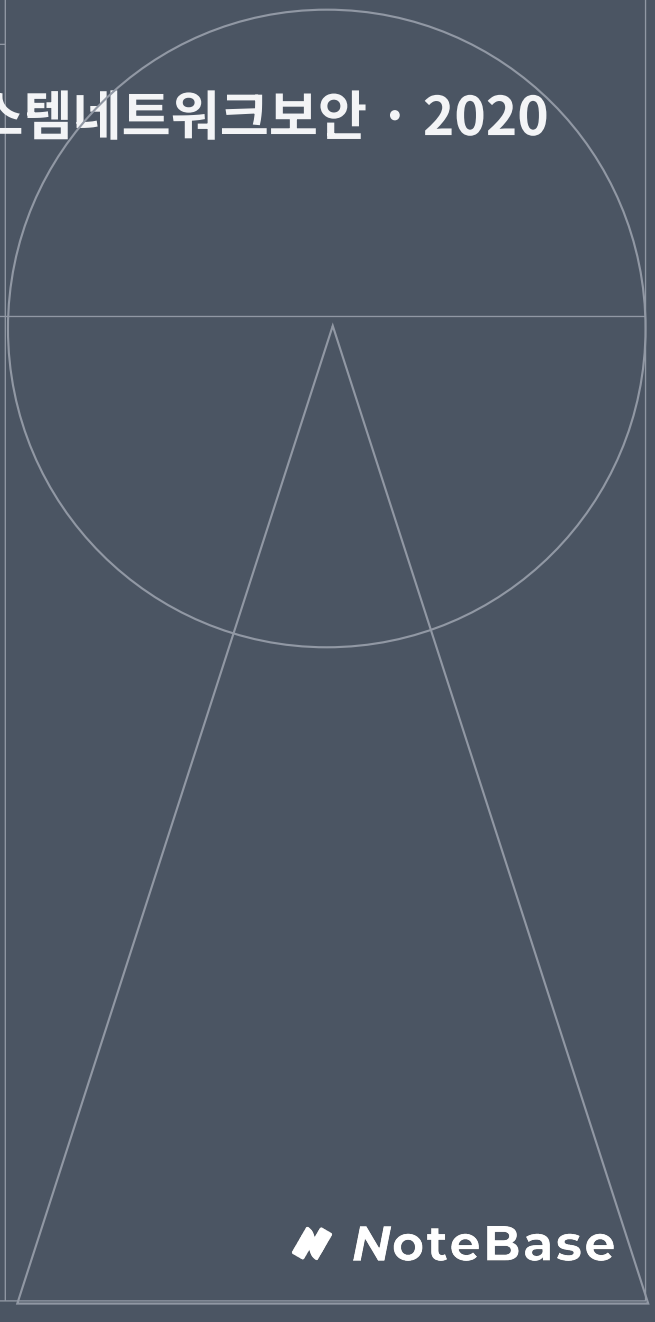
기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2020



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2020

공무원/경찰/경력채용 · 시스템네트워크보안 · 2020

문 1. ARP 스푸핑(Spoofing) 공격은 ARP 캐시 테이블에 저장된 대응 관계를 조작해 수행하는 공격 방법이다. 다음에서 ARP 캐시 테이블에 저장되는 대응 관계가 가장 적절하게 연결된 것은?

① MAC 주소 - IP 주소

② TCP 포트 - IP 주소

③ 도메인 이름 - IP 주소

④ MAC 주소 - 도메인 이름

정답 1번

간단한 해설

ARP 캐시는 로컬 링크에서 통신할 때 사용하는 **IP 주소와 MAC 주소의 대응**을 저장한다. 도메인 이름의 주소 해석이나 TCP 서비스 포트의 구분과는 역할이 다르다.

핵심 풀이

ARP는 이더넷 같은 로컬 네트워크에서 IPv4 주소에 대응하는 링크 계층 주소인 MAC 주소를 알아내는 프로토콜이다. ARP 캐시는 알아낸 **IP 주소와 MAC 주소의 대응**을 보관하여 같은 주소를 찾을 때 매번 질의하지 않도록 한다.

