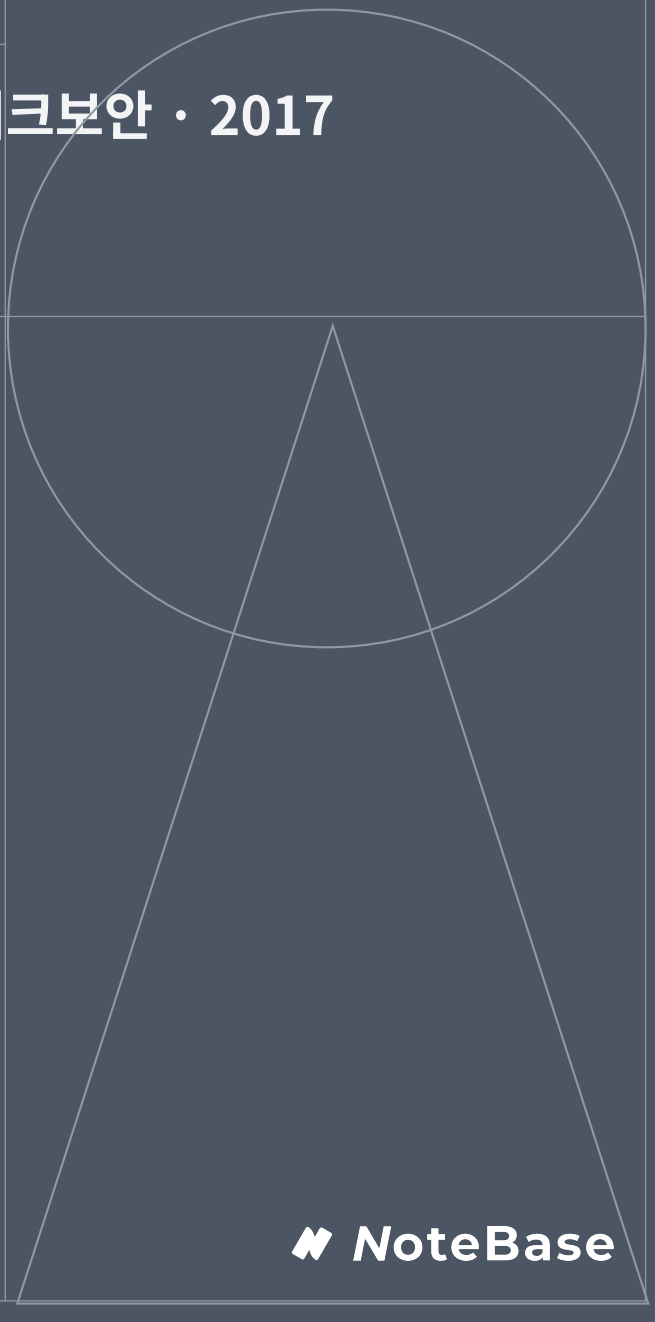
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2017



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2017

공무원/국가직/9급 · 네트워크보안 · 2017

문 1. 네트워크에 연결된 노드가 사용할 IP 주소를 자동으로 할당해주는 프로토콜은?

① DHCP(Dynamic Host Configuration Protocol)

② ICMP(Internet Control Message Protocol)

③ ARP(Address Resolution Protocol)

④ IGMP(Internet Group Management Protocol)

정답 1번

간단한 해설

DHCP는 네트워크에 연결된 장치가 사용할 **IP 주소를 자동으로 할당**하는 프로토콜이다.

공통 해설

DHCP(Dynamic Host Configuration Protocol)는 장치가 통신에 필요한 IP 주소 등의 설정 정보를 서버에서 자동으로 받도록 하는 프로토콜이다. 동적 할당에서는 클라이언트가 주소를 요청하면 서버가 관리하는 주소 풀, 즉 할당할 수 있는 주소의 집합에서 사용 가능한 IP 주소를 정해 일정 기간 사용하도록 임대한다. 따라서 관리자가 각 장치에 IP 주소를 일일이 입력하지 않아도 된다. 발문의 핵심인 **노드가 사용할 IP 주소의 자동 할당**이 DHCP의 기능에 해당한다.

NoteBase

문 2. 공격 유형에 관한 설명으로 옳지 않은 것은?

① 사회공학적 공격은 신뢰 관계나 인간의 심리를 이용하여 중요한 정보를 획득하는 것이다.

② 무차별(brute force) 공격은 특정 값을 찾아내기 위해 가능한 모든 조합을 시도하는 공격이다.

③ 스니핑은 네트워크상에서 다른 사용자들의 트래픽을 도청하는 것이다.

④ 재연(replay) 공격은 두 개체 간의 패킷을 중간에서 가로채서 변조하여 전송함으로써 정당한 사용자로 가장하는 공격이다.

정답 4번

간단한 해설

④의 '패킷을 가로채서 변조하여 전송'하는 방식은 **중간자 공격**의 설명이다. 재연(replay) 공격은 이전에 전송된 유효한 메시지를 획득한 뒤 **다시 전송하여 재사용**하는 공격이다.

