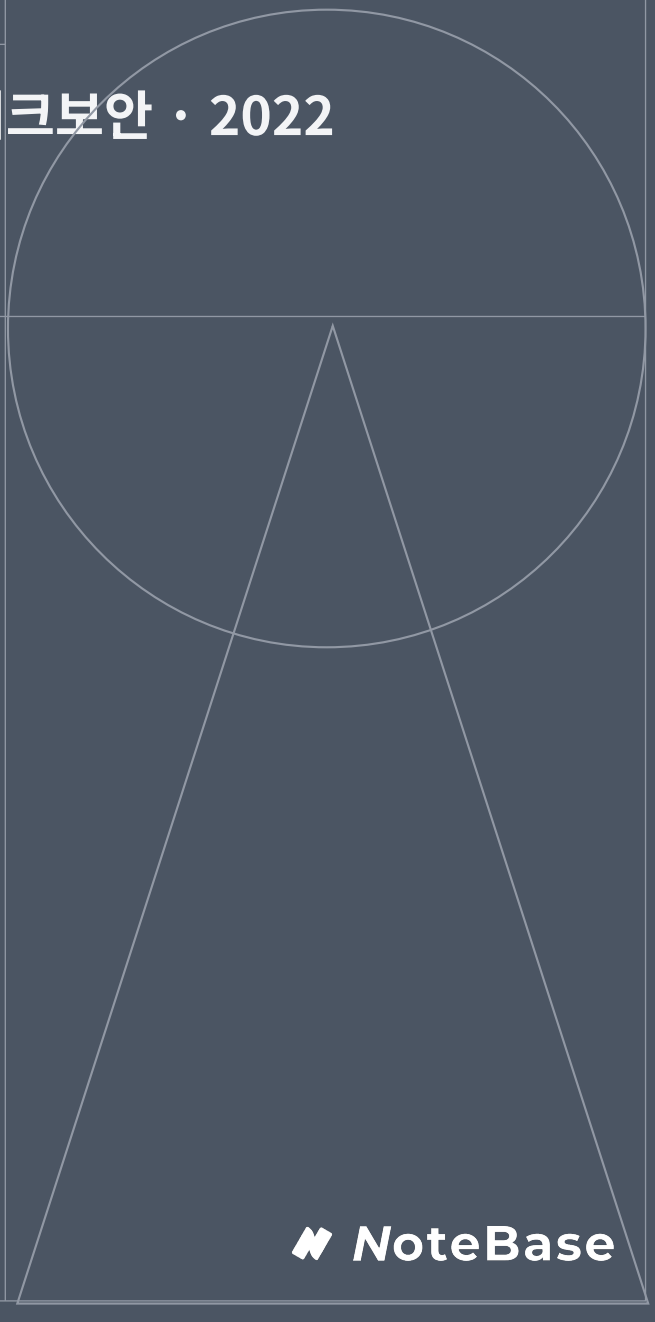
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2022



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2022

공무원/국가직/9급 · 네트워크보안 · 2022

문 1. 네트워크 명령어에 대한 설명으로 옳지 않은 것은?

① hostname: 컴퓨터 이름을 확인한다.

② nslookup: DNS를 통해 도메인 이름을 검색한다.

③ ipconfig: 인터페이스에 설정된 라우팅 테이블을 검색한다.

④ ping: 컴퓨터의 네트워크 상태를 점검한다.

정답 3번

간단한 해설

ipconfig는 **IP 주소·서브넷 마스크·기본 게이트웨이 등 TCP/IP 설정**을 확인하는 명령어이다. 라우팅 테이블은 **route print** 또는 netstat -r로 확인한다.

선지별 해설

① O: hostname은 명령을 실행한 **컴퓨터의 호스트 이름**을 표시한다. IP 주소가 아니라 컴퓨터에 설정된 이름을 확인하는 명령어이다.

② O: nslookup은 **DNS 서버에 질의**하여 도메인 이름에 대응하는 IP 주소 등 DNS 정보를 조회한다. 예를 들어 도메인 이름을 지정하면 그 이름에 등록된 주소를 확인할 수 있다.

③ X: ipconfig는 네트워크 인터페이스의 **IP 주소·서브넷 마스크·기본 게이트웨이 등 TCP/IP 설정**을 표시한다. 라우팅 테이블은 목적지 네트워크별로 사용할 경로를 담은 정보로, Windows에서는 route print 또는 netstat -r로 확인한다. 따라서 ipconfig의 기능을 라우팅 테이블 조회로 설명한 부분이 잘못되었다.

④ O: ping은 대상에 ICMP 에코 요청을 보내고 응답을 확인하여 **IP 통신 가능 여부**를 점검한다. 응답 시간이나 패킷 손실도 확인할 수 있다. 다만 방화벽에서 ICMP를 차단할 수 있으므로 응답이 없다는 사실만으로 대상 컴퓨터의 고장을 단정할 수는 없다.

NoteBase

문 2. 다음에서 설명하는 네트워크 도구는?

◯ IP 헤더에 있는 TTL의 특성을 이용한다.
◯ TTL 값은 IP 패킷이 전송될 수 있는 최대 hop 수이다.
◯ 최종 목적지까지의 라우터에 대한 경로 및 응답속도를 표시해 준다.
◯ 특정 사이트와의 접속이 느릴 경우 네트워크의 어느 구간에서 느린지 확인할 수 있다.

① wireshark
② tcpdump
③ traceroute
④ netstat

정답 3번

간단한 해설

traceroute는 **TTL을 1씩 늘려 탐색 패킷을 보내고**, 경로상의 라우터가 보내는 응답으로 **홉별 경로와 왕복 응답 시간**을 확인하는 도구이다.