IP 주소는 네트워크 계층에서 호스트를 식별하고, MAC 주소는 로컬 링크에서 프레임을 전달할 대상을 지정한다. 목적지가 다른 네트워크에 있으면 보통 원격 호스트가 아니라 **다음 홉인 게이트웨이의 MAC 주소**를 알아내어 프레임을 전달한다.

TCP 포트는 호스트 안의 통신 종단점·서비스를 구별하므로 ARP의 주소 변환 대상이 아니다. 도메인 이름과 IP 주소의 대응은 DNS가 담당하며, MAC 주소와 도메인 이름도 ARP 캐시에 저장하는 대응 관계가 아니다.

ARP 스푸핑은 이 IP–MAC 대응을 거짓 정보로 오염시켜 프레임이 잘못된 대상으로 전달되게 하는 공격이다. 따라서 대응 관계가 맞는 선택지는 ① MAC 주소–IP 주소이다.

NoteBase

문 2. 다음 중 TCP/UDP 프로토콜을 사용하는 서비스에 대하여, <서비스명> <포트번호> <전송프로토콜>의 관계를 연결한 것으로 가장 적절하지 않은 것은?

① <서비스명>: SMTP, <포트번호>: 25, <전송프로토콜>: TCP

② <서비스명>: DHCP, <포트번호>: 67,68, <전송프로토콜>: UDP

③ <서비스명>: SSH, <포트번호>: 22, <전송프로토콜>: UDP

④ <서비스명>: SSL, <포트번호>: 443, <전송프로토콜>: TCP

정답 3번

간단한 해설

SSH의 기본 접속은 **TCP 22번**을 사용한다. 포트 번호는 맞지만 전송 프로토콜을 UDP로 연결한 부분이 잘못되었다.

선지별 해설

① O: SMTP는 전자우편을 전송하는 프로토콜이며, 메일 서버 간 전달에 기본적으로 **TCP 25번**을 사용한다. 연결을 맺고 명령과 응답을 주고받으므로 제시된 연결이 적절하다.

② O: DHCP는 호스트에 IP 주소 등의 네트워크 설정을 제공한다. DHCPv4는 **UDP 서버 67번, 클라이언트 68번**을 사용하므로 포트와 전송 프로토콜이 올바르게 연결되어 있다.

③ X: SSH는 암호화된 원격 접속을 제공하며 기본적으로 **UDP가 아니라 TCP 22번**을 사용한다. 따라서 전송 프로토콜을 UDP로 연결한 ③이 가장 적절하지 않다.

④ O: 이 연결은 SSL/TLS로 보호하는 웹 서비스인 **HTTPS의 통상적인 TCP 443번**을 가리키는 것으로 이해한다. 엄밀히 말하면 SSL 자체에 모든 응용에 공통인 443번 전용 포트가 있는 것은 아니며, 적용하는 응용 서비스에 따라 포트가 달라진다.

NoteBase

문 3. 다음 중 Unix 서버의 사용자 계정에 관련된 파일의 설명으로 가장 적절하지 않은 것은?

① /etc/passwd: 사용자 기본 정보 파일

② /etc/shadow: 암호화된 사용자 패스워드, 패스워드 정책이 포함된 파일

③ /etc/group: 그룹 기본 정보 파일

④ /etc/login.defs: 사용자 계정 생성 시 기본 정보를 가지고 있는 파일

정답 4번

출제 포인트

사용자·그룹 정보 저장 파일과 계정 생성에 적용하는 기본값·정책 설정 파일의 역할을 구분하는 문제이다.

핵심 개념

/etc/passwd는 사용자 계정의 기본 정보를, /etc/shadow는 패스워드 해시와 계정별 패스워드 사용 기간 정보를, /etc/group은 그룹 정보를 저장한다.
/etc/default/useradd는 새 계정의 기본 그룹·홈 디렉터리 경로·로그인 셸 등의 기본값을 설정한다.
/etc/login.defs는 패스워드 사용 기간의 기본 정책, 사용자·그룹 ID 범위 등 계정 관리 정책을 설정한다.

