ X: 수집한 정보에서 정상 행위의 특성을 학습하여 기준을 만드는 데 시간이 소요된다는 것은 **학습 기반 이상 탐지**의 특성이다. 데이터 마이닝 등을 이용해 정상 행위의 모델을 만든 뒤 현재 행위와 비교할 수 있다. 오용 탐지는 알려진 공격 패턴을 구축·갱신해야 하지만, 정상 행위를 장기간 학습하는 것이 기본 탐지 원리는 아니다.

NoteBase

문 20. IPsec의 ESP에서 재전송 공격(replay attack)을 방지하기 위해 사용하는 것은?

① Sequence Number

② SPI(Security Parameters Index)

③ ICV(Integrity Check Value)

④ Next Header

정답 1번

간단한 해설

ESP는 **Sequence Number(순서 번호)**로 이미 받은 패킷이 다시 도착했는지 확인한다. 공격자가 정상 패킷을 복사해 재전송해도 같은 순서 번호가 중복되므로 이를 탐지하여 폐기할 수 있다.

핵심 풀이

Sequence Number: 재전송 공격은 이전의 정상 패킷을 가로채 다시 보내는 공격이다. ESP 송신자는 같은 보안 연관(SA)에서 패킷을 보낼 때마다 순서 번호를 증가시키고, 수신자는 수신 윈도와 수신 이력을 이용해 **이미 수신한 순서 번호의 중복**을 검사한다. 예를 들어 순서 번호 10인 패킷을 정상적으로 수신한 뒤 같은 패킷이 다시 도착하면 중복으로 폐기한다. 수신 윈도보다 오래된 순서 번호의 패킷도 폐기한다.

SPI(Security Parameters Index): 패킷을 처리할 보안 연관(SA)을 식별하는 값이다. 어떤 보안 설정을 적용할지 찾는 데 쓰이며, **같은 패킷이 다시 왔는지 판별하는 순서 번호와 구별**된다.

ICV(Integrity Check Value): 패킷의 무결성을 검증하는 값이다. 원래 패킷을 그대로 복사해 재전송하면 무결성 검사를 통과할 수 있으므로, **무결성 검사만으로 중복 수신을 판별할 수는 없다**. ESP의 재전송 방지는 순서 번호의 위조를 막는 무결성 보호와 함께 사용한다.

Next Header: ESP가 운반하는 데이터의 프로토콜 종류를 나타낸다. 예를 들어 TCP나 UDP 등을 구별하는 데 쓰이며, 패킷의 중복 여부를 나타내지는 않는다.

NoteBase