공통 해설

traceroute는 목적지까지 패킷이 거치는 라우터의 경로를 추적하는 도구이다. 핵심 원리는 **TTL 만료로 발생하는 ICMP 시간 초과 응답**을 이용해 중간 라우터를 알아내는 것이다. 라우터는 패킷을 전달할 때 TTL을 줄이며, TTL이 0이 되면 패킷을 폐기하고 일반적으로 송신자에게 ICMP 시간 초과 메시지를 보낸다.

traceroute는 TTL을 1, 2, 3 등으로 늘려 가며 탐색 패킷을 보낸다. TTL이 1이면 첫 번째 라우터에서, 2이면 두 번째 라우터에서 만료되므로, 응답한 라우터의 주소를 차례로 확인하여 목적지까지의 경로를 추적할 수 있다. 이처럼 TTL을 조절하여 홉별 응답을 얻는 방식이 지문에서 설명한 도구를 식별하는 기준이다.

함께 표시되는 응답 시간은 탐색 패킷을 보낸 뒤 해당 응답을 받을 때까지의 왕복 시간이다. 이를 홉별로 살펴 지연이 의심되는 위치를 파악하는 데 활용한다. 각 값은 송신자에서 해당 홉까지의 왕복 시간이므로, 이웃한 두 라우터 사이의 전송 시간 자체를 뜻하지는 않는다.

NoteBase

문 3. 비대칭키 암호화 알고리즘에서 수신자의 공개키로 데이터를 암호화하여 전송할 때 얻을 수 있는 보안성은?

① 가용성
② 인증
③ 부인방지
④ 기밀성

정답 4번

간단한 해설

수신자의 공개키로 암호화한 데이터는 대응하는 **수신자의 개인키**로 복호화한다. 개인키를 가진 수신자만 내용을 읽도록 보호하는 성질이 **기밀성**이다.

공통 해설

비대칭키 암호화에서는 서로 대응하는 공개키와 개인키를 사용한다. 송신자가 수신자의 공개키로 데이터를 암호화하면, 수신자는 자신의 개인키로 암호문을 원래 데이터로 복원한다. 안전한 암호화 방식을 사용하고 개인키를 비밀로 유지하면, 제삼자는 전송 중인 암호문을 가로채더라도 내용을 알아내기 어렵다. 이처럼 **허가받지 않은 자에게 정보의 내용이 노출되지 않도록 보호**하는 보안성이 기밀성이다.

이 방식에서 제한되는 것은 데이터를 읽을 수 있는 주체이다. 수신자의 공개키는 누구나 사용할 수 있으므로, 그 공개키로 암호화했다는 사실만으로 송신자의 신원을 인증하거나 송신자가 전송 사실을 부인하지 못하게 하는 부인방지를 보장하지는 않는다. 또한 암호화 자체가 통신이나 서비스의 중단을 막아 가용성을 보장하는 것도 아니다.

NoteBase

문 4. TCP 포트의 개방 여부를 확인하기 위한 스텔스 스캔으로 옳지 않은 것은?

① FIN 스캔

② NULL 스캔

③ XMAS 스캔

④ TCP Open 스캔

정답 4번

간단한 해설

TCP Open 스캔은 **3-way handshake를 완료**하여 실제 TCP 연결을 맺는 방식이다. 연결을 완전히 맺지 않고 응답을 살피는 스텔스 스캔과 달리, 대상 서비스에 연결 기록이 남기 쉽다.

선지별 해설

FIN·NULL·XMAS 스캔은 TCP 연결을 맺지 않고 특정 플래그 조합의 패킷을 보내는 스텔스 스캔이다. 표준에 따른 TCP 동작에서는 닫힌 포트가 RST로 응답하고 열린 포트는 응답하지 않는다. 다만 패킷 필터링으로도 무응답이 발생할 수 있으므로, 무응답만으로 개방을 확정할 수는 없다. 운영체제의 TCP 구현에 따라 응답 동작도 달라질 수 있다.

① O: FIN 스캔은 **FIN 플래그만 설정**한 TCP 패킷을 보낸다. 정상적인 연결 수립 절차를 거치지 않고, 해당 패킷에 대한 응답으로 포트 상태를 추정한다.

② O: NULL 스캔은 **TCP 플래그를 모두 해제**한 패킷을 보낸다. SYN으로 연결을 요청하는 대신 플래그가 없는 패킷에 대한 응답 차이를 이용하므로 스텔스 스캔에 해당한다.

③ O: XMAS 스캔은 **FIN·PSH·URG 플래그를 함께 설정**한 패킷을 보낸다. FIN·NULL 스캔과 보내는 플래그 조합은 다르지만, 연결을 맺지 않고 응답 차이를 이용한다는 원리는 같다.

④ X: TCP Open 스캔은 **TCP 연결을 완전히 수립하는 스캔**으로, 스텔스 스캔에 해당하지 않는다. 열린 포트에 SYN을 보내고 SYN/ACK를 받으면 ACK를 보내 3-way handshake를 완료한다. 실제 연결이 만들어지므로 대상 서비스에 기록이 남기 쉽다. 연결을 완료하지 않는 TCP SYN 스캔은 Half Open 스캔으로 구별한다.

NoteBase

문 5. 스위치 재밍(switch jamming)에 대한 설명으로 옳은 것은?

① 스위치 MAC 테이블의 저장 용량을 넘으면 더미 허브(dummy hub)처럼 브로드캐스트(broadcast) 한다.

② 방어대책은 게이트웨이 MAC 주소를 동적으로 설정한다.

③ 공격자는 클라이언트가 DNS 서버로 전송하는 DNS Query 패킷을 중간에 가로챈다.

④ MAC flooding은 스위치에 이상이 있을 때 자동으로 모든 보안 기능을 차단하는 것이다.