선지별 해설

O/X는 설명의 적절성을 나타내며, X는 이 문항에서 상대적으로 가장 적절하지 않은 설명이다.
① O. /etc/passwd에는 사용자 이름, 사용자 ID, 기본 그룹 ID, 홈 디렉터리, 로그인 셸 등 사용자 기본 정보가 저장된다.
② O. /etc/shadow에는 패스워드 해시와 마지막 변경일, 최소·최대 사용 기간, 만료 경고 기간 등이 저장된다. 선지의 '암호화된 사용자 패스워드'는 평문 대신 패스워드 해시를 저장한다는 뜻으로 이해한다. 패스워드 정책은 여기서 계정별 사용 기간·만료 설정을 뜻한다.
③ O. /etc/group에는 그룹 이름, 그룹 ID, 그룹 구성원 목록 등 그룹 기본 정보가 저장된다.
④ X. '사용자 계정 생성 시 기본 정보를 가지고 있는 파일'이라는 설명은 /etc/default/useradd의 대표 역할에 더 직접적으로 대응한다. /etc/login.defs는 계정 관리 정책을 설정하는 파일로 설명하는 것이 더 정확하다. 다만 /etc/login.defs도 새 계정 생성 시 참조되므로, 계정 생성과 무관하다는 뜻으로 교정하면 안 된다. 기본 그룹·홈 경로·로그인 셸 등의 기본값과 패스워드 사용 기간·ID 범위 등의 정책을 구분하는 것이 핵심이다.

오답 포인트

④의 '계정 생성 시 기본 정보'라는 넓은 표현 때문에 두 설정 파일을 혼동하기 쉽다. /etc/login.defs도 계정 생성에 관여하지만, 새 계정의 기본 환경값을 설정하는 /etc/default/useradd와 계정 관리 정책을 설정하는 /etc/login.defs의 대표 역할을 구분한다.

NoteBase

다시 나오면 이렇게 판단

파일이 사용자·그룹별 정보를 저장하는지, 새 계정의 기본값을 정하는지, 계정 관리 정책을 정하는지를 먼저 구분한다. 계정 생성 기본값이면 /etc/default/useradd, 패스워드 사용 기간이나 ID 범위 정책이면 /etc/login.defs에 대응시킨다.

암기 포인트

passwd는 사용자, shadow는 패스워드·만료, group은 그룹, default/useradd는 생성 기본값, login.defs는 계정 관리 정책이다.

NoteBase

문 4. 다음 중 TLS 1.3에 대한 설명으로 가장 적절하지 않은 것은?

① 0-RTT(Zero-Round Trip Time)이 추가되었다.

② 해시 알고리즘 중 MD5와 SHA-224가 사용되지 않는다.

③ 모든 핸드쉐이크(Handshake) 메시지가 암호화된다.

④ RC4 알고리즘이 제거되었다.

정답 3번

간단한 해설

TLS 1.3은 **ServerHello 이후**의 핸드셰이크 메시지를 암호화한다. 초기 ClientHello와 ServerHello까지 모두 암호화되는 것은 아니다.

선지별 해설

① O: TLS 1.3에는 미리 공유한 키를 바탕으로 핸드셰이크 완료 전에 일부 응용 데이터를 보내는 **0-RTT 조기 데이터** 방식이 추가되었다. 재접속 등의 지연을 줄이지만 일반적인 1-RTT 데이터와 보안 보장이 같지는 않으며 재전송 공격에 주의해야 한다.

② O: TLS 1.3은 지원 알고리즘을 정비하여 **MD5와 SHA-224를 협상·사용하지 않도록** 한다. 특히 서명 알고리즘 협상에서 이러한 이전 해시·서명 조합을 허용하지 않는다.

③ X: TLS 1.3에서 암호화되는 것은 **ServerHello 이후의 핸드셰이크 메시지**이다. 초기 ClientHello와 ServerHello는 키 합의에 필요한 정보를 교환하므로 기본 핸드셰이크에서 평문으로 전달된다. 따라서 모든 핸드셰이크 메시지가 처음부터 암호화된다는 설명은 부적절하다.

