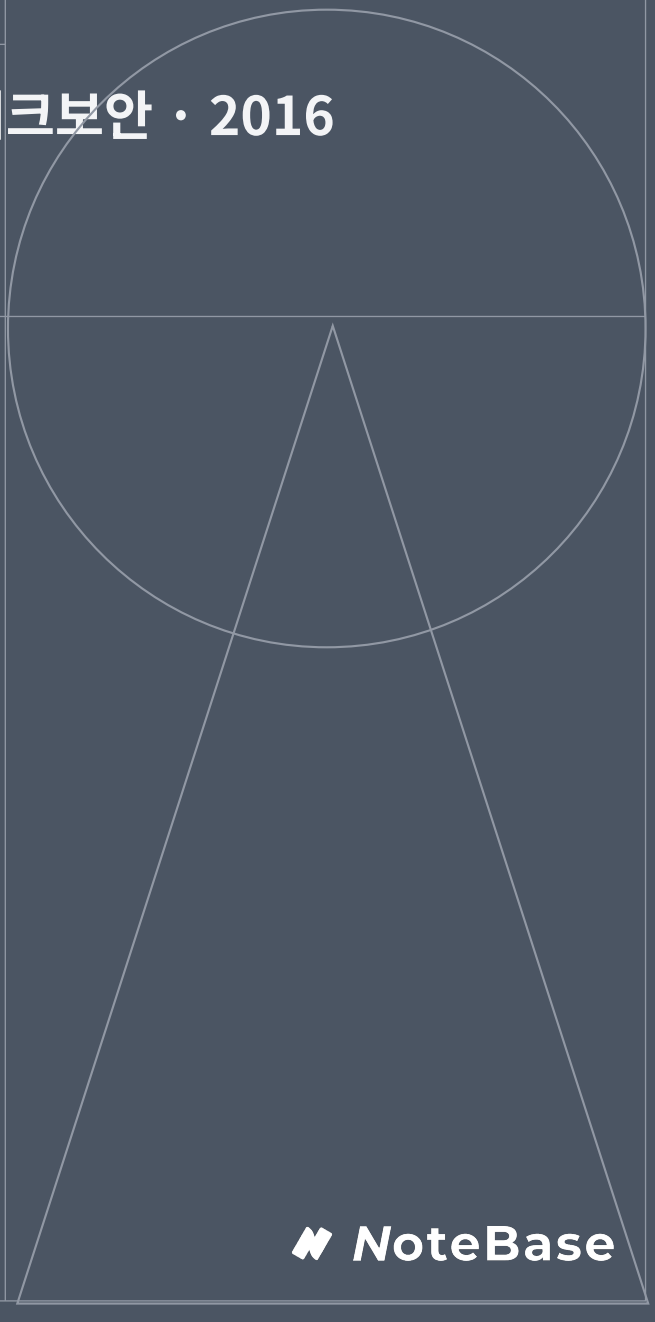
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2016



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2016

공무원/국가직/9급 · 네트워크보안 · 2016

문 1. ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

○ OSI 7계층에서 (㉠)은 물리 계층으로부터 제공되는 물리적 특성을 이용하여 인접한 두 장치 간에 데이터 송·수신을 수행한다.
○ (㉠)은 (㉡)와 (㉢)라는 두 개의 부계층으로 나뉜다.

① ㉠: 데이터링크 계층, ㉡: 논리링크제어, ㉢: 오류제어

② ㉠: 데이터링크 계층, ㉡: 논리링크제어, ㉢: 매체접근제어

③ ㉠: 네트워크 계층, ㉡: 흐름제어, ㉢: 오류제어

④ ㉠: 네트워크 계층, ㉡: 흐름제어, ㉢: 매체접근제어

정답 2번

간단한 해설

인접한 두 장치 사이에서 데이터를 주고받는 계층은 **데이터링크 계층**이다. IEEE 802 구조에서는 이를 **논리링크제어(LLC)와 매체접근제어(MAC)** 부계층으로 나눈다.

NoteBase

빈칸별 해설

㉠ 데이터링크 계층: 물리 계층이 제공하는 비트 전송 기능을 이용하여 데이터를 프레임 단위로 주고받는다. 지문의 **인접한 두 장치 간**이라는 조건이 이 계층에 해당한다. 네트워크 계층은 여러 네트워크를 거쳐 목적지까지 패킷을 전달하기 위한 경로 선택 등을 담당한다.

㉡ 논리링크제어(LLC): IEEE 802에서 데이터링크 계층의 위쪽에 위치하며, 상위 네트워크 계층에 링크 서비스를 제공한다. 아래쪽의 MAC 방식이 달라도 상위 계층이 링크 서비스를 이용할 수 있도록 하는 역할이다. 선지의 흐름제어는 수신 측의 처리 능력에 맞추어 전송량을 조절하는 기능으로, **부계층의 명칭은 아니다**.

㉢ 매체접근제어(MAC): 데이터링크 계층의 아래쪽에서 물리 계층과 연결되며, **전송 매체에 접근하는 방식**을 제어한다. 예를 들어 여러 장치가 매체를 공유할 때 어떤 방식으로 전송 기회를 얻을지를 정한다. 오류제어는 전송 중 발생한 오류를 검출하거나 복구하는 기능을 뜻하며, 두 부계층 중 하나의 명칭이 아니다.

㉠은 데이터링크 계층, ㉡은 논리링크제어, ㉢은 매체접근제어로 연결되며, 이는 ②의 조합과 일치한다.