정답 1번

간단한 해설

MAC 테이블이 가짜 주소로 가득 차 정상 주소를 학습하지 못하면, 목적지 포트를 알 수 없는 프레임이 **같은 VLAN의 여러 포트로 플러딩**되어 허브처럼 트래픽이 노출될 수 있다.

선지별 해설

① O: 스위치는 MAC 테이블에 저장된 MAC 주소와 포트의 대응 정보를 이용해 프레임을 전달한다. 테이블이 가득 차 정상 주소를 학습하지 못하면, **목적지 포트를 모르는 유니캐스트 프레임**을 수신 포트를 제외한 같은 VLAN의 포트로 플러딩한다. 선지의 '브로드캐스트'는 이처럼 허브와 같이 여러 포트로 전달하는 현상을 가리킨다. 프레임의 목적지 MAC 주소 자체를 브로드캐스트 주소로 바꾸는 것은 아니다.

② X: 게이트웨이 MAC 주소를 동적으로 설정하는 것은 스위치 재밍의 방어대책이 아니다. 스위치 재밍에는 **포트 보안으로 포트별 학습 가능한 MAC 주소 수를 제한**하여 테이블이 위조 주소로 채워지는 것을 막는다. 게이트웨이 IP 주소와 실제 MAC 주소의 대응을 ARP 테이블에 정적으로 고정하는 것은 ARP 스푸핑에 대한 대응이다.

③ X: DNS 질의를 가로채는 것은 스위치 재밍의 고유한 공격 절차가 아니다. DNS 질의를 가로챈 뒤 **위조 DNS 응답으로 잘못된 IP 주소를 알려 주는 공격**은 DNS 스푸핑에 해당한다. 스위치 재밍은 DNS 질의 자체가 아니라 스위치의 MAC 테이블 용량을 공격한다.

④ X: MAC flooding은 **다수의 위조 출발지 MAC 주소를 가진 프레임으로 MAC 테이블을 채우는 공격**이다. 그 결과 학습되지 않은 목적지로 향하는 트래픽이 플러딩되어 공격자에게 노출될 수 있다. 스위치 이상을 감지해 모든 보안 기능을 자동으로 차단하는 기능을 뜻하지 않는다.

NoteBase

문 6. 윈도 시스템에서 다음과 같이 이더넷 인터페이스의 송수신 패킷 정보를 얻기 위한 netstat 명령어의 옵션은?

인터페이스 통계		
	받음	보냄
바이트	3879974308	172124956
유니캐스트 패킷	1098604	985784
비유니캐스트 패킷	11306144	94056
버림	0	0
오류	0	0
알 수 없는 프로토콜	0	

① netstat -an

② netstat -e

③ netstat -r

④ netstat -s

정답 2번

간단한 해설

그림은 송수신 바이트와 패킷 수를 보여 주는 **이더넷 인터페이스 통계**이다. 이 정보를 표시하는 netstat 옵션은 **-e**이다.

NoteBase

핵심 풀이

그림의 '인터페이스 통계'에는 '받음'과 '보냄' 열이 있고, 바이트·유니캐스트 패킷·비유니캐스트 패킷·버림·오류 등의 항목이 표시되어 있다. 이는 이더넷의 송수신 상태를 집계한 것으로, **netstat -e**로 확인한다. 바이트는 데이터의 양을, 패킷 수는 전송 단위의 개수를 나타낸다.

-s와의 구분: netstat -s는 TCP·UDP·IP·ICMP 등 **프로토콜별 통계**를 표시한다. 통계를 출력한다는 점은 같지만, 문제의 화면은 프로토콜별 항목이 아니라 이더넷 인터페이스의 송수신 항목으로 구성되어 있으므로 -e에 해당한다.

-an과의 구분: netstat -an은 -a와 -n을 함께 지정한 명령이다. -a는 활성 TCP 연결과 수신 대기 중인 TCP·UDP 포트를 표시하고, -n은 주소와 포트 번호를 **숫자 형식**으로 표시한다. 송수신 바이트·패킷 수를 집계하는 옵션은 아니다.

-r과의 구분: netstat -r은 패킷을 어느 경로로 보낼지 판단하는 데 사용하는 **IP 라우팅 테이블**을 표시한다. 인터페이스의 송수신 통계와는 출력 대상이 다르다.

NoteBase

문 7. SSL 프로토콜에 대한 설명으로 옳은 것은?

① ChangeCipherSpec 프로토콜은 오류와 비정상 상태를 알기 위해 사용한다.

② Handshake 프로토콜은 대기와 활성 상태 사이에서 이동되는 값들의 처리 과정을 규정한다.

③ Record 프로토콜은 기밀성과 메시지 무결성을 제공한다.

④ Alert 프로토콜은 암호 그룹 협의와 클라이언트와 서버 간 인증 정보를 교환하기 위해 사용한다.

정답 3번

간단한 해설

Record 프로토콜은 전송 데이터를 **암호화하여 기밀성**을 제공하고, **메시지 인증 코드(MAC)로 무결성**을 확인한다. 암호화는 내용의 노출을 막고, MAC 검증은 전송 중 데이터가 변조되었는지 확인하는 역할을 한다.

선지별 해설

① X: 오류와 비정상 상태를 상대방에게 알리는 것은 **Alert 프로토콜**이다. ChangeCipherSpec 프로토콜은 이후 레코드에 새로 합의한 암호 명세와 키를 적용한다는 사실을 알린다.