④ O: TLS 1.3은 RC4 등 이전 암호 알고리즘을 제거하고 **AEAD 방식의 인증 암호**를 사용한다. RC4는 TLS 1.3에서 선택할 수 있는 암호 알고리즘이 아니다.

NoteBase

문 5. 다음에서 설명하는 은닉전략(Concealment Strategy) 바이러스로 가장 적절한 것은?

· 감염시킬 때마다 변이가 일어난다.
· 변이가 일어날 때마다 자신을 완벽하게 새로 만들어서 탐지하기 어렵다.
· 모양만 변경하지 않고 동작도 변화시킨다.

① 암호화된 바이러스(Encrypted Virus)
② 스텔스 바이러스(Stealth Virus)
③ 폴리모픽 바이러스(Polymorphic Virus)
④ 메타모픽 바이러스(Metamorphic Virus)

정답 4번

간단한 해설

감염할 때마다 **바이러스 본체 코드 자체를 재구성**하는 것이 메타모픽의 핵심이다. 코드 구현이 달라져도 핵심 악성 기능까지 반드시 달라지는 것은 아니다.

핵심 풀이

메타모픽 바이러스는 감염·복제 과정에서 **자기 본체 코드를 새 형태로 재구성**한다. 따라서 감염할 때마다 변이가 일어나고 자신을 새로 만든다는 두 단서가 메타모픽의 특징을 직접 가리킨다.

원문의 '동작도 변화시킨다'는 표현은 주의해서 읽어야 한다. 메타모픽은 명령 구성과 실행 구현을 바꾸지만 **핵심 악성 기능 자체가 반드시 달라지는 것은 아니다**. 같은 기능을 다른 코드로 구현할 수 있으므로, 이 문구를 악성 목적까지 매번 바뀐다는 일반 정의로 외우면 부정확하다.

암호화된 바이러스는 본체를 암호화하여 내용을 숨기는 방식이다.

스텔스 바이러스는 감염 흔적이나 시스템이 보여 주는 정보를 숨기는 데 초점이 있다.

폴리모픽 바이러스는 대표적으로 암호화된 형태와 복호화 부분을 변화시키며, **본체 코드 자체를 다시 구성하는 메타모픽**과 구별한다.

따라서 자신을 새로 만들어 본체 코드를 변형한다는 핵심 단서에 해당하는 것은 메타모픽 바이러스인 ④이다.

NoteBase

문 6. 다음에서 sudo 명령에 대한 가장 적절한 것을 모두 고른 것은?

㉠ sudo 명령은 일반 사용자 계정을 root 계정으로 전환하기 위해 사용된다.
㉡ sudo 명령을 사용할 때 암호는 root 계정의 암호를 사용한다.
㉢ root 계정으로 실행 가능한 명령을 일반 사용자가 실행할 수 있게 해준다.
㉣ 사용자가 sudo 명령을 사용할 수 있도록 /etc/sudoers 파일에 권한을 설정한다.

① ㉠㉣
② ㉠㉡㉣
③ ㉢㉣
④ ㉡㉢㉣

정답 3번

간단한 해설

sudo는 정책으로 허용된 명령을 **다른 사용자 권한으로 실행**하게 한다. 기본적인 인증에서는 호출자 자신의 암호를 사용하며, 허용 범위는 sudoers 정책에 따른다.

보기별 해설

㉠ X: sudo의 기본 역할은 계정 자체를 root로 바꾸는 것이 아니라, **허용된 명령을 다른 사용자 권한으로 실행**하는 것이다. 일반적인 계정 전환 명령인 su와 구별한다. 다만 sudo -i나 sudo -s처럼 허용된 셸을 실행하면 root 셸을 얻을 수도 있으므로, sudo로 root 셸을 실행할 수 없다는 의미는 아니다.