NoteBase

문 2. ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

○ (㉠) 기법은 이미 알려진 공격 패턴을 근거로 침입을 탐지하는 기법
○ (㉡) 기법은 정상적인 활동에 대한 프로파일을 생성하고, 이 프로파일과 확률적으로 비교하여 벗어나는 행위를 탐지하는 기법
○ (㉢) IDS(Intrusion Detection System)는 네트워크상의 모든 패킷을 캡처링한 후 이를 분석하여 침입을 탐지하는 시스템
※ 이상탐지 : Anomaly Detection, 오용탐지 : Misuse Detection

① ㉠: 이상탐지, ㉡: 오용탐지, ㉢: 네트워크 기반
② ㉠: 이상탐지, ㉡: 오용탐지, ㉢: 호스트 기반
③ ㉠: 오용탐지, ㉡: 이상탐지, ㉢: 네트워크 기반
④ ㉠: 오용탐지, ㉡: 이상탐지, ㉢: 호스트 기반

정답 3번

간단한 해설

이미 알려진 공격 패턴과 대조하는 방식은 **오용탐지**, 정상 활동의 프로파일에서 벗어나는 행위를 찾는 방식은 **이상탐지**이다. 네트워크상의 패킷을 수집·분석하는 IDS는 **네트워크 기반**이다.

빈칸별 해설

㉠·㉡은 침입을 판단하는 방법을, ㉢은 분석하는 자료의 수집 대상과 위치를 구분한다.

㉠ 오용탐지: **이미 알려진 공격 패턴**을 기준으로 현재 활동이 그 패턴에 해당하는지 확인한다. 정상 활동과의 차이를 찾는 것이 아니라, 알려진 공격의 특징과 일치하는지를 판단한다.

㉡ 이상탐지: 정상적인 활동의 특성을 정리한 프로파일을 만들고, 관찰한 활동이 **정상 프로파일에서 벗어나는지**를 통계적으로 비교한다. 판단 기준이 알려진 공격 패턴이 아니라 정상 활동의 범위라는 점에서 오용탐지와 구별된다.

㉢ 네트워크 기반: 네트워크를 오가는 **패킷을 수집·분석**하여 침입을 탐지한다. 호스트 기반 IDS가 개별 호스트의 로그나 시스템 활동 등을 분석하는 것과 구별된다. 제시문의 '네트워크상의 모든 패킷을 캡처링한 후 이를 분석'한다는 설명이 네트워크 기반 IDS를 가리킨다.

㉠ 오용탐지, ㉡ 이상탐지, ㉢ 네트워크 기반의 연결은 ③의 구성과 일치한다.

NoteBase

문 3. 다음에서 설명하는 보안 공격 유형은?

◯ 먼저 목표를 정하여 사전 조사를 실시한다.
◯ 조사를 바탕으로 공격 대상 컴퓨터에 악성코드를 감염시킨다.
◯ 내부 인프라로 서서히 침투하여 몰래 드나들 수 있도록 백도어 및 툴을 설치한다.
◯ 내부 인프라 접속 권한을 상승시키고 정보를 탈취하기 시작한다.
◯ 이후 장기간에 걸쳐 내부 인프라를 장악한 후, 더 많은 정보를 유출하거나 시스템을 파괴하는 등 또 다른 보안 사고를 유발한다.

① 루트킷(Rootkit) 공격
② 랜섬웨어(Ransomware) 공격
③ 지능적 지속 위협(APT) 공격
④ 블루스나프(BlueSnarf) 공격

정답 3번

간단한 해설

특정 목표를 사전 조사한 뒤 은밀히 침투하여 **장기간 접근 권한을 유지**하며 정보를 탈취하는 것은 지능적 지속 위협(APT)의 특징이다. 악성코드 감염 한 번이 아니라 지속적인 내부 장악을 이어 간다는 점이 핵심이다.

공통 해설

지능적 지속 위협(APT, Advanced Persistent Threat)은 특정 대상을 겨냥해 여러 공격 수단을 활용하고, 침투한 뒤에도 **은밀한 접근을 장기간 유지**하며 정보 탈취 등의 목적을 수행하는 위협이다. 특정 악성코드 하나의 명칭이 아니라, 목표에 맞추어 침투와 활동을 지속하는 공격 양상을 뜻한다.

지문의 사전 조사는 공격할 대상을 정하고 그에 맞는 침투를 준비하는 과정이다. 악성코드 감염으로 내부에 진입한 뒤 백도어와 툴을 설치하는 것은 다시 드나들 통로와 활동 수단을 확보하기 위한 것이고, 권한 상승은 더 많은 내부 자원에 접근할 수 있게 한다. 이어서 장기간 내부 인프라를 장악하고 정보를 유출하거나 시스템을 파괴한다는 설명은 **표적에 대한 지속적인 침투·활동**을 보여 주므로 APT 공격에 해당한다.

NoteBase

문 4. 다음에서 설명하는 네트워크는?

◯ 일반적으로 안전하지 않은 공용 네트워크를 이용하여 사설 네트워크를 구성하는 기술로서, 전용선을 이용한 사설 네트워크에 비해 저렴한 비용으로 안전한 망을 구성할 수 있다.
◯ 공용 네트워크로 전달되는 트래픽은 암호화 및 메시지 인증 코드 등을 사용하여 기밀성과 무결성을 제공한다.

① LAN(Local Area Network)
② WAN(Wide Area Network)
③ MAN(Metropolitan Area Network)
④ VPN(Virtual Private Network)

정답 4번

간단한 해설

공용 네트워크를 이용하면서 암호화와 메시지 인증 코드로 통신을 보호하여 **가상의 사설망**을 구성하는 기술은 VPN이다. 기존 공용망을 활용하므로 전용선 기반 사설망보다 비용을 줄일 수 있다.

공통 해설

VPN(Virtual Private Network, 가상 사설망)은 인터넷과 같은 공용 네트워크 위에 논리적인 사설망을 구성하는 기술이다. 물리적인 전용선을 별도로 구축하는 대신 기존 공용망을 활용하므로, 전용선 기반 사설망보다 저렴하게 망을 구성할 수 있다.