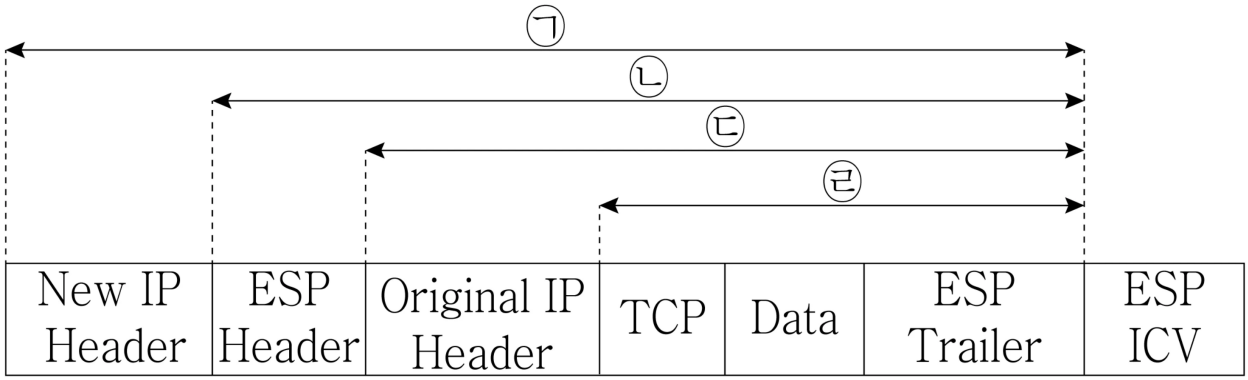
② X: 대기 상태의 보안 매개변수를 현재 활성 상태로 전환하는 것은 **ChangeCipherSpec 프로토콜**의 역할이다. Handshake 프로토콜은 사용할 암호 방식과 키를 협의하고 필요한 인증 정보를 교환한다. 협의한 설정을 준비하는 과정과 실제 통신에 적용하는 상태 전환을 구분해야 한다.

③ O: Record 프로토콜은 상위 계층에서 받은 데이터를 레코드 단위로 처리하고, 합의된 보안 설정에 따라 보호한다. **대칭키 암호화**로 제삼자가 내용을 읽지 못하게 하고, **메시지 인증 코드(MAC)**를 생성·검증하여 메시지의 변조 여부를 확인한다. 이 두 기능이 각각 기밀성과 메시지 무결성에 해당한다.

④ X: 암호 그룹 협의와 클라이언트·서버 간 인증 정보 교환은 **Handshake 프로토콜**의 역할이다. Alert 프로토콜은 오류의 종류와 심각도를 알리고, 연결 종료도 통지한다. 치명적 오류를 알리는 경우에는 연결을 즉시 종료한다.

NoteBase

문 8. IPSec의 ESP 터널 모드에서 암호화 범위로 옳은 것은?



① ㉠

② ㉡

③ ㉢

④ ㉣

정답 3번

간단한 해설

ESP 터널 모드에서는 **원래 IP 헤더를 포함한 내부 IP 패킷과 ESP Trailer**를 암호화한다. 그림의 ㉢처럼 Original IP Header에서 시작하여 ESP Trailer 끝까지이며, 새 IP 헤더·ESP Header·ESP ICV는 제외한다.

선지별 해설

① X: ㉠은 New IP Header부터 ESP Trailer 끝까지로, 새 IP 헤더와 ESP Header까지 포함한다. 새 IP 헤더는 터널 구간의 패킷 전달에 사용되며, 두 헤더 모두 암호화 범위에서 제외하므로 **Original IP Header부터** 시작해야 한다.

② X: ㉡은 ESP Header부터 ESP Trailer 끝까지이다. **ESP Header는 암호화하지 않으므로** 이를 제외하고, 바로 뒤의 Original IP Header부터 암호화해야 한다.

③ O: ㉢은 **Original IP Header·TCP·Data·ESP Trailer**를 포함한다. 터널 모드는 원래 IP 패킷 전체를 ESP 내부에 넣으므로 원래 IP 헤더까지 암호화하며, 패딩·패딩 길이·다음 헤더 정보를 담은 ESP Trailer도 암호화한다. 오른쪽의 ESP ICV는 무결성 검사용 값으로 암호화 범위에 포함되지 않는다.

④ X: ㉣은 TCP부터 ESP Trailer 끝까지여서 **Original IP Header를 빠뜨린다**. 터널 모드에서는 원래 IP 헤더도 내부 IP 패킷의 일부로 암호화하므로, 시작점을 TCP 앞의 Original IP Header까지 넓혀야 한다.

NoteBase

문 9. TLS에 대한 설명으로 옳지 않은 것은?

① TLS는 SSL을 기반으로 만들어진 인터넷 표준이다.

② TLS의 의사난수 함수(pseudorandom function)는 데이터 확장 함수(data-expansion function)를 활용한다.

③ TLS의 의사난수 함수는 비밀(secret), 식별용 라벨(label), 종자(seed)를 입력받는다.

④ TLS의 마스터 비밀(master secret) 생성을 위해 데이터 확장 함수는 사전 마스터 비밀(pre-master secret), ‘master secret’ 문자, 2개의 임의의 수를 입력받는다.

정답 4번

간단한 해설

④에 제시된 입력 구성은 **의사난수 함수(PRF)**에 대한 설명이다. 데이터 확장 함수는 비밀과 확장할 데이터를 입력받으며, PRF는 **라벨과 종자를 연결한 값**을 그 데이터로 전달한다.

선지별 해설

① O: TLS는 **SSL 3.0을 바탕으로 표준화**된 통신 보안 프로토콜이다. 인터넷에서 통신하는 두 주체 사이에 기밀성과 무결성 등을 제공하도록 IETF가 표준화했다.

② O: TLS의 PRF는 내부적으로 **데이터 확장 함수**를 이용한다. 데이터 확장 함수는 비밀과 종자를 바탕으로 HMAC 연산을 반복하고 그 결과를 이어 붙여, 필요한 길이의 출력을 만든다.