㉡ X: 일반적인 sudoers 기본 정책에서는 root의 암호가 아니라 **명령을 호출한 사용자 자신의 암호**로 인증한다. rootpw·targetpw 등의 별도 정책 설정이나 암호 입력 면제 설정에 따라 달라질 수 있으므로, 항상 root 암호를 사용한다는 설명은 부적절하다.

㉢ O: sudo는 권한 정책이 허용하는 범위에서 일반 사용자가 **root 등 대상 사용자의 권한**으로 명령을 실행하게 한다. 아무 사용자나 모든 명령을 무제한 실행할 수 있게 한다는 뜻은 아니다.

㉣ O: sudoers 정책에서는 /etc/sudoers와 그 파일에서 포함하는 설정을 통해 사용자·대상 계정·허용 명령 등의 **실행 권한**을 지정한다. 따라서 일반 사용자의 sudo 사용 권한을 이 파일에 설정한다는 설명은 부합한다.

따라서 적절한 보기는 ㉢과 ㉣이며, 이를 함께 제시한 조합은 ③이다.

NoteBase

문 8. VPN(Virtual Private Network)에 대한 설명으로 가장 적절하지 않은 것은?

① 공중망을 이용하여 사설망과 같은 효과를 얻는다.

② 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.

③ VPN 구현 기술에는 터널링, 암호화, 인증, 접근제어 등이 있다.

④ IPsec은 VPN 터널의 업계 표준 프로토콜로 강력한 사용자 인증과 암호화를 제공하는 OSI 2계층 프로토콜이다.

정답 4번

간단한 해설

IPsec은 **OSI 3계층인 네트워크 계층**에서 IP 패킷을 보호한다. 따라서 이를 2계층 프로토콜이라고 한 설명이 적절하지 않다.

선지별 해설

① O: VPN은 인터넷과 같은 공중망 위에 논리적으로 분리된 통신 경로를 구성하여 **사설망처럼 통신할 수 있게 하는 기술**이다. 물리적인 전용 회선을 새로 구축하는 것과는 구별된다.

② O: 공중망을 활용하므로 전용 회선을 별도로 확보하는 사설망에 비해 **일반적으로 구축비용을 줄일 수 있다**. 다만 실제 비용은 회선, 장비, 운영 규모와 서비스 계약에 따라 달라질 수 있다.

③ O: 터널링은 원래 패킷을 다른 패킷에 담아 전달하고, 암호화는 전송 내용의 기밀성을 보호한다. 인증은 통신 상대 등을 확인하며, 접근제어는 허용된 자원만 이용하게 한다. 이들은 **VPN을 구현하고 보호하는 주요 기술**이다.

④ X: IPsec은 IP 패킷을 보호하는 **OSI 3계층인 네트워크 계층**의 보안 프로토콜 체계이므로 2계층 프로토콜이라는 부분이 틀렸다. IPsec은 VPN 구현에 널리 사용되며 구성에 따라 무결성, 데이터 출처 인증, 암호화 등을 제공한다. 모든 구성에서 사용자 인증과 암호화가 일괄적으로 제공된다는 의미로 이해해서는 안 된다.

NoteBase

문 9. Linux의 네트워크 관련 명령 <보기 1>과 설명 <보기 2>를 가장 적절하게 연결한 것은?

<보기 1>
(가) ifconfig (나) nslookup
(다) route (라) netstat

<보기 2>
㉠ DNS(Domain Name Service) 서버에 질의하기
㉡ 네트워크 인터페이스 설정하기
㉢ 네트워크의 상태정보를 출력하기
㉣ 기본 게이트웨이 설정하기

① (가): ㉠, (나): ㉡, (다): ㉢, (라): ㉣
② (가): ㉡, (나): ㉠, (다): ㉣, (라): ㉢
③ (가): ㉠, (나): ㉡, (다): ㉣, (라): ㉢
④ (가): ㉡, (나): ㉠, (다): ㉢, (라): ㉣

정답 2번

간단한 해설

ifconfig는 인터페이스 설정, nslookup은 DNS 질의에 사용한다. **기본 게이트웨이 설정은 route**, 네트워크 상태 출력은 netstat의 역할이다.