선지별 해설

① O: 사회공학적 공격은 **사람의 신뢰나 심리**를 악용하여 비밀번호 등 중요한 정보를 얻는 방식이다. 예를 들어 관리자를 사칭하여 사용자에게 비밀번호를 알려 달라고 요구하는 행위가 이에 해당한다.

② O: 무차별(brute force) 공격은 비밀번호나 암호키 등 목표 값을 찾기 위해 **가능한 후보를 빠짐없이 대입**하는 방식이다. 일부 유력한 후보만 추측하는 것이 아니라 가능한 조합을 체계적으로 시도한다.

③ O: 스니핑은 네트워크를 흐르는 패킷을 수집하여 다른 사용자의 통신 내용을 엿듣는 것이다. 핵심은 **트래픽의 도청**이며, 패킷을 변조하여 상대방에게 전달하는 행위와 구별된다.

④ X: 두 개체 사이에서 패킷을 가로채고 내용을 변조하여 전달하면서 통신 당사자로 가장하는 것은 **중간자 공격**이다. 재연(replay) 공격은 이전의 유효한 메시지를 획득한 뒤 다시 전송하여 인증이나 처리를 부당하게 반복시키는 방식이다. 예를 들어 가로챈 인증 메시지를 나중에 다시 보내 인증을 시도하는 경우이며, 핵심은 메시지의 변조가 아니라 **기존 메시지의 재사용**이다.

NoteBase

문 3. 외부와 내부 네트워크의 경계에서 기본적인 패킷 필터링 기능만을 제공하는 데 적합한 네트워크 보안 구성은?

① 스크리닝 라우터

② 스크린드 호스트 게이트웨이

③ 스크린드 서브넷 게이트웨이

④ 응용레벨 게이트웨이

정답 1번

간단한 해설

스크리닝 라우터는 네트워크 경계에서 IP 주소·포트 번호 등의 정보를 기준으로 **패킷의 통과 여부를 결정**한다. 기본적인 패킷 필터링만 필요한 구성에 적합하다.

공통 해설

패킷 필터링은 패킷 헤더의 출발지·목적지 IP 주소, 프로토콜, TCP·UDP 포트 번호 등을 미리 정한 규칙과 대조하여 통과시키거나 차단하는 기능이다. 이 기능을 가진 라우터를 외부망과 내부망의 경계에 배치한 구성이 **스크리닝 라우터**이다. 예를 들어 특정 출발지 IP 주소에서 들어오는 패킷을 차단하도록 설정할 수 있다.

문제의 핵심 조건은 **기본적인 패킷 필터링만 제공**한다는 점이다. 스크리닝 라우터는 패킷 헤더를 기준으로 접근을 제어하므로 이 조건에 들어맞는다. 응용 서비스의 내용을 해석하는 기능이나 별도 보안 호스트·완충 네트워크를 갖추는 구성까지 요구하는 것은 아니다.

NoteBase

문 4. 스위칭 환경에서의 스니핑 기법이 아닌 것은?

① ICMP 리다이렉트

② 스위치 재밍(jamming)

③ ARP 리다이렉트

④ TCP 세션 하이재킹

정답 4번

간단한 해설

TCP 세션 하이재킹은 이미 맺어진 **TCP 연결을 탈취하여 정상 통신 당사자로 가장**하는 공격이다. 스니핑으로 얻은 정보를 이용할 수는 있지만, 통신 패킷을 수집·도청하는 스니핑 기법 자체와는 구별된다.

선지별 해설

스니핑은 네트워크를 흐르는 패킷을 수집하여 통신 내용을 엿보는 행위이다. 스위치는 일반적으로 목적지 MAC 주소에 해당하는 포트로 유니캐스트 프레임을 전달하므로, 다른 호스트의 통신을 도청하려면 그 트래픽이 공격자의 포트에도 도달하도록 유도해야 한다.

① O: ICMP 리다이렉트는 호스트에 특정 목적지로 가는 다음 경로를 알려 주는 기능이다. 이를 악용하여 위조된 메시지를 호스트가 받아들이게 하면, 패킷이 **공격자를 경유하도록 경로를 변경**하여 도청할 수 있다.

② O: 스위치 재밍은 서로 다른 출발지 MAC 주소를 가진 프레임을 대량으로 보내 스위치의 MAC 주소 테이블을 소진시키는 기법이다. 새 주소를 학습하지 못하면 목적지 주소가 테이블에 없는 프레임이 **같은 VLAN의 다른 포트로 플러딩**될 수 있으므로, 공격자는 자신의 포트에 전달되는 다른 호스트의 트래픽을 수집할 수 있다. 모든 스위치가 무조건 전체 트래픽을 모든 포트로 보내는 것은 아니다.

③ O: ARP 리다이렉트는 위조된 ARP 정보를 이용하여 호스트의 **IP 주소와 MAC 주소의 대응 관계를 변조**하고, 트래픽을 공격자에게 유도하는 기법이다. 예를 들어 게이트웨이 IP 주소에 공격자의 MAC 주소가 대응되도록 하면, 게이트웨이로 가야 할 프레임을 공격자가 받아 도청한 뒤 실제 게이트웨이로 전달할 수 있다.