③ O: PRF의 입력은 **비밀·식별용 라벨·종자**이다. 비밀은 키 유도의 비밀 재료이고, 라벨은 생성할 값의 용도를 구분하는 문자열이며, 종자는 출력 생성에 함께 사용하는 데이터이다. PRF는 라벨과 종자를 연결한 값을 내부 데이터 확장 함수에 전달한다.

④ X: 사전 마스터 비밀, 'master secret' 라벨, 클라이언트와 서버의 난수를 입력으로 사용하는 함수는 **PRF**이다. 이때 두 난수는 클라이언트 난수 뒤에 서버 난수를 이어 붙여 하나의 종자로 사용하며, PRF 출력의 처음 48바이트가 마스터 비밀이 된다. 내부의 데이터 확장 함수는 **비밀과 확장할 데이터라는 두 입력**을 받는다. 마스터 비밀 생성 시 비밀에는 사전 마스터 비밀을, 데이터에는 'master secret' 라벨과 두 난수를 차례로 연결한 값을 받는다. 따라서 선지의 '데이터 확장 함수'는 '의사난수 함수(PRF)'로 고쳐야 한다.

NoteBase

문 10. 부채널 공격(side channel attack)에 대한 설명으로 옳은 것은?

① 하드웨어적인 공격 기법이며, 전력분석, 시차분석, 전자파분석 등의 공격이 있다.

② 은닉 채널을 이용해 암호화 알고리즘이나 시스템 동작에서 발생하는 다양한 누수 정보를 획득한다.

③ 역어셈블러, 디버거를 이용해 소프트웨어의 오류 및 결함을 찾아 악용하는 공격이다.

④ 숨겨진 메시지를 사진이나 동영상 속에 부호화하는 스테가노그래피는 부채널 공격에 대응하기 위해 개발되었다.

정답 1번

간단한 해설

부채널 공격은 암호 장치가 동작할 때 나타나는 **전력 소비·처리 시간·전자파의 차이**를 분석해 비밀정보를 추정한다. 전력분석, 시차분석, 전자파분석은 이러한 누수 정보를 이용하는 대표적인 기법이다.

선지별 해설

① O: 부채널 공격은 암호 알고리즘을 구현한 장치에서 새어 나오는 정보를 이용한다. 전력분석은 소비 전력의 변화, 시차분석은 연산에 걸리는 시간의 차이, 전자파분석은 장치가 방출하는 전자파를 분석한다. 이처럼 **구현 장치의 물리적 특성**을 이용해 암호키 등의 비밀정보를 추정하므로 하드웨어적인 공격 기법으로 설명한다.

② X: 시스템 동작에서 발생하는 누수 정보를 얻는다는 부분은 부채널 공격의 특징이지만, 이를 '은닉 채널'을 이용한다고 한 부분이 틀리다. 은닉 채널은 협력하는 주체들이 보안정책을 위반하여 정보를 몰래 전달하는 통로이다. 부채널 공격은 이러한 비밀 통신이 아니라 **동작 과정에서 의도치 않게 새어 나오는 정보**를 관찰·분석한다.

③ X: 역어셈블러와 디버거로 프로그램의 구조와 실행 상태를 분석하는 것은 **역공학을 이용한 소프트웨어 분석**이다. 이를 통해 발견한 오류나 결함을 악용할 수 있지만, 그 자체가 부채널 공격의 정의는 아니다. 부채널 공격의 핵심은 코드의 결함을 찾는 것이 아니라 전력·시간·전자파 등의 누수 정보로 비밀정보를 추정하는 데 있다.

④ X: 스테가노그래피는 사진이나 동영상 등 다른 데이터 속에 메시지를 넣어 **메시지의 존재 자체를 숨기는** 기술이다. 부채널 공격에 대응하기 위해 개발된 기술이라는 설명은 틀리다. 메시지의 존재를 감추는 것과 암호 장치의 전력·시간·전자파 누수를 줄이는 것은 서로 다른 과제이다.

NoteBase

문 11. 디지털 포렌식(digital forensic)에서 ‘증거가 위조되거나 변조되지 않았다’는 것을 증명하는 원칙은?

① 무결성
② 신속성
③ 재현성
④ 정당성

정답 1번

간단한 해설

증거가 **위조·변조되지 않고 원래의 내용대로 유지됨**을 보장하는 원칙이 무결성이다.

공통 해설

디지털 포렌식에서 무결성은 디지털 증거가 위조·변조되지 않고 원래의 내용대로 유지되는 것을 뜻한다. 증거의 수집·보관·분석 과정에서 **내용의 동일성을 유지**하는 것이 핵심이다. 예를 들어 확보한 파일의 내용을 분석자가 임의로 수정했다면, 그 파일이 처음 확보한 증거와 같은 내용을 담고 있다고 볼 수 없으므로 무결성이 훼손된다. 문제의 '증거가 위조되거나 변조되지 않았다'는 설명은 이러한 무결성의 원칙에 해당한다.

NoteBase

문 12. 대칭키 암호화 알고리즘으로 옳지 않은 것은?

① ARIA

② SEED

③ DES

④ ECC

정답 4번

간단한 해설

ECC는 공개키와 개인키를 구분하는 **비대칭키 암호 기술**이다. 암호화와 복호화에 같은 비밀키를 사용하는 대칭키 암호로 분류하지 않는다.

선지별 해설

① O: ARIA는 **128비트 블록을 처리하는 대칭키 블록 암호**이다. 키 길이는 128·192·256비트를 지원하며, 암호화와 복호화에 같은 비밀키를 사용한다.