NoteBase

대응 관계 해설

(가) ifconfig → ㉡: ifconfig는 **네트워크 인터페이스의 주소·동작 상태를 설정**하거나 표시한다. IP주소·넷마스크를 지정하고 인터페이스를 활성화·비활성화하는 역할이므로 '네트워크 인터페이스 설정하기'에 해당한다.

(나) nslookup → ㉠: nslookup은 **DNS 서버에 이름 정보를 질의**하는 도구이다. 도메인 이름에 대응하는 IP주소 등 DNS 레코드를 조회하므로 'DNS 서버에 질의하기'와 연결된다. 인터페이스의 주소 자체를 설정하는 명령은 아니다.

(다) route → ㉢: route는 커널의 IP 라우팅 테이블을 조회·수정한다. 기본 경로를 추가하면서 **기본 게이트웨이를 지정**할 수 있으므로 '기본 게이트웨이 설정하기'에 해당한다. 기본 게이트웨이는 더 구체적으로 일치하는 경로가 없을 때 패킷을 전달할 다음 경유지이다.

(라) netstat → ㉣: netstat은 네트워크 연결·소켓, 라우팅 테이블, 인터페이스 통계 등 **네트워크의 상태 정보**를 출력한다. 여기서는 조회 기능을 묻고 있으므로 기본 게이트웨이를 설정하는 route와 구별한다.

따라서 (가)–㉡, (나)–㉠, (다)–㉢, (라)–㉣의 대응이며 ②와 일치한다.

NoteBase

문 10. 다음에 설명하는 메모리 위법행위(Memory Corruption)의 취약점으로 가장 적절한 것은?

· 브라우저에서 많이 발생하는 취약점으로, 반납된 포인터를 사용할 때 발생한다.
· 자바스크립트, 파일 로딩 등으로 힙 메모리를 조작할 수 있는 상황에서 공격이 가능하다.

① Heap Buffer Overflow
② Stack Overflow
③ Use - After - Free
④ Double Free

정답 3번

간단한 해설

해제한 메모리를 기존 포인터로 다시 사용하는 취약점은 Use-After-Free이다. 반납된 힙 영역이 다른 객체에 재사용되면 오래된 포인터가 의도하지 않은 내용을 참조할 수 있다.

핵심 풀이

Use-After-Free는 **해제한 메모리를 기존 포인터로 다시 참조**하여 발생하는 취약점이다. 메모리를 반납해도 그 주소를 가진 포인터가 남을 수 있으며, 이를 댕글링 포인터라고 한다. 따라서 지문의 반납된 포인터 사용이 핵심 단서이다.

브라우저에서 자바스크립트 실행이나 파일 로딩으로 객체의 할당·해제가 일어나면 해제된 힙 영역이 다른 객체에 재사용될 수 있다. 이때 오래된 포인터가 새로 들어온 내용을 원래 객체처럼 참조하면 잘못된 읽기·쓰기나 실행 흐름의 변조로 이어질 수 있다. 힙 메모리를 조작할 수 있다는 단서는 이러한 재사용 상황과 연결된다.

Heap Buffer Overflow는 힙 버퍼의 경계를 넘어 접근하는 문제이고, Stack Overflow는 스택의 허용 범위를 넘는 문제이다. 둘 다 **해제 후 재참조**라는 지문의 핵심과 다르다.

Double Free는 이미 해제한 메모리를 다시 해제하는 문제이다. 해제된 메모리를 다시 사용하는 Use-After-Free와 행위가 다르므로, 지문에 해당하는 것은 ③ Use - After - Free이다.

NoteBase

문 11. 다음 중 IPv6에 대한 설명으로 가장 적절하지 않은 것은?

① 주소의 길이는 64비트이다.

② 주소할당은 네트워크 규모, 단말기 수에 따라 순차적으로 할당한다.

③ 주소의 개수는 2^{128}개이다.

④ 전달 방식에는 유니캐스트, 애니캐스트 등이 있다.