지문에서 **암호화는 기밀성**을 제공하여 전송 내용을 제삼자가 알아보기 어렵게 하고, **메시지 인증 코드는 무결성**을 확인하여 전송 중 내용이 변조되었는지 검출하게 한다. 이처럼 안전하지 않은 공용망을 통과하는 트래픽을 보호하면서 사설망처럼 이용한다는 설명이 VPN에 해당한다.

LAN·MAN·WAN은 네트워크를 연결 범위에 따라 구분하는 명칭이다. 이 명칭 자체가 공용망 위에 암호화와 인증을 적용한 사설망을 구성한다는 뜻은 아니므로, 지문이 설명하는 기술과 구별된다.

NoteBase

문 5. 다음의 실행 결과를 제시하는 명령어는?

프로토콜	로컬 주소	외부 주소	상태
TCP	111.111.111.111:49217	222.222.222.221:ms-sql-s	ESTABLISHED
		(중략)	
TCP	111.111.111.111:49216	222.222.222.222:ftp	TIME_WAIT

① nslookup

② route

③ tracert

④ netstat

정답 4번

간단한 해설

프로토콜, 로컬·외부 주소와 함께 ESTABLISHED·TIME_WAIT 같은 **TCP 연결 상태**가 표시되어 있다. 이는 연결 현황을 보여 주는 **netstat**의 출력이다.

공통 해설

netstat는 컴퓨터의 TCP 연결 현황을 표시하는 명령어이다. 각 행에는 사용 중인 프로토콜, 로컬 컴퓨터와 원격 컴퓨터의 IP 주소·포트, TCP 연결 상태가 함께 나타난다. 제시된 결과의 **'프로토콜－로컬 주소－외부 주소－상태'** 열 구성이 이 출력 형식에 해당한다.

첫 행의 로컬 주소 '111.111.111.111:49217'은 이 컴퓨터의 IP 주소와 포트를 뜻하고, 외부 주소는 통신 상대의 주소와 서비스 정보를 나타낸다. 상태 열의 **ESTABLISHED**는 TCP 연결이 수립된 상태이고, TIME_WAIT는 연결 종료 후 일정 시간 대기하는 상태이다. 이처럼 개별 TCP 연결의 양 끝 주소와 상태를 나열한 결과이므로 netstat의 실행 결과로 식별할 수 있다.

NoteBase

문 6. 패킷 필터 방화벽이 네트워크 계층에서 검사할 수 없는 정보는?

① TCP 연결 상태

② 송·수신지 IP주소

③ 송·수신지 포트 번호

④ TCP 플래그 비트

정답 1번

간단한 해설

전통적인 패킷 필터 방화벽은 **개별 패킷의 헤더**를 검사하며, 이전 패킷들과 연결해 **TCP 연결 상태를 추적하지는 않는다**. 연결 상태를 확인하려면 상태 기반 검사 기능이 필요하다.

공통 해설

전통적인 패킷 필터 방화벽은 연결별 통신 이력을 저장하지 않고 각 패킷을 독립적으로 규칙과 대조하는 비상태 검사 방식이다. 따라서 검사 기준은 **현재 패킷의 헤더에서 직접 읽을 수 있는 정보**이다. 송·수신지 IP주소는 IP 헤더에, 송·수신지 포트 번호와 TCP 플래그 비트는 TCP 헤더에 있으므로 필터링에 사용할 수 있다. 네트워크 계층에서 동작하더라도 패킷에 담긴 전송 계층 헤더의 필드까지 검사할 수 있다.

반면 TCP 연결 상태는 여러 패킷의 교환 과정을 연결해 파악하는 정보이다. 예를 들어 현재 패킷의 ACK 비트가 설정되어 있다는 사실은 읽을 수 있지만, 이것만으로 앞서 연결 수립 절차가 정상적으로 이루어졌다고 확인할 수는 없다. **TCP 연결 상태의 추적**은 연결별 상태 테이블을 유지하는 상태 기반 검사 방화벽의 기능이며, 전통적인 패킷 필터 방화벽이 검사할 수 없는 정보에 해당한다.

NoteBase

문 7. 무선랜의 보안을 강화하기 위한 대책으로 안전하지 않은 것은?

① 무선랜 AP 접속 시 데이터 암호화와 사용자 인증 기능을 제공하도록 설정한다.

② 무선랜 AP에 지향성 안테나를 사용한다.

③ 무선랜 AP에 MAC 주소를 필터링하여 등록된 MAC 주소만 허용하는 정책을 설정한다.

④ 무선랜 AP의 이름인 SSID를 브로드캐스팅하도록 설정한다.

정답 4번

간단한 해설

SSID를 브로드캐스팅하면 주변 기기가 **무선랜의 이름과 존재를 쉽게 확인**할 수 있으므로 보안을 강화하는 대책이 되지 않는다. SSID를 숨기더라도 접근을 차단하는 것은 아니므로, 실제 보호에는 암호화와 인증이 필요하다.

선지별 해설

① O: 데이터 암호화는 무선 구간에서 전송 내용을 도청하더라도 내용을 알아보기 어렵게 하고, 사용자 인증은 접속하려는 사용자가 허가된 사용자인지 확인한다. 따라서 **암호화와 인증을 함께 적용**하면 정보 노출과 비인가 접속을 줄일 수 있다.

② O: 지향성 안테나는 전파를 특정 방향으로 집중시키므로, 서비스할 구역에 맞게 방향과 출력을 조절하면 **불필요한 방향으로의 전파 확산**을 줄일 수 있다. 다만 전파의 도달 범위를 조절하는 보조 대책이며, 통신 내용을 암호화하거나 도청 자체를 막는 기능은 아니다.

③ O: MAC 주소 필터링은 접속을 요청한 기기의 MAC 주소를 허용 목록과 대조하여 등록되지 않은 주소의 접속을 제한한다. 다만 공격자가 허용된 MAC 주소를 알아내어 위조할 수 있으므로 **단독으로는 강력한 인증 수단이 되지 못한다**. 암호화 및 사용자 인증과 함께 사용하는 보조적 접근 통제이다.