② O: SEED는 **128비트 키와 128비트 블록**을 사용하는 대칭키 블록 암호이다. 송신자와 수신자가 같은 비밀키를 공유하여 데이터를 암호화하고 복호화한다.

③ O: DES는 64비트 블록을 처리하는 대칭키 블록 암호이다. 키는 패리티 비트를 포함하면 64비트이지만, **실제 암호 연산에 사용하는 키 길이는 56비트**이다.

④ X: ECC는 타원곡선의 수학적 성질을 이용하는 **공개키 암호 기술**이다. 공개할 수 있는 공개키와 비밀로 보관하는 개인키를 구분하므로, 같은 비밀키를 공유하는 대칭키 암호가 아니라 비대칭키 암호로 분류해야 한다.

NoteBase

문 13. 네트워크 서비스의 기본 포트 번호로 옳지 않은 것은?

① SMTP(Simple Message Transfer Protocol): 25

② DNS(Domain Name Service): 53

③ RPC(Remote Procedure Call): 111

④ SNMP(Simple Network Management Protocol): 143

정답 4번

간단한 해설

SNMP의 기본 요청·응답 포트는 **UDP 161번**이다. ④의 143번은 전자우편을 조회·관리하는 **IMAP**의 기본 포트이다.

선지별 해설

① O: SMTP는 전자우편을 전송하는 프로토콜로, 메일 서버 사이의 전송에 기본적으로 **TCP 25번** 포트를 사용한다.

② O: DNS는 도메인 이름에 대응하는 IP 주소 등의 정보를 제공하며, 기본 포트는 **53번**이다. 일반적인 질의·응답에는 주로 UDP를 사용하고, 영역 전송 등에는 TCP를 사용한다.

③ O: RPC는 다른 컴퓨터의 프로시저를 호출하는 방식이다. 선지의 111번은 RPC 서비스를 찾는 **포트매퍼(portmapper·rpcbind)**의 기본 포트이며, TCP와 UDP에서 사용한다. 실제 RPC 서비스의 통신 포트는 포트매퍼를 통해 확인한다.

④ X: SNMP는 네트워크 장비의 상태와 관리 정보를 주고받는 프로토콜로, 관리 요청과 응답에는 기본적으로 **UDP 161번** 포트를 사용한다. 선지의 143번은 메일 서버에 보관된 전자우편을 조회·관리하는 IMAP의 기본 TCP 포트이므로, SNMP의 기본 포트는 161번으로 고쳐야 한다.

NoteBase

문 14. 침입탐지시스템(intrusion detection system)에 대한 설명으로 옳지 않은 것은?

① 침입탐지 유형에는 비정상행위 탐지(anomaly detection)와 오용 탐지(misuse detection) 등으로 구분된다.

② 비정상행위 탐지는 알려지지 않은 공격을 탐지하기에 효과적이지만 False Positive가 높아질 수 있다.

③ 오용 탐지는 알려진 공격 패턴을 기반으로 공격을 탐지하므로 알려지지 않은 공격 탐지에는 효과적이지 못하다.

④ 전문가 시스템 모델은 비정상행위 탐지에 널리 사용되는 기법이다.

정답 4번

간단한 해설

전문가 시스템 모델은 알려진 공격 지식을 규칙으로 만들어 적용하는 **오용 탐지**의 대표적인 기법이다.
비정상행위 탐지는 **정상적인 행위에서 벗어나는 정도**를 기준으로 침입을 탐지한다.

선지별 해설

① O: 침입탐지는 탐지 기준에 따라 비정상행위 탐지와 오용 탐지 등으로 구분한다. 비정상행위 탐지는 **정상 행위와의 차이**를, 오용 탐지는 **알려진 공격 패턴과의 일치**를 기준으로 삼는다.

② O: 비정상행위 탐지는 정상적인 사용자·시스템의 행위 특성을 기준으로 삼아, 여기에서 크게 벗어나는 활동을 탐지한다. 따라서 공격 패턴이 미리 알려지지 않았더라도 정상 행위와 차이가 나면 탐지할 수 있다. 다만 정상적인 활동의 변화까지 공격으로 판단할 수 있어 **정상을 공격으로 잘못 판단하는 오탐(False Positive)**이 높아질 수 있다.

③ O: 오용 탐지는 미리 등록한 공격 패턴이나 규칙과 관찰된 활동을 대조한다. 알려진 공격에는 효과적이지만, **등록된 패턴이나 규칙에 포착되지 않는 새로운 공격**은 놓칠 수 있으므로 알려지지 않은 공격 탐지에는 한계가 있다.

④ X: 전문가 시스템 모델은 전문가의 공격 지식을 '조건이 충족되면 공격으로 판단한다'와 같은 규칙으로 지식베이스에 저장하고, 관찰된 활동에 규칙을 적용하여 침입 여부를 추론한다. 알려진 공격 지식을 활용하므로 **오용 탐지의 대표적인 기법**으로 분류한다. 선지의 '비정상행위 탐지'를 '오용 탐지'로 고쳐야 한다. 비정상행위 탐지는 정상 행위의 통계적 특성이나 학습된 모형에서 벗어나는 활동을 찾아내는 방식이다.

NoteBase

문 15. 다음에서 설명하는 서비스 거부(denial of service) 공격은?

◯ ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용해 패킷을 확장함으로써 서비스 거부 공격 수행
◯ 다이렉트 브로드캐스트(direct broadcast) 악용

① 티어드롭 공격(teardrop attack)
② 스머프 공격(smurf attack)
③ 죽음의 핑 공격(ping of death attack)
④ SYN 플러딩 공격(SYN flooding attack)

정답 2번

간단한 해설

ICMP와 브로드캐스트를 이용해 응답 패킷을 증폭시키는 것은 스머프 공격의 특징이다. 피해자의 IP 주소를 출발지로 위조한 요청에 여러 시스템이 응답하면서 피해자에게 트래픽이 집중된다.