④ X: TCP 세션 하이재킹은 기존 TCP 연결의 순서 번호 등 연결 정보를 이용하여 정상 통신 당사자를 가장하고, 위조한 TCP 세그먼트를 끼워 넣어 **연결을 탈취하는 공격**이다. 스니핑은 패킷을 수집·도청하는 것이므로, TCP 세션 하이재킹 자체를 스위칭 환경의 스니핑 기법으로 분류할 수 없다. 스니핑이 세션 탈취에 필요한 정보를 얻는 수단으로 이용될 수 있다는 점과 구별해야 한다.

NoteBase

문 5. 다음의 ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

무선 랜에서의 프라이버시 강화를 위하여 IEEE 802.11에서 (㉠)를 정의하였으나, 이 표준에서 무결성 보장과 키 사용의 심각한 약점이 발견되었다. (㉡)에서 이를 개선할 목적으로 IEEE 802.11i의 초안에 기초한 중간 조치로 (㉢)를 공표하였고, 이후 IEEE 802.11i 전체 표준을 따르는 새로운 보안 대책이 등장하게 되었다.

① ㉠: WPA, ㉡: Wi-Fi Alliance, ㉢: WPA2

② ㉠: WPA, ㉡: IETF, ㉢: WPA2

③ ㉠: WEP, ㉡: Wi-Fi Alliance, ㉢: WPA

④ ㉠: WEP, ㉡: IETF, ㉢: WPA

정답 3번

간단한 해설

WEP의 취약점을 보완하기 위해 Wi-Fi Alliance가 마련한 것이 **WPA**이다. WPA는 IEEE 802.11i의 **초안에 기초한 중간 조치**이며, 전체 표준을 따르는 WPA2와 구별된다.

빈칸별 해설

㉠ WEP: IEEE 802.11에서 유선 랜에 준하는 프라이버시를 제공하려고 도입한 보안 방식이다. 그러나 무결성 검사에 사용하는 CRC-32는 우발적인 오류 검출용이므로 **공격자의 의도적인 변조를 막기에 부적합**하다. 또한 짧은 초기화 벡터가 반복되면 같은 키 스트림이 재사용될 수 있어 암호화에도 취약점이 생긴다.

㉡ Wi-Fi Alliance: 무선 랜 제품의 상호운용성을 인증하는 산업계 단체로, WEP의 문제에 대응하기 위해 WPA를 공표했다. IEEE는 IEEE 802.11i 표준을 제정하는 기관이며, 이 문장에서 묻는 **WPA의 공표 주체는 Wi-Fi Alliance**이다.

㉢ WPA: IEEE 802.11i가 완성되기 전에 그 초안의 일부를 바탕으로 마련한 보안 대책이다. 기존 장비에서도 보안을 개선할 수 있도록 TKIP를 활용해 키 사용과 무결성 보호를 보완했다. 지문의 마지막에 나오는 IEEE 802.11i 전체 표준에 대응하는 것은 **WPA2**이므로, 중간 조치를 뜻하는 빈칸에는 WPA가 들어간다.

㉠ WEP, ㉡ Wi-Fi Alliance, ㉢ WPA의 연결은 ③과 일치한다.

NoteBase

문 6. 거리 벡터가 아닌 링크 상태를 활용하는 자율시스템(autonomous system) 도메인 내의 라우팅 프로토콜은?

① RIP(Routing Information Protocol)

② OSPF(Open Shortest Path First)

③ BGP(Border Gateway Protocol)

④ IGRP(Interior Gateway Routing Protocol)

정답 2번

간단한 해설

OSPF는 **자율시스템 내부**에서 사용하는 **링크 상태 라우팅 프로토콜**이다. 링크의 연결 관계와 비용 정보를 바탕으로 최단 경로를 구한다.

공통 해설

OSPF(Open Shortest Path First)는 하나의 자율시스템 내부에서 경로 정보를 교환하는 내부 라우팅 프로토콜이다. 경로를 결정할 때 **링크 상태 방식**을 사용하므로, 문제의 두 조건인 자율시스템 내부에서의 사용과 링크 상태 활용에 모두 해당한다.

링크 상태 방식에서는 라우터 사이의 연결 관계와 링크 비용을 알리는 정보를 교환하여 네트워크의 연결 구조를 파악한다. OSPF는 이 정보로 구성한 링크 상태 데이터베이스를 바탕으로 자신을 출발점으로 하는 최단 경로 트리를 만들고 라우팅 테이블을 구성한다. 이웃이 알려 준 목적지까지의 거리 정보를 바탕으로 경로를 갱신하는 거리 벡터 방식과 달리, **연결 구조를 바탕으로 직접 최단 경로를 계산**한다는 점이 핵심이다.

NoteBase

문 7. SSL(Secure Socket Layer)에서 서버와 클라이언트 간의 인증과 키 교환 메시지를 주고받는 프로토콜은?