정답 1번

간단한 해설

IPv6 주소의 전체 길이는 **128비트**이므로 이론적인 주소 공간은 2^{128}개이다. 64비트의 부분 필드와 전체 주소 길이를 구분해야 한다.

선지별 해설

① X: IPv6 주소 전체의 길이는 **128비트**이다. 64비트는 많은 일반적인 주소 구성에서 인터페이스 식별자 등에 쓰이는 길이로, 전체 IPv6 주소 길이와 혼동하면 안 된다.

② O: 이 문항에서는 네트워크의 규모와 필요를 고려하여 주소 공간을 배분한다는 취지로 판단한다. 다만 원문의 '순차적으로'는 엄밀한 프로토콜 규칙이 아니다. IPv6 주소 공간은 **계층적인 프리픽스 단위**로 관리하며 서브넷 수와 확장 필요 등을 고려한다. 개별 단말 주소가 반드시 연속 번호로 배정되는 것은 아니고, 자동 설정 등 여러 방식이 가능하다.

③ O: 128비트 각각이 두 가지 값을 가지므로 전체 비트 조합 수는 2^{128}개이다. 이는 **이론적인 전체 주소 공간**의 크기이며, 모든 조합이 일반 단말의 전역 유니캐스트 주소로 사용된다는 뜻은 아니다.

④ O: 유니캐스트는 하나의 인터페이스로 전달하고, 애니캐스트는 같은 주소를 공유하는 인터페이스들 가운데 라우팅 기준으로 가까운 하나에 전달한다. IPv6에는 멀티캐스트도 있으며 **브로드캐스트 주소는 사용하지 않는다**.

따라서 전체 주소 길이를 64비트로 제시한 ①이 가장 적절하지 않다.

NoteBase

문 12. 침입탐지시스템(Intrusion Detection System)에 대한 기능으로 가장 적절한 것을 모두 고른 것은?

㉠ 네트워크를 실시간 감시하는 기능
㉡ 네트워크에 유해한 트래픽을 탐지하고 차단하는 기능
㉢ 네트워크를 통한 웜 공격, 바이러스 공격 등을 탐지하고 차단하는 기능
㉣ 침입 분석 및 사용자 리포트 기능

① ㉠㉡
② ㉠㉣
③ ㉡㉢
④ ㉢㉣

정답 2번

간단한 해설

IDS는 **감시·탐지·분석·보고**를 중심으로 하고, IPS는 탐지한 공격의 차단까지 수행한다. 따라서 IDS의 기능으로 적절한 것은 **㉠과** ㉣이다.

보기별 해설

㉠ O: 네트워크 기반 IDS는 네트워크 트래픽을 감시하고 분석하여 침입 징후나 비정상 행위를 탐지한다. 따라서 **네트워크의 실시간 감시**는 IDS의 대표적인 기능이다.

㉡ X: 유해 트래픽을 **탐지하는 것**은 IDS의 기능이지만, 탐지와 함께 트래픽을 직접 차단하는 것은 IDS와 IPS를 구별할 때 **IPS의 대표적인 기능**이다. 이 문항은 탐지·알림 중심의 IDS와 차단까지 수행하는 IPS를 구별하고 있으므로, 탐지와 차단을 함께 묶은 설명은 적절하지 않다.

㉢ X: 웜이나 바이러스 관련 공격 징후를 탐지할 수 있다는 점만으로 틀린 것은 아니다. 다만 공격을 탐지하고 **직접 차단하는 기능까지** 포함하여 서술했으므로, 이 문항의 IDS와 IPS 구별에서는 IPS의 기능에 해당한다.

㉣ O: IDS는 수집한 이벤트와 경보를 분석하고, 관리자가 침입 여부와 대응 필요성을 파악할 수 있도록 기록과 보고서를 제공한다. 따라서 **침입 분석 및 사용자 리포트**는 IDS의 기능이다.

적절한 보기는 ㉠과 ㉣이므로 이에 해당하는 조합은 ②이다. 실제 제품은 차단 장비와 연동하거나 능동 대응 기능을 포함할 수 있으므로, IDS가 어떠한 대응에도 관여할 수 없다는 뜻은 아니다.