④ X: SSID는 무선랜을 구별하는 네트워크 이름이다. SSID를 브로드캐스팅하면 주변 기기의 무선랜 검색 목록에 이름이 표시되어 네트워크를 쉽게 발견할 수 있으므로, **브로드캐스팅 자체는 보안 강화 수단이 아니다**. 이름의 노출을 줄이려면 SSID 브로드캐스팅을 중지할 수 있지만, 숨긴 SSID도 무선 통신을 분석하면 알아낼 수 있다. 따라서 SSID 숨김만으로 안전해지는 것은 아니며, 암호화와 인증을 적용해야 한다.

NoteBase

문 8. IPSec 프로토콜의 인증 헤더(AH)와 보안 페이로드 캡슐화(ESP)에서 제공하는 보안서비스 중 ESP에서만 제공하는 보안서비스는?

① 재전송 공격 방지(Replay Attack Protection)

② 메시지 기밀성(Confidentiality)

③ 메시지 무결성(Integrity)

④ 개체 인증(Entity Authentication)

정답 2번

간단한 해설

AH는 내용을 암호화하지 않지만, ESP는 **암호화를 통한 메시지 기밀성**을 제공할 수 있다. 기밀성은 권한 없는 사람이 메시지 내용을 알아보지 못하게 하는 성질이다.

공통 해설

AH와 ESP를 구분하는 기준은 **메시지 내용을 암호화하여 숨길 수 있는가**이다. AH는 메시지의 변조 여부와 송신 출처를 확인하는 인증·무결성 기능을 제공하고 재전송 공격도 방지할 수 있지만, 메시지 자체를 암호화하지는 않는다. ESP는 이러한 보안서비스에 더하여 암호화로 메시지 내용을 보호하는 기밀성을 제공할 수 있다. 따라서 제시된 서비스 중 ESP에만 있는 것은 메시지 기밀성이다.

재전송 공격 방지·메시지 무결성·인증은 AH에서도 제공하므로 ESP만의 특징이 아니다. 여기서 선지의 '개체 인증'은 패킷의 송신 출처를 확인하는 인증 기능과 연결하여 이해한다. ESP에서 실제로 사용하는 서비스는 설정에 따라 달라지며, **기밀성을 사용하려면 암호화 기능을 활성화**해야 한다.

NoteBase

문 9. NAT(Network Address Translation)에 대한 설명으로 옳지 않은 것은?

① 한정된 공인 IP주소 부족 문제의 해결이 가능하다.

② 공인 IP와 NAT IP의 매핑이 1:1만 가능하다.

③ 주소 변환 기능을 제공한다.

④ 내부 시스템에 네트워크 구조를 노출하지 않는 보안상의 이점을 제공한다.

정답 2번

간단한 해설

②의 '1:1만 가능하다'는 제한이 잘못되었다. NAT에는 1:1 주소 변환뿐 아니라, 포트 번호로 통신을 구분하여 **여러 내부 IP주소가 하나의 공인 IP주소를 공유**하는 NAPT(PAT)도 있다.

선지별 해설

① O: 내부 호스트마다 공인 IP주소를 하나씩 부여하는 대신, 사설 IP주소를 사용하고 외부 통신 시 주소를 변환할 수 있다. 특히 NAPT를 이용하면 **여러 호스트가 하나의 공인 IP주소를 공유**하므로 필요한 공인 IPv4 주소 수를 줄여 주소 부족 문제를 완화한다.

② X: 정적 NAT에서는 내부 IP주소와 공인 IP주소를 1:1로 대응시킬 수 있지만, NAT 전체가 이 방식으로 제한되지는 않는다. **NAPT(PAT)는 IP주소와 TCP/UDP 포트 번호를 함께 변환**하여 여러 내부 호스트를 하나의 공인 IP주소에 대응시킨다. 예를 들어 내부 호스트 A와 B가 같은 공인 IP주소로 통신하더라도 서로 다른 변환 포트 번호를 사용하면, NAT 장비는 돌아온 패킷을 어느 호스트로 보낼지 구분할 수 있다.

③ O: NAT는 패킷이 서로 다른 주소 영역 사이를 지날 때 **IP 헤더의 주소를 변환**한다. 내부 호스트가 외부로 보낸 패킷의 사설 출발지 주소를 공인 주소로 바꾸고, 응답 패킷은 해당 변환 관계에 따라 내부 호스트의 주소로 되돌려 전달한다.

④ O: 선지의 보안상 이점은 **내부 주소 체계의 외부 노출을 줄이는 효과**로 이해한다. 외부에서는 변환된 공인 IP주소를 보므로 내부 호스트의 사설 IP주소가 그대로 드러나지 않는다. 이는 내부 시스템 자체에 네트워크 구조를 숨긴다는 의미는 아니며, NAT만으로 모든 공격을 차단한다는 뜻도 아니다.

NoteBase

문 10. SSL(Secure Socket Layer)의 레코드 프로토콜에서 응용 메시지를 처리하는 동작 순서를 바르게 나열한 것은?

※ MAC : Message Authentication Code

① 압축→단편화→암호화→MAC 첨부→SSL 레코드 헤더 붙이기

② 압축→단편화→MAC 첨부→암호화→SSL 레코드 헤더 붙이기

③ 단편화→MAC 첨부→압축→암호화→SSL 레코드 헤더 붙이기

④ 단편화→압축→MAC 첨부→암호화→SSL 레코드 헤더 붙이기

정답 4번

간단한 해설

MAC은 **압축된 데이터의 변조를 검출**하기 위한 값으로, 데이터에 붙인 뒤 **데이터와 함께 암호화**한다. 따라서 MAC을 암호화 뒤에 첨부하거나 MAC 첨부 뒤에 압축하는 순서는 맞지 않는다.