① Record

② Handshake

③ Change Cipher Spec

④ Alert

정답 2번

간단한 해설

SSL에서 **Handshake**는 서버와 클라이언트가 통신에 사용할 보안 조건을 협상하고, 인증과 키 교환에 필요한 메시지를 주고받는 프로토콜이다.

공통 해설

Handshake는 SSL 통신에 사용할 암호 알고리즘 등을 협상하고, 통신 상대를 인증하며 암호화에 필요한 키를 마련하는 절차를 담당한다. 인증서와 키 교환 관련 메시지는 이 절차에서 교환된다. 다만 **클라이언트 인증은 선택적**이므로 모든 연결에서 반드시 양방향 인증을 하는 것은 아니다.

발문의 구별 기준은 메시지를 운반하는 기능이 아니라 **인증과 키 교환 절차를 담당하는 기능**이다. Handshake 메시지도 Record에 실려 전달되지만, 인증·키 교환 메시지의 내용과 교환 절차를 정하는 프로토콜은 Handshake이다.

NoteBase

문 8. 클라이언트가 위조된 웹사이트에 접속하게 하는 것을 목적으로 하는 공격 기법은?

① DNS 스푸핑

② ARP 스푸핑

③ 스니핑

④ SYN flooding

정답 1번

간단한 해설

DNS 스푸핑은 **도메인 이름에 대응하는 IP 주소를 속여** 클라이언트가 공격자의 위조 웹사이트로 접속하도록 유도한다.

공통 해설

DNS는 도메인 이름에 대응하는 IP 주소를 알려 주어 클라이언트가 접속할 서버를 찾게 한다. DNS 스푸핑은 이 이름 해석 과정에서 **정상 서버의 IP 주소 대신 공격자가 지정한 IP 주소**를 알려 주도록 DNS 응답이나 저장된 DNS 정보를 위조하는 공격이다. 클라이언트가 위조된 정보를 신뢰하면 정상 웹사이트의 도메인 이름을 입력해도 위조 웹사이트 쪽으로 접속을 시도하게 된다. 따라서 문제의 '위조된 웹사이트에 접속하게 하는 것'은 DNS의 이름과 주소 사이의 대응을 속이는 방식과 연결된다.

NoteBase

문 9. 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로, TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용되는 것은?

① ping

② netstat

③ nmap

④ nbtstat

정답 3번

간단한 해설

호스트를 찾고 서비스·운영체제를 탐지하며 **TCP Xmas 스캔을 지원하는** 네트워크 탐색 도구는 **nmap**이다.

공통 해설

nmap(Network Mapper)은 고든 라이언(Gordon Lyon)이 개발한 네트워크 탐색·보안 점검 도구이다. 대상에 탐색 패킷을 보내고 응답을 분석하여 **호스트의 존재, 포트 상태, 서비스와 운영체제 정보**를 조사한다. 문제는 이러한 탐색 기능을 갖춘 도구의 명칭을 묻는다.

TCP Xmas 스캔은 **FIN·PSH·URG 플래그를 설정한 TCP 패킷**을 보내 반응을 살피는 포트 스캔 방식이다. 정상적인 TCP 연결을 완성하지 않고 포트 상태를 조사하며, nmap은 이를 -sX 옵션으로 지원한다. 따라서 호스트·서비스·운영체제 탐지와 Xmas 스캔이라는 단서가 nmap의 기능에 함께 대응한다.

NoteBase

문 10. 유닉스 시스템의 'traceroute'가 발신지에서 목적지까지의 패킷 전달 경로를 추적하는 과정에서 사용하지 않는 것은?

① ICMP

② TCP

③ UDP

④ IP 패킷의 TTL(Time To Live) 필드

정답 2번

간단한 해설

유닉스 traceroute의 전통적인 기본 방식은 **UDP 탐사 패킷과 ICMP 응답**을 이용한다. IP 패킷의 TTL을 단계적으로 늘려 경로를 알아내며, 이 기본 방식에서는 **TCP를 사용하지 않는다**.

공통 해설

유닉스 traceroute의 전통적인 기본 방식은 **UDP 패킷의 IP 헤더에 있는 TTL을 1부터 차례로 늘려** 보내는 것이다. TTL은 패킷이 라우터를 거칠 때 감소하며, 소진되면 해당 라우터가 패킷을 폐기하고 발신지에 ICMP Time Exceeded 메시지를 보낸다. TTL이 1인 탐사로 첫 번째 라우터를, 2인 탐사로 두 번째 라우터를 확인하는 식으로 응답한 라우터의 주소를 모아 경로를 파악한다.

탐사 패킷은 목적지에서 사용하지 않을 것으로 예상되는 UDP 포트로 보낸다. 패킷이 목적지에 도달했을 때 그 포트가 열려 있지 않으면, 목적지는 ICMP Port Unreachable 메시지를 반환한다. 이 응답으로 목적지에 도달했음을 확인한다. 따라서 UDP는 탐사 패킷 전송에, ICMP는 중간 라우터와 목적지의 응답에, TTL 필드는 탐사 범위를 한 홉씩 늘리는 데 사용된다.