공통 해설

스머프 공격(smurf attack)은 네트워크의 여러 시스템을 이용하여 ICMP 응답 트래픽을 증폭시키는 서비스 거부 공격이다. 공격자는 ICMP Echo Request의 **출발지 IP 주소를 피해자의 주소로 위조**하고, 이를 특정 네트워크의 브로드캐스트 주소로 보낸다. 다이렉트 브로드캐스트는 특정 네트워크에 속한 모든 호스트를 대상으로 패킷을 전달하는 방식이다.

해당 브로드캐스트가 전달되고 호스트들이 요청에 응답하면, 여러 호스트의 ICMP Echo Reply가 위조된 출발지인 피해자에게 몰린다. 하나의 요청으로 여러 응답을 유발하므로 피해자의 회선과 처리 자원에 부하를 줄 수 있다. 따라서 지문의 'ICMP 패킷', '네트워크의 시스템을 이용한 패킷 확장', '다이렉트 브로드캐스트 악용'은 이 증폭 구조를 가리키며, 스머프 공격이라는 명칭에 대응한다.

NoteBase

문 16. 공격자가 TCP 세션 하이재킹(session hijacking)을 위해 대상 호스트에 첫 번째로 보내는 TCP 패킷 플래그(flag)는?

① RST

② FIN

③ ACK

④ SYN

정답 1번

간단한 해설

기존 호스트를 먼저 통신에서 배제하는 세션 하이재킹에서는 **RST로 연결을 강제로 초기화**한다. 이를 통해 정상 호스트의 통신을 중단시킨 뒤 공격자가 해당 호스트를 가장한다.

핵심 풀이

TCP 세션 하이재킹은 정상 호스트를 가장하여 이미 성립한 통신을 가로채는 공격이다. 이 문항에서 묻는 것은 정상 호스트를 먼저 통신에서 배제하는 방식으로, 공격자는 상대방이 보낸 것처럼 위조한 RST 패킷을 대상 호스트에 보낸다. 대상 호스트가 이를 유효한 패킷으로 받아들이면 **해당 호스트의 TCP 연결 상태를 즉시 폐기**하므로 정상 통신이 중단된다. RST는 정상 호스트를 배제하는 수단이며, 실제 통신을 이어받으려면 공격자가 그 호스트를 가장해 서버와 통신해야 한다.

FIN은 **송신할 데이터가 더 없음을 알리는 정상 종료**에 사용된다. 수신 측이 FIN을 확인하더라도 반대 방향의 송신은 계속될 수 있으므로, 연결 상태를 즉시 폐기하는 RST와 구별된다.

SYN은 새로운 TCP 연결을 설정할 때 순서번호를 동기화하는 데 사용하고, ACK는 확인응답 번호가 유효함을 나타낸다. 따라서 기존 호스트의 연결을 강제로 초기화하는 역할과 구별된다.

NoteBase

문 17. ICMP에 대한 설명으로 옳은 것은?

① 전송 계층에서의 오류 탐지를 위해 사용한다.

② 송신자의 패킷이 목적지에 도달하지 못했을 때 송신자는 ICMP Echo Reply 메시지를 수신한다.

③ TTL이 0이 되면 ICMP 시간초과(time exceeded) 오류 메시지가 발생한다.

④ UDP에 의해 전송된다.

정답 3번

간단한 해설

패킷을 전달하던 라우터에서 **TTL이 0이 되면 패킷을 폐기**하고, ICMP 시간초과(Time Exceeded) 메시지로 송신자에게 그 원인을 알린다. TTL은 패킷이 네트워크에서 무한히 순환하는 것을 막는 값이다.

선지별 해설

① X: ICMP는 **인터넷 계층에서 IP 패킷 처리 중 발생한 오류를 보고**하고 진단 정보를 전달하는 프로토콜이다. 따라서 '전송 계층에서의 오류 탐지'라는 설명은 계층과 역할을 잘못 연결한 것이다.

② X: Echo Reply는 **Echo Request를 받은 대상이 보내는 응답**이다. 목적지에 도달할 수 없음을 알리는 오류 메시지는 Destination Unreachable이다. 다만 패킷이 도달하지 못했다고 해서 항상 오류 메시지가 송신자에게 돌아오는 것은 아니다.

③ O: 라우터가 패킷을 전달할 때 TTL을 감소시키며, 그 값이 0이 되면 더 이상 전달하지 않고 폐기한다. 이때 송신자에게 원인을 알리는 메시지가 **ICMP 시간초과(Time Exceeded)**이다. 전송 도중 TTL이 만료된 경우에는 Type 11, Code 0을 사용한다.

④ X: ICMP 메시지는 **IP 패킷의 데이터 부분에 직접 실려 전송**된다. UDP에 담아 전송하는 구조가 아니며, IPv4 헤더의 Protocol 필드 값 1이 ICMP를 나타낸다.

NoteBase

문 18. IKE 키 결정 알고리즘의 특징에 대한 설명으로 옳지 않은 것은?

① 방해 공격을 방지하기 위해 비표(nonce)를 사용한다.

② 두 당사자가 군(group)을 협상할 수 있다.

③ Diffie-Hellman 공개키 값의 교환이 가능하다.

④ 중간자 공격을 방지하기 위해 Diffie-Hellman 교환을 인증한다.

정답 1번

간단한 해설

비표(nonce)는 교환마다 새 값을 사용하여 **재전송 공격을 방지**하는 데 쓰인다. 상대에게 불필요한 연산을 반복하게 하는 방해 공격에 대응하는 수단은 **쿠키(cookie)**이다.