NoteBase

올바른 순서

단편화 → 압축 → MAC 첨부 → 암호화 → SSL 레코드 헤더 붙이기

단편화: 응용 메시지를 레코드로 처리할 수 있는 크기의 조각으로 나눈다. 이후의 압축과 보안 처리는 이 **단편화된 데이터 단위**로 수행한다.

압축: 단편화된 데이터에 세션에서 정한 압축 방식을 적용한다. 실제 압축을 사용하는 경우 데이터를 손실 없이 줄이며, 압축하지 않는 방식이 선택되면 데이터가 그대로 통과한다. MAC은 이 단계에서 나온 **압축 처리 결과**를 바탕으로 계산하므로 압축이 MAC 첨부보다 앞선다.

MAC 첨부: MAC은 비밀키를 이용하여 메시지의 무결성과 출처를 검증하는 메시지 인증 코드이다. 압축된 데이터와 순서번호 등 필요한 정보를 이용하여 MAC을 계산하고 데이터에 붙인다. 수신자는 같은 방식으로 계산한 값과 비교하여 변조 여부를 확인한다.

암호화: **압축된 데이터와 첨부된 MAC을 함께 암호화**하여 내용을 보호한다. 따라서 MAC을 암호화 뒤에 붙이는 순서로 바꾸면 SSL 레코드 프로토콜의 처리 방식과 달라진다. 블록 암호를 사용하는 경우에는 필요한 패딩도 포함하여 암호화한다.

SSL 레코드 헤더 붙이기: 암호화된 본문 앞에 콘텐츠 유형, 프로토콜 버전, 본문 길이 등을 담은 헤더를 붙여 전송할 레코드를 구성한다. 헤더의 길이 정보는 **암호화된 본문의 길이**를 나타내므로 최종 본문이 만들어진 뒤 그에 맞게 설정한다.

NoteBase

문 11. ㉠과 ㉡에 들어갈 용어를 바르게 연결한 것은?

○ (㉠)는(은) 네트워크 중간에서 상대방의 패킷 정보를 도청하는 수동적 공격이다.
○ (㉠) 공격의 대응 방안으로 텔넷의 경우 원격 접속 시 평문 패킷의 암호화를 지원하기 위해 (㉡)를(을) 사용한다.

① ㉠: ARP watch, ㉡: SSH
② ㉠: ARP watch, ㉡: PGP
③ ㉠: Sniffing, ㉡: SSH
④ ㉠: Sniffing, ㉡: PGP

정답 3번

간단한 해설

네트워크 패킷을 몰래 수집해 내용을 엿보는 수동적 공격은 **스니핑(Sniffing)**이다. 평문으로 통신하는 텔넷 대신 **SSH의 암호화된 원격 접속**을 이용하면 도청에 따른 정보 노출을 방지할 수 있다.

빈칸별 해설

㉠ Sniffing: 스니핑은 네트워크를 흐르는 패킷을 수집하여 그 내용을 엿보는 공격이다. 제시문처럼 통신 내용을 변경하지 않고 관찰하는 방식은 **수동적 공격**에 해당한다. 암호화되지 않은 인증정보가 담긴 패킷을 수집하면 그 정보를 읽을 수 있다. ARP watch는 IP 주소와 MAC 주소의 대응 관계 및 그 변화를 감시하는 도구이므로, 제시된 도청 공격의 명칭에 해당하지 않는다.

㉡ SSH: SSH(Secure Shell)는 원격 접속 시 **인증정보와 세션 데이터를 암호화**하여 전송하는 프로토콜이다. 평문 통신을 하는 텔넷 대신 SSH로 원격 접속하면 공격자가 패킷을 수집하더라도 암호화된 통신 내용을 그대로 읽을 수 없다. SSH는 텔넷의 평문 패킷 자체를 암호화하는 부가 기능이 아니라, 암호화된 원격 접속을 제공하는 별도의 프로토콜이다. PGP는 전자우편이나 파일 등의 암호화·전자서명에 사용되며, 이 문항에서 요구하는 원격 접속 프로토콜에 해당하지 않는다.

㉠에 Sniffing, ㉡에 SSH를 연결한 조합은 ③이다.

NoteBase

문 12. 정보보호 시스템들의 로그를 수집하여 분석 및 모니터링을 통해 전사적 차원의 정보시스템 보안성을 향상시키고 안전성을 높이는 시스템은?

① ESM(Enterprise Security Management)

② NAC(Network Access Control)

③ MAM(Mobile Application Management)

④ MDM(Mobile Device Management)

정답 1번

간단한 해설

여러 정보보호 시스템의 로그를 모아 **통합 분석·모니터링**하는 기능은 ESM(전사적 보안관리)에 해당한다. 개별 보안 장비의 정보를 종합하여 조직 전체의 보안 상황을 파악하는 것이 핵심이다.

공통 해설

ESM(Enterprise Security Management)은 여러 정보보호 시스템에서 발생하는 로그와 보안 이벤트를 수집하여 통합적으로 분석·모니터링하는 시스템이다. 로그는 시스템의 동작이나 보안 사건 등을 기록한 정보이며, ESM은 이를 한곳에 모아 **전사적 차원의 보안 상황**을 관리한다.

예를 들어 방화벽과 침입탐지시스템의 이벤트를 함께 분석하면, 장비별 기록을 따로 확인할 때 놓치기 쉬운 연관된 이상 징후를 파악하는 데 도움이 된다. 문항의 '정보보호 시스템들의 로그를 수집'하고 '분석 및 모니터링'한다는 설명은 이러한 ESM의 통합 보안관리 기능에 해당한다.

NoteBase

문 13. 방화벽의 구축 형태 중 베스천 호스트 방식에 대한 설명으로 옳지 않은 것은?

① 외부와 내부 네트워크를 연결해주는 역할을 수행한다.

② 외부에서 내부 네트워크로 접속할 때 원하지 않는 접근은 차단할 수 없다.