TCP는 이 기본 방식의 탐사에 사용되지 않는다. 다만 일부 traceroute 구현은 별도 옵션으로 TCP 탐사를 지원하므로, TCP를 어떤 traceroute에서도 사용할 수 없다는 뜻은 아니다.

NoteBase

문 11. DMZ(demilitarized zone) 네트워크내에 일반적으로 두지 않는 것은?

① 웹 서버

② 이메일 서버

③ DNS 서버

④ 내부 접속용 데이터베이스 서버

정답 4번

간단한 해설

DMZ는 외부에 공개할 서버를 내부망과 분리해 두는 영역이다. **내부 접속용 데이터베이스 서버**는 외부 공개가 필요하지 않으므로 일반적으로 보호된 **내부망**에 둔다.

공통 해설

DMZ는 외부망과 내부망 사이에서 방화벽 등으로 접근을 통제하는 별도의 네트워크 영역이다. **외부에 제공해야 하는 서비스인지**가 서버 배치의 기준이다. 외부 공개 서버를 내부망에서 분리하면 해당 서버가 침해되더라도 내부 시스템으로 공격이 확산될 위험을 줄일 수 있다.

외부 이용자에게 서비스를 제공하는 웹 서버·이메일 서버·DNS 서버는 일반적으로 DMZ에 배치할 수 있다. 반면 내부 접속용 데이터베이스 서버는 내부 업무용 데이터를 보관하고 내부의 허가된 시스템에 서비스를 제공하므로, 일반적으로 **DMZ가 아닌 내부망**에 배치한다. DMZ의 서버가 내부 데이터베이스를 이용해야 할 때에도 방화벽으로 필요한 통신만 허용한다.

NoteBase

문 12. 다음 설명에 해당하는 네트워크 장비가 바르게 연결된 것은?

(가) 두 개 이상의 LAN을 하나로 연결하는 장치
(나) 여러 대의 컴퓨터를 손쉽게 연결할 수 있도록 여러 개의 입력과 출력 포트를 가지고 있으며, 한 포트에서 수신된 신호를 다른 모든 포트로 재전송하는 장치
(다) 이종 통신망 간에도 프로토콜을 변환하여 정보를 주고받을 수 있는 장치
(라) 패킷의 수신 주소를 토대로 경로를 정해서 패킷을 전송함으로써 둘 이상의 네트워크를 연결하는 장치

① (가): 브리지, (나): 허브, (다): 라우터, (라): 게이트웨이
② (가): 브리지, (나): 허브, (다): 게이트웨이, (라): 라우터
③ (가): 허브, (나): 브리지, (다): 게이트웨이, (라): 라우터
④ (가): 허브, (나): 브리지, (다): 라우터, (라): 게이트웨이

정답 2번

간단한 해설

서로 다른 통신 규약을 쓰는 망 사이에서 **프로토콜을 변환**하는 장비는 게이트웨이이다. 라우터는 패킷의 **목적지 주소를 바탕으로 경로를 선택**하여 다른 네트워크로 전달한다.

대응 관계 해설

(가) 브리지: 둘 이상의 LAN 또는 LAN 세그먼트를 연결하는 장비이다. 데이터 링크 계층에서 프레임의 **목적지 MAC 주소**를 확인하여 다른 세그먼트로 전달할지 판단한다. 단순히 신호를 모든 포트로 재전송하는 허브와 구별된다.

(나) 허브: 여러 컴퓨터를 연결하는 다중 포트 장비로, 물리 계층에서 동작한다. 한 포트로 들어온 신호를 **수신 포트를 제외한 다른 모든 포트로 재전송**하며, 목적지 주소를 분석하여 전달 포트를 고르지 않는다.

(다) 게이트웨이: 서로 다른 통신망 사이에서 **프로토콜을 변환**하여 정보를 주고받게 하는 장비이다. 이 문항에서는 단순한 망 연결보다 서로 다른 통신 규약을 맞추어 준다는 기능이 결정적인 구별 기준이다.

(라) 라우터: 네트워크 계층에서 패킷의 목적지 IP 주소와 라우팅 정보를 이용하여 전달 경로를 선택한다. **목적지 네트워크로 향하는 경로에 따라 패킷을 전달**하므로 둘 이상의 네트워크를 연결할 수 있다.

(가) 브리지, (나) 허브, (다) 게이트웨이, (라) 라우터의 대응이므로 ②의 연결과 일치한다.

NoteBase

문 13. IPv4의 주소 부족 현상을 해결하기 위한 접근 방법이 아닌 것은?

① NAT

② SNMP

③ IPv6

④ DHCP

정답 2번

간단한 해설

SNMP는 네트워크 장비의 상태를 수집하고 제어하는 **네트워크 관리 프로토콜**이다. 주소를 공유·재사용하거나 주소 공간을 확장하는 기능이 아니므로 IPv4 주소 부족을 해결하는 방법에 해당하지 않는다.