선지별 해설

① X: 비표(nonce)는 한 번의 교환에 사용하는 새로운 난수로, 과거의 교환 메시지를 다시 보내는 **재전송 공격을 방지**하고 새 키 재료를 생성하는 데 쓰인다. 방해 공격에 대응하는 수단은 쿠키이다. 쿠키를 먼저 교환하여 위조된 주소의 요청 등으로 고비용 공개키 연산이 반복되는 것을 줄인다. 다만 쿠키가 모든 서비스 거부 공격을 완전히 막는 것은 아니다.

② O: 두 당사자는 Diffie-Hellman 교환에 사용할 **군과 그 매개변수**를 협상할 수 있다. 군은 키 교환의 수학적 연산이 이루어지는 구조이며, 양측이 같은 군의 매개변수를 사용해야 서로 일치하는 공유 비밀값을 계산할 수 있다. 다만 IKEv1의 공격적 모드에서는 메시지 구성상 군 협상이 제한된다.

③ O: IKE에서는 키 교환 메시지에 Diffie-Hellman **공개키 값**을 실어 서로 전달한다. 각 당사자는 받은 상대방의 공개값과 자신의 비밀값으로 같은 공유 비밀값을 계산한다. 공유 비밀값 자체를 네트워크로 보내는 방식은 아니다.

④ O: 인증 없는 Diffie-Hellman 교환만으로는 상대방의 신원을 확인할 수 없어, 공격자가 양측 사이에서 공개값을 바꾸어 각각 별도의 키를 맺는 중간자 공격이 가능하다. IKE는 전자서명이나 사전 공유키 등의 방법으로 **Diffie-Hellman 교환을 인증**하여 이러한 공격을 방지한다.

NoteBase

문 19. IPSec의 보안 연관(security association)을 식별하기 위한 매개변수로 옳지 않은 것은?

① 보안 매개변수 색인(security parameters index)

② 발신지 IP 주소

③ 수신지 IP 주소

④ 보안 프로토콜 식별자(security protocol identifier)

정답 2번

간단한 해설

보안 연관을 식별할 때 쓰는 주소는 발신지가 아니라 **수신지 IP 주소**이다. 보안 연관은 SPI, 수신지 IP 주소, 보안 프로토콜 식별자의 조합으로 식별한다.

선지별 해설

보안 연관(SA)은 한 방향의 통신에 적용할 보안 알고리즘과 키 등의 정보를 공유하는 관계이다. 보안 연관의 식별 기준은 SPI, 수신지 IP 주소, 보안 프로토콜 식별자의 조합이다.

① O: 보안 매개변수 색인(SPI)은 AH 또는 ESP 헤더에 포함되는 색인 값이다. 수신 측은 이 값을 다른 식별 매개변수와 함께 사용하여 **패킷에 적용할 보안 연관**을 찾는다.

② X: 발신지 IP 주소는 보안 연관을 식별하는 세 매개변수에 포함되지 않는다. 식별 조합에 들어가는 주소는 **발신지가 아니라 수신지 IP 주소**이다.

③ O: 수신지 IP 주소는 보안 처리를 수행하는 수신 측을 나타내며, SPI 및 보안 프로토콜 식별자와 함께 보안 연관을 구별한다. 따라서 **수신지 IP 주소**는 식별 매개변수에 해당한다.

④ O: 보안 프로토콜 식별자는 해당 보안 연관이 **AH와 ESP 중 어느 프로토콜을 사용하는지** 구분한다. 하나의 보안 연관은 AH 또는 ESP 중 하나에 연결되므로, 프로토콜의 구분도 식별 기준에 포함된다.

NoteBase

문 20. 다음의 설명에서 옳지 않은 것은?

① 스턱스넷(stuxnet): 사용자가 키보드로 입력하는 내용을 몰래 가로채어 기록한다.

② 랜섬웨어(ransomware): 시스템의 폴더 또는 파일 등을 암호화하여 금전을 요구한다.

③ 트로이 목마(trojan horse): 겉으로는 정상적인 프로그램으로 보이지만 악성코드가 숨겨져 있다.

④ 스파이웨어(spyware): 사용자 정보를 무단으로 수집하여 동의 없이 다른 곳으로 보낸다.

정답 1번

간단한 해설

키보드 입력 내용을 몰래 가로채어 기록하는 것은 **키로거(keylogger)**의 기능이다. 스턱스넷은 **산업 제어 시스템을 공격하는 웜**으로, 제어 프로그램을 변조하여 설비의 정상 작동을 방해한다.

선지별 해설

① X: 사용자의 키보드 입력을 몰래 가로채어 기록하는 것은 **키로거**의 기능이다. 스턱스넷은 산업 제어 시스템을 표적으로 하는 웜으로, 설비의 동작을 제어하는 PLC의 프로그램을 변조하여 정상 작동을 방해한다. 따라서 스턱스넷을 키보드 입력 기록 기능으로 설명한 부분이 잘못되었다.

② O: 랜섬웨어는 파일이나 폴더 등을 암호화하여 사용자가 자료를 이용하지 못하게 하고, **복구를 대가로 금전을 요구**하는 악성코드이다. 자료에 대한 접근을 막고 이를 협박 수단으로 삼는다는 점이 핵심이다.

③ O: 트로이 목마는 **정상적이거나 유용한 프로그램처럼 위장**하지만 내부에 악성 기능을 숨긴 프로그램이다. 사용자가 정상 프로그램으로 믿고 실행하면 숨겨진 악성 기능이 작동한다.

④ O: 스파이웨어는 사용자의 활동이나 개인정보 등을 **동의 없이 수집·전송**하는 악성 소프트웨어이다. 사용자가 모르는 사이 정보를 감시하고 외부로 유출한다는 점에서 설명과 일치한다.

NoteBase