③ 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.

④ 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

정답 2번

간단한 해설

베스천 호스트는 사용자 인증과 접근 통제를 통해 **허용되지 않은 외부 접근을 차단할 수 있다**. 따라서 '원하지 않는 접근은 차단할 수 없다'는 설명은 그 기능을 반대로 서술한 것이다.

선지별 해설

① O: 베스천 호스트는 외부에 노출되는 접점에서 공격에 견디도록 보안을 강화한 호스트이다. 내부와 외부 사이의 통신을 **중계하면서 접근을 통제**하므로, 두 네트워크를 연결하는 역할을 수행한다.

② X: 베스천 호스트는 사용자 인증과 접근 통제 정책을 적용하여 외부에서 들어오는 접속의 허용 여부를 판단한다. 따라서 원하지 않는 접근은 **'차단할 수 없다'가 아니라 '차단할 수 있다'**로 고쳐야 한다. 외부와의 통신을 중계하더라도 모든 접근을 허용하는 것은 아니다.

③ O: 로그인 정보로 사용자를 인증하는 경우, 유출된 정보를 이용한 공격자가 정상 사용자로 인증되어 내부 접근 권한을 얻을 수 있다. 이는 **인증 정보가 탈취되면 사용자 인증에 의존한 보호가 무력화된다**는 취약점을 뜻한다.

④ O: 내부 접근을 통제하는 베스천 호스트 자체가 손상되거나 침해되어 통제 기능을 잃으면, 이를 통한 내부 네트워크 보호도 무너진다. 보호의 핵심인 **베스천 호스트 자체의 안전성**이 유지되어야 내부 접근 통제가 제대로 작동한다.

NoteBase

문 14. <보기 1>의 보안 위협과 <보기 2>의 그에 대한 설명을 바르게 연결한 것은?

<보기 1>
ㄱ. 방해(Interruption)
ㄴ. 가로채기(Interception)
ㄷ. 변조(Modification)

<보기 2>
A. 송신측에서 수신측으로 메시지를 전송할 때 제3자가 수신측과 연결할 수 없도록 하는 행위
B. 송신측과 수신측이 메시지를 주고받는 사이에 제3자가 도청하는 행위
C. 송신측에서 수신측으로 메시지를 전송할 때 제3자가 일부 또는 전부를 변경하여 수신측에 전송하는 행위

① ㄱ: A, ㄴ: B, ㄷ: C
② ㄱ: A, ㄴ: C, ㄷ: B
③ ㄱ: B, ㄴ: A, ㄷ: C
④ ㄱ: B, ㄴ: C, ㄷ: A

정답 1번

간단한 해설

가로채기는 메시지를 **몰래 읽는 행위**이고, 변조는 메시지의 **내용을 바꾸는 행위**이다. 도청만 하는 B와 내용을 변경하여 전달하는 C를 구분한다.

NoteBase

대응 관계 해설

ㄱ. 방해(Interruption) → A: 방해는 정상적인 통신이나 서비스 이용을 막는 위협이다. A에서는 제3자가 송신측과 수신측의 연결을 막아 메시지를 전달할 수 없게 하므로, 필요할 때 통신을 이용할 수 있는 **가용성**이 침해된다.

ㄴ. 가로채기(Interception) → B: 가로채기는 권한 없는 제3자가 전송되는 정보에 접근하는 위협이다. B의 도청은 메시지를 변경하는 것이 아니라 그 내용을 몰래 알아내는 행위이므로, 허가된 사람만 정보를 알 수 있도록 하는 **기밀성**이 침해된다.

ㄷ. 변조(Modification) → C: 변조는 권한 없는 제3자가 정보의 내용을 바꾸는 위협이다. C에서는 메시지의 일부 또는 전부를 변경하여 수신측에 전달하므로, 정보가 임의로 변경되지 않도록 하는 **무결성**이 침해된다. 단순히 내용을 엿보는 B와 달리 수신측이 받는 내용 자체가 달라진다.

따라서 ㄱ–A, ㄴ–B, ㄷ–C로 연결되며, ①의 연결과 일치한다.

NoteBase

문 15. HTTPS에 대한 설명으로 옳지 않은 것은?

① HTTPS 연결로 명시되면 포트 번호 443번이 사용되어 SSL을 호출한다.

② HTTPS는 웹 브라우저와 웹 서버 간의 안전한 통신을 구현하기 위한 것이다.

③ HTTPS는 HTTP over TLS 표준 문서에 기술되어 있다.

④ HTTPS 사용 시 요청된 문서의 URL은 암호화할 수 없다.

정답 4번

간단한 해설

HTTPS에서는 요청 메시지가 암호화되므로 **URL의 경로와 질의 문자열도 암호화**된다. 따라서 요청된 문서의 URL은 암호화할 수 없다는 설명은 잘못이다.

선지별 해설

① O: HTTPS의 **기본 포트는 443번**이며, HTTP 메시지를 교환하기 전에 SSL/TLS 보안 연결을 설정한다. 포트를 별도로 지정하면 다른 포트도 사용할 수 있다. 현재는 SSL의 후속 프로토콜인 TLS를 사용한다.