선지별 해설

① O: NAT는 내부의 사설 IP 주소를 외부 통신에 사용할 공인 IP 주소로 변환한다. 특히 포트 번호까지 변환하는 NAPT 방식은 여러 내부 호스트가 **하나의 공인 IP 주소를 공유**하여 통신하게 하므로 공인 IPv4 주소의 수요를 줄인다.

② X: SNMP는 라우터·스위치 등 네트워크 장비의 관리 정보를 조회하거나 설정하고, 장비의 상태를 감시하는 프로토콜이다. 그 역할은 **네트워크 관리**이며, 주소 공유·재사용이나 주소 공간 확장을 통한 IPv4 주소 부족 해결 방법에는 해당하지 않는다.

③ O: IPv6는 IP 주소 길이를 IPv4의 32비트에서 **128비트로 확장**하여 훨씬 많은 장치에 주소를 부여할 수 있게 한다. 기존 IPv4 주소 자체를 늘리는 것이 아니라 더 큰 주소 공간을 갖는 체계로 전환하여 주소 부족에 대응한다.

④ O: DHCP의 동적 할당은 IP 주소를 일정한 임대 기간 동안 제공하고, 더 이상 사용하지 않아 반환되거나 임대가 만료된 주소를 다른 클라이언트에게 다시 할당할 수 있게 한다. 이렇게 **제한된 주소 풀을 재사용**하여 주소 낭비를 줄인다. 주소 공간 자체를 확장하지는 않지만 주소 부족을 완화하는 방법이다.

NoteBase

문 14. 패킷 재조합의 문제를 악용하여 오프셋이나 순서가 조작된 일련의 패킷 조각들을 보냄으로써 자원을 고갈시키는 서비스 거부(DoS) 공격은?

① Land
② Teardrop
③ SYN flooding
④ Smurf

정답 2번

간단한 해설

Teardrop은 **IP 패킷 조각의 오프셋을 조작**하여 재조합 과정의 취약점을 악용하는 공격이다. 조각들이 차지하는 범위가 겹치도록 만들어 수신 시스템의 정상적인 처리를 방해한다.

공통 해설

IP 패킷이 여러 조각으로 나뉘어 전송되면 수신 측은 이를 원래 패킷으로 재조합한다. 이때 오프셋은 각 조각의 데이터가 원래 패킷의 어느 위치에 놓이는지를 나타낸다. **Teardrop은 조각의 오프셋과 길이를 악의적으로 구성**하여 데이터 범위가 서로 겹치는 등 비정상적인 조각들을 보내고, 이를 처리하는 재조합 기능의 취약점을 악용하는 DoS 공격이다. 취약한 시스템은 재조합 과정에서 오류가 발생하거나 동작이 중단될 수 있다.

문제의 핵심 단서는 **조작된 패킷 조각과 패킷 재조합의 문제**이다. 공격이 겨냥하는 지점이 조각을 원래 패킷으로 복원하는 처리 과정이므로, 제시된 공격은 Teardrop에 해당한다.

NoteBase

문 15. IEEE 802.11i RSN(Robust Security Network) 동작 단계에 대한 설명으로 옳지 않은 것은?

① 발견 단계에서는 STA(Station)와 AP(Access Point)가 서로를 인지하여 일련의 보안 능력에 합의하고, 해당 보안 능력을 이용하여 향후 통신에 사용할 연관을 설정한다.

② 인증 단계에서는 STA와 AS(Authentication Server)간의 상호 인증을 위하여 EAP(Extensible Authentication Protocol)를 교환한다.

③ 키 관리 단계에서는 STA와 AP간에 사용되는 한 쌍의 쌍별 키와 멀티캐스팅 통신에 사용되는 그룹 키가 정의된다.

④ 보호 데이터 전송 단계에서는 CRC(Cyclic Redundancy Check)로 메시지 인증과 데이터 기밀성을 제공한다.

정답 4번

간단한 해설

CRC는 전송 중 발생한 **오류를 검출**하는 방식이며, 메시지 인증이나 데이터 기밀성을 제공하지 않는다.
RSN에서는 **CCMP 같은 보안 프로토콜**로 데이터를 보호한다.

선지별 해설

① O: 발견 단계에서는 무선 단말인 STA가 AP를 찾고, 서로 지원하는 인증 방식과 데이터 보호 방식 등 **보안 능력을 협의**하여 연관을 설정한다. 이때 정한 보안 방식은 이후 인증과 보호 데이터 전송의 기준이 된다.

② O: 인증 서버를 이용하는 방식에서는 STA와 AS가 **EAP를 이용하여 상호 인증**한다. AP는 두 주체 사이에서 인증 메시지를 중계하며, 실제 인증은 선택한 EAP 방식에 따라 이루어진다.

③ O: 키 관리 단계에서는 STA와 AP 사이의 개별 통신을 보호할 **쌍별 키**를 도출하고, 멀티캐스트·브로드캐스트 통신을 보호할 **그룹 키**를 배포한다. 개별 단말과의 통신에는 해당 단말과 AP의 키를, 여러 단말에 함께 보내는 통신에는 그룹 키를 사용한다.