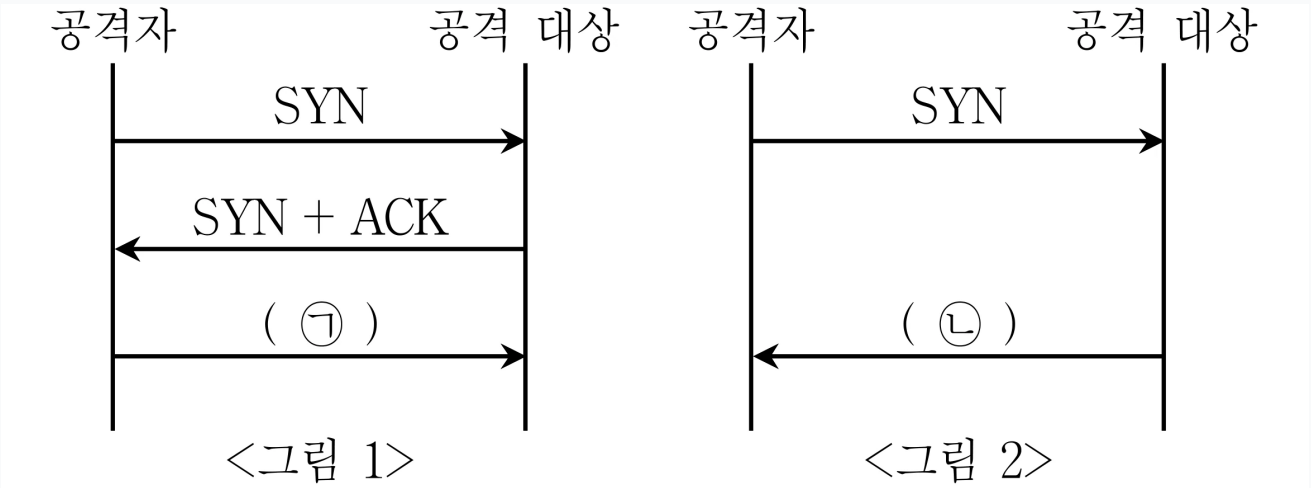
② O: HTTPS는 웹 브라우저와 웹 서버 사이에서 HTTP 통신을 보호한다. 전송 내용을 암호화하여 도청을 막고, **무결성 검증과 서버 인증**을 통해 전송 중 변조와 서버 사칭에 대응한다.

③ O: RFC 2818 'HTTP Over TLS'는 **HTTP를 TLS 위에서 사용하는 방식**을 기술한 문서이다. TLS 연결을 먼저 설정하고, 그 연결을 통해 HTTP 요청과 응답을 주고받는 구조를 설명한다.

④ X: HTTPS에서는 HTTP 요청 전체가 TLS로 보호되므로 **요청 URL의 경로와 질의 문자열도 암호화**된다. 예를 들어 경로가 '/search'이고 질의 문자열이 'q=security'라면, 이 내용은 통신 구간에서 평문으로 전송되지 않는다. 따라서 '암호화할 수 없다'를 '요청 메시지에 포함된 경로와 질의 문자열은 암호화된다'로 고쳐야 한다. 다만 HTTPS가 접속 대상의 IP 주소까지 숨기는 것은 아니므로, URL에 관련된 모든 정보가 감춰진다는 뜻으로 확대해서는 안 된다.

NoteBase

문 16. 다음 그림은 TCP half open 스캔 절차이다. ㉠과 ㉡에 들어갈 패킷을 바르게 연결한 것은?



※ <그림 1>은 공격 대상 서버의 포트가 열린 경우이고, <그림 2>는 공격 대상 서버의 포트가 닫힌 경우임.

① ㉠: ACK, ㉡: ACK

② ㉠: ACK, ㉡: RST

③ ㉠: RST, ㉡: RST + ACK

④ ㉠: RST, ㉡: SYN + ACK

정답 3번

간단한 해설

열린 포트에서 SYN + ACK를 받으면 **RST**를 보내 연결을 완성하지 않는다. 닫힌 포트는 SYN 요청에 **RST + ACK**로 응답하여 연결을 거부한다.

빈칸별 해설

㉠: RST. <그림 1>에서 공격 대상은 SYN을 받은 뒤 SYN + ACK를 공격자에게 보낸다. 이는 해당 포트가 연결 요청을 받아들일 수 있는 열린 상태라는 뜻이다. 일반적인 TCP 연결이라면 공격자가 ACK를 보내 3방향 핸드셰이크를 완성하지만, half open 스캔은 포트의 개방 여부만 확인하므로 **ACK 대신 RST를 보내 연결 시도를 중단**한다. 따라서 공격자에서 공격 대상으로 향하는 마지막 화살표에는 RST가 들어간다.

㉡: RST + ACK. <그림 2>는 공격 대상의 포트가 닫힌 경우이므로, 서버에서 공격자로 향하는 응답은 **연결을 거부하는 RST + ACK**이다. SYN + ACK는 열린 포트의 응답이므로 여기에 들어갈 수 없다. 이때 ACK는 받은 SYN에 대한 확인을 나타내며, RST와 함께 설정되어 있으므로 연결 수락을 뜻하지 않는다.

㉠은 RST, ㉡은 RST + ACK이므로 ③의 조합과 일치한다.

NoteBase

문 18. ARP Spoofing 공격에 대응하기 위한 명령어로 옳은 것은?

① arp -a IP주소 MAC주소

② arp -d IP주소 MAC주소

③ arp -s IP주소 MAC주소

④ arp -v IP주소 MAC주소

정답 3번

간단한 해설

arp -s는 IP주소와 올바른 MAC주소의 대응을 **정적 ARP 항목으로 등록**한다. 이 대응을 고정하면 거짓 ARP 정보로 해당 항목을 바꾸는 ARP Spoofing에 대응할 수 있다.