④ X: CRC는 우발적인 전송 오류를 검출하는 값으로, 비밀키 없이 계산할 수 있어 공격자가 데이터를 바꾸고 CRC도 다시 계산할 수 있다. 따라서 **메시지 인증과 기밀성을 제공하지 않는다**. 보호 데이터 전송에는 협의된 보안 프로토콜과 설정된 키를 사용하며, AES 기반 CCMP의 경우 CTR 방식으로 기밀성을, CBC-MAC으로 메시지 인증과 무결성을 제공한다.

NoteBase

문 16. 128.23.16.0/20이 시작 주소인 IP 주소 블록을 동일한 크기의 8개 주소 블록으로 나눌 경우 얻어지는 서브넷의 시작 주소로 옳은 것은?

① 128.23.0.0/23

② 128.23.2.0/23

③ 128.23.20.0/23

④ 128.23.32.0/23

정답 3번

간단한 해설

8개로 균등 분할하려면 네트워크부를 3비트 늘려 **/23**으로 만든다. 각 블록은 주소 512개를 포함하므로 세 번째 옥텟이 16부터 **2씩 증가**하며, 128.23.20.0/23도 그중 하나이다.

계산 과정

원래 블록의 범위: IPv4 주소는 32비트이고 /20은 앞의 20비트가 네트워크부라는 뜻이다. 128.23.16.0/20의 주소 범위는 **128.23.16.0~128.23.31.255**이다. 분할한 서브넷은 모두 이 범위 안에 있어야 한다.

분할 후 접두사 길이: 호스트부에서 3비트를 서브넷 구분에 사용하면 $2^3 = 8$개의 동일한 크기 블록이 생긴다. 따라서 네트워크부 길이는 20 + 3 = 23비트가 되어 각 서브넷의 접두사는 **/23**이다.

서브넷 크기와 간격: /23에서 남는 호스트부는 32 - 23 = 9비트이므로 서브넷마다 $2^9 = 512$개의 주소가 있다. 네 번째 옥텟은 0~255의 256개 값을 가지므로, 주소 512개는 세 번째 옥텟의 값 두 개에 해당한다. 따라서 시작 주소는 네 번째 옥텟이 0인 상태에서 **세 번째 옥텟이 2씩 증가**한다.

시작 주소와 선택지 대응: 세 번째 옥텟은 16, 18, 20, 22, 24, 26, 28, 30이 된다. 이 중 20을 사용하는 **128.23.20.0/23**이 ③에 해당한다. ①과 ②는 원래 블록의 시작 주소보다 앞에 있고, ④는 원래 블록의 끝 주소를 벗어난다.

NoteBase

문 17. 윈도우즈 시스템에서 “route PRINT -4” 명령을 실행한 결과로 표현되는 정보가 아닌 것은?

① 네트워크 마스크

② 게이트웨이

③ TCP/UDP 포트

④ 인터페이스

정답 3번

간단한 해설

route PRINT -4는 **IPv4 라우팅 테이블**을 표시한다. TCP/UDP 포트는 응용 프로그램의 통신을 구분하는 전송 계층 정보이므로 이 출력에 포함되지 않는다.

공통 해설

route PRINT -4에서 PRINT는 라우팅 테이블을 출력하고, -4는 IPv4 경로를 대상으로 지정한다. 라우팅 테이블은 **목적지 IP 주소에 따라 패킷을 어떤 경로로 보낼지** 결정하는 데 쓰인다. 목적지 네트워크와 네트워크 마스크는 경로가 적용되는 주소 범위를 나타내며, 게이트웨이는 다음에 전달할 라우터를, 인터페이스는 패킷을 내보낼 로컬 네트워크 접점을 나타낸다. 따라서 네트워크 마스크·게이트웨이·인터페이스는 출력에 포함되는 경로 정보이다.

TCP/UDP 포트는 **호스트 내부의 응용 프로세스나 서비스를 구분**하는 전송 계층 정보이다. 목적지 네트워크로 가는 경로를 나타내는 항목이 아니므로 route PRINT -4에는 표시되지 않으며, 포트 사용 정보는 netstat 같은 명령으로 확인한다.

NoteBase

문 18. UDP(User Datagram Protocol)의 헤더 포맷에 포함되어 있는 필드는?

① 시퀀스 번호(sequence number)

② 목적지 IP 주소(destination IP address)

③ 체크섬(checksum)

④ 헤더 길이(header length)

정답 3번

간단한 해설

UDP 헤더에는 전송 중 발생한 오류를 검출하기 위한 **체크섬** 필드가 포함된다.

공통 해설

UDP 헤더는 **출발지 포트, 목적지 포트, 길이, 체크섬**의 네 필드로 구성된다. 각 필드는 16비트이며, 헤더 크기는 8바이트로 고정된다. 체크섬은 UDP 헤더와 데이터의 오류를 검출하는 데 사용된다. 여기서 길이 필드는 헤더 길이만이 아니라 **UDP 헤더와 데이터의 전체 길이**를 바이트 단위로 나타낸다.

NoteBase

문 19. IPsec에 대한 설명으로 옳지 않은 것은?

① 전송모드에서 AH(Authentication Header)는 IP 페이로드와 IP 헤더의 선택된 부분을 인증한다.

② 전송모드에서 ESP(Encapsulating Security Payload)는 IP 헤더는 암호화하지 않고 IP 페이로드를 암호화한다.

③ 터널모드에서는 패킷 암호화를 지원하는 ESP와 인증을 제공하는 AH가 같이 사용되어야 한다.

④ IKE(Internet Key Exchange) 프로토콜을 사용하여 보안 연관(Security Association)을 설정한다.

정답 3번

간단한 해설

터널모드는 원래 IP 패킷을 새 IP 패킷 안에 넣는 방식이며, **ESP와 AH를 반드시 함께 사용해야 하는 것은 아니다**. ESP는 자체적으로 암호화와 인증·무결성 보호를 함께 제공할 수 있다.

선지별 해설

① O: AH는 데이터의 출처 인증과 무결성 보호를 제공한다. 전송모드에서는 IP 페이로드와 함께 **IP 헤더 중 인증 가능한 필드**도 보호한다. 다만 TTL처럼 전송 도중 바뀌고 수신 시의 값을 미리 알 수 없는 필드는 그 실제 값을 인증 대상으로 삼지 않으므로, IP 헤더 전체를 그대로 인증하는 것은 아니다.

② O: 전송모드의 ESP는 암호화 기능을 사용할 때 TCP·UDP 헤더와 데이터 등 **IP 페이로드를 암호화**하며, 원래 IP 헤더는 암호화하지 않는다. 따라서 페이로드의 내용을 숨기면서도 IP 헤더의 주소 정보는 패킷 전달에 사용할 수 있다.

③ X: 터널모드는 원래 IP 헤더와 페이로드를 포함한 패킷 전체를 내부 패킷으로 넣고, 바깥에 새 IP 헤더를 붙이는 방식이다. 이는 패킷을 감싸는 방식의 구분이므로 **ESP와 AH의 동시 사용을 요구하지 않는다**. 필요한 보안 서비스에 따라 ESP 또는 AH를 단독으로 사용하거나 둘을 조합할 수 있다. 특히 ESP 자체가 암호화와 인증·무결성 보호를 함께 제공할 수 있으므로, 인증을 위해 AH를 반드시 추가할 필요는 없다.

④ O: 보안 연관(SA)은 IPsec 통신에 적용할 보안 프로토콜, 알고리즘, 키 등의 보안 매개변수를 정한 관계이다. **IKE는 통신 상대를 인증하고 보안 매개변수와 키를 협상**하여 SA를 설정·관리하는 데 사용된다. 이렇게 정한 정보에 따라 실제 패킷에 AH나 ESP 보호를 적용한다.

NoteBase

문 20. ARP(Address Resolution Protocol)에 대한 설명으로 옳지 않은 것은?

① ARP는 논리 주소를 물리 주소로 변환해준다.

② ARP 패킷에는 발신자와 해당 수신자의 물리 주소와 논리 주소가 포함된다.

③ ARP 패킷은 데이터링크 프레임에 캡슐화된다.

④ 같은 네트워크상에서 ARP 요청 패킷과 ARP 응답 패킷은 브로드캐스트 된다.

정답 4번

간단한 해설

상대의 MAC 주소를 알아내는 ARP 요청은 **브로드캐스트**로 보내지만, 응답은 일반적으로 **요청자에게 유니캐스트**로 보낸다. 응답자는 요청 패킷에 담긴 발신자의 MAC 주소를 알고 있으므로 전체 호스트에게 응답할 필요가 없다.

선지별 해설

① O: ARP는 IPv4 주소와 같은 **논리 주소에 대응하는 물리 주소(MAC 주소)**를 알아내는 프로토콜이다. 같은 링크에서 프레임을 전달할 상대의 IP 주소는 알지만 MAC 주소를 모를 때 주소 대응 정보를 구한다.

② O: ARP 패킷에는 **발신자와 대상의 물리 주소·논리 주소 필드**가 있다. 다만 요청 단계에서는 대상의 MAC 주소를 알아내려는 것이므로, 대상 물리 주소 필드에 실제 대상의 MAC 주소가 들어 있어야 하는 것은 아니다. 응답에서는 해당 MAC 주소를 알려 준다.

③ O: ARP 패킷은 **데이터링크 계층의 프레임에 캡슐화**되어 전달된다. 이더넷에서는 ARP 패킷을 이더넷 프레임의 데이터 부분에 넣으며, IP 패킷에 넣어 보내는 방식이 아니다.

④ X: 일반적인 주소 확인 과정에서 ARP 요청은 같은 브로드캐스트 도메인의 호스트들에게 보내지만, 응답은 **요청자의 MAC 주소를 목적지로 하는 유니캐스트**로 보낸다. 요청 패킷에 발신자의 MAC 주소가 포함되어 있으므로 응답자는 그 주소로 직접 회신할 수 있다. 따라서 요청과 응답이 모두 브로드캐스트된다는 설명을 고쳐야 한다.

NoteBase