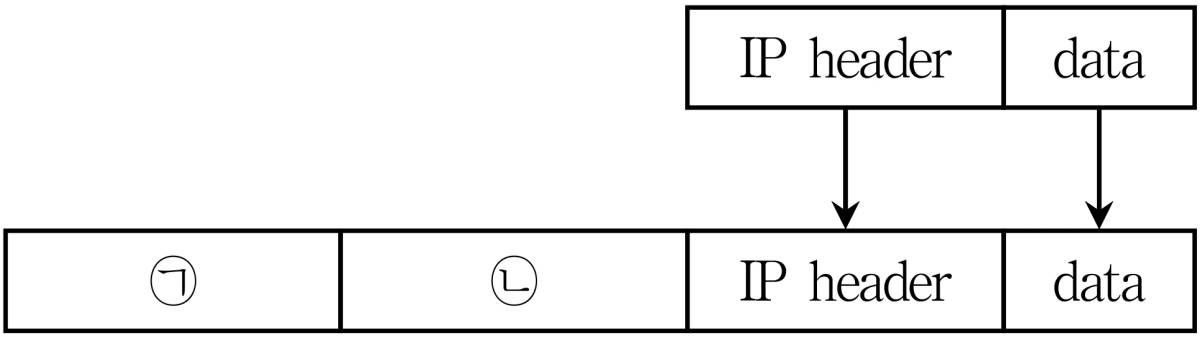
공통 해설

ARP 캐시는 IPv4 주소와 MAC주소의 대응을 저장한다. ARP Spoofing은 거짓 ARP 정보를 보내 이 대응을 공격자의 MAC주소로 바꾸는 공격이다. 따라서 보호할 통신 상대의 정확한 주소 대응을 확인하고, 이를 **정적 ARP 항목으로 고정**하는 것이 대응 방법이다.

arp -s IP주소 MAC주소는 지정한 IP주소와 MAC주소를 정적 항목으로 ARP 캐시에 등록하는 명령이다. 이때 등록할 MAC주소는 **실제 통신 상대의 신뢰할 수 있는 MAC주소**여야 한다. 이렇게 등록한 항목은 동적으로 수신한 거짓 ARP 정보로 변경되지 않으므로 해당 주소에 대한 ARP 캐시 변조를 막는다. 캐시를 조회하거나 기존 항목을 삭제하는 것만으로는 이처럼 주소 대응을 고정할 수 없다.

NoteBase

문 19. 다음은 IPSec 터널모드에서 IP 패킷을 암호화하고 인증 기능을 수행하는 그림이다. ㉠과 ㉡에 추가되는 헤더 정보를 바르게 연결한 것은?



① ㉠: new IP header, ㉡: ESP/AH

② ㉠: ESP/AH, ㉡: new IP header

③ ㉠: IKE header, ㉡: new IP header

④ ㉠: new IP header, ㉡: IKE header

정답 1번

간단한 해설

터널모드는 원래 IP 헤더와 데이터를 통째로 내부 패킷으로 감싸고, 그 앞에 라우팅용 **새 IP 헤더**와 보호 기능을 위한 **ESP/AH 헤더**를 차례로 둔다.

빈칸별 해설

그림의 화살표는 기존 IP header와 data가 새 패킷 안에 함께 포함됨을 나타낸다. 터널모드는 이 원래 IP 패킷 전체를 캡슐화하므로, 기존 IP 헤더 앞에 외부 전송용 헤더와 보안 프로토콜 헤더가 추가된다.

㉠: new IP header이다. 그림에서 가장 바깥쪽에 놓인 **새 IP 헤더**는 터널의 시작점과 끝점 주소를 담아 터널 구간의 라우팅에 사용된다. 원래 송신자와 수신자 주소를 담은 기존 IP 헤더는 내부 패킷에 남는다.

㉡: ESP/AH이다. 새 IP 헤더와 기존 IP 헤더 사이에는 **IPSec 보안 프로토콜 헤더**가 놓인다. ESP는 설정에 따라 암호화에 의한 기밀성과 무결성·데이터 출처 인증을 제공할 수 있다. AH는 무결성·데이터 출처 인증을 제공하지만 암호화 기능은 없다. 따라서 ESP/AH라는 표기를 두 프로토콜 모두 암호화를 수행한다는 뜻으로 해석해서는 안 된다. IKE는 키 교환과 보안 연결(SA)의 설정·관리에 쓰이며, 이 위치에서 원래 데이터 패킷을 보호하는 ESP/AH 헤더를 대신하지 않는다.

따라서 ㉠은 new IP header, ㉡은 ESP/AH이며, 이는 ①의 연결과 일치한다.

NoteBase

문 20. OSI 계층구조와 계층별로 사용되는 보안 프로토콜의 연결이 옳지 않은 것은?

① 네트워크 계층 - IPsec

② 응용 계층 - SSH

③ 데이터링크 계층 - TLS

④ 전송 계층 - SSL

정답 3번

간단한 해설

TLS는 데이터링크 계층의 프레임을 보호하는 프로토콜이 아니라, **TCP 위에서 응용 데이터를 보호**하는 보안 프로토콜이다. 이 문항에서는 SSL과 함께 전송 계층 보안으로 분류한다.

선지별 해설

① O: IPsec은 **IP 계층에서 패킷을 보호**하는 보안 프로토콜 체계이다. 인증과 무결성 보호 등의 보안 서비스를 제공하며, 사용하는 프로토콜과 설정에 따라 암호화도 제공하므로 네트워크 계층과 연결된다.

② O: SSH는 원격 로그인과 명령 실행 등을 안전하게 제공하는 **응용 계층 프로토콜**이다. 일반적으로 TCP 연결을 이용하며, 인증과 암호화를 통해 원격 접속 과정에서 주고받는 데이터를 보호한다.

③ X: TLS는 TCP 같은 신뢰성 있는 전송 프로토콜 위에서 동작하며, 응용 데이터의 기밀성과 무결성을 보호한다. 따라서 '데이터링크 계층 - TLS'는 이 문항의 분류에 따라 **'전송 계층 - TLS'**로 고쳐야 한다. 데이터링크 계층에서 프레임을 직접 보호하는 방식과는 동작 위치가 다르다.

④ O: SSL은 통신 상대의 인증, 암호화, 무결성 보호를 통해 응용 프로그램 사이의 통신을 보호한다. 이 문항에서는 이를 전송 계층 보안 프로토콜로 분류한다. 구체적인 동작 위치는 **TCP 위와 응용 프로토콜 아래**이며, TLS도 이러한 구조를 이어받았다.

NoteBase