NoteBase

문 13. 프락시 방화벽(Proxy Firewall)의 장점으로 가장 적절하지 않은 것은?

① 트래픽 처리 성능이 향상된다.

② 가능하면 응용프로그램 계층까지 전체적으로 패킷 안의 정보를 검사한다.

③ 패킷 필터링보다 좋은 성능의 보안을 제공한다.

④ 보호되는 시스템과 보호되지 않는 시스템 사이의 연결을 차단시킨다.

정답 1번

간단한 해설

프락시 방화벽은 세밀한 검사와 연결 중계로 보안을 강화하지만, 그만큼 **추가 처리 부담과 지연**이 생길 수 있다. 처리 속도 향상을 일반적인 장점으로 보기는 어렵다.

선지별 해설

① X: 프락시 방화벽은 연결을 중계하고 응용 계층의 내용을 해석·검사하므로 **추가 처리 부담**이 발생한다. 따라서 단순 패킷 필터링에 비해 처리 지연이나 처리량 감소가 생길 수 있으며, 트래픽 처리 성능 향상을 일반적인 장점으로 보기는 어렵다.

② O: 지원하는 응용 프로토콜의 헤더와 데이터 내용까지 해석하여 **응용 계층 수준의 검사**를 할 수 있다. 단순히 주소와 포트만 비교하는 것보다 세밀한 접근 제어가 가능하다는 장점이다.

③ O: 단순 패킷 필터링보다 통신 내용과 응용 프로토콜의 특성을 자세히 확인하여 **더 세밀한 보안 정책**을 적용할 수 있다. 여기서 좋은 보안 성능은 처리 속도가 빠르다는 뜻이 아니라, 검사·통제의 정밀도가 높다는 의미이다.

④ O: 외부와 내부 호스트가 직접 연결되지 않도록 프락시가 통신을 대신 중계한다. 즉, **양 끝 호스트의 직접 연결**을 끊고 각각 프락시와 별도 연결을 맺게 하는 것이며, 허용된 통신까지 전부 금지한다는 뜻은 아니다.

NoteBase

문 14. NAT(Network Address Translation)는 내부 네트워크의 사설 IP 주소를 외부 네트워크의 공인 IP 주소로 변환 또는 역변환하는 기술을 의미한다. 다음 중 NAT의 장점으로 가장 적절하지 않은 것은?

① 공중망에 접속 유연성 제공

② 내부망 주소 방식에 대한 일관성 제공

③ 네트워크 보안 기능 제공

④ 네트워크 속도 향상

정답 4번

간단한 해설

NAT는 주소를 변환하는 기술이며 **통신 속도를 높이는 기술은 아니다**. 오히려 변환과 매핑 처리로 추가 부하가 발생할 수 있다.

선지별 해설

① O: NAT는 내부 사설 주소와 외부 공인 주소를 매핑하므로, 내부 호스트가 사설 주소를 유지하면서 공중망에 접속할 수 있다. 특히 포트까지 변환하는 NAPT를 사용하면 **여러 내부 호스트가 하나의 공인 주소를 공유**할 수 있어 외부 접속 구성이 유연해진다.

② O: 내부 주소 체계를 외부 주소 체계와 분리하므로, 인터넷 서비스 제공자나 할당받은 공인 주소가 바뀌어도 NAT 설정을 조정하여 **내부 주소 체계를 유지**할 수 있다. 내부 호스트의 주소를 일괄 변경해야 하는 부담이 줄어든다.

③ O: 외부에 내부 사설 주소를 그대로 노출하지 않아 내부 주소 구조를 숨기는 효과가 있다. 또한 일반적인 동적 NAT에서는 기존 매핑이 없는 외부발 연결이 제한될 수 있다. 다만 **NAT 자체가 방화벽이나 암호화를 대신하지는 않으며**, 설정과 매핑 방식에 따라 접근 가능 범위가 달라진다.

④ X: NAT는 주소·포트 변환과 매핑 조회 등의 추가 처리를 수행하므로, **네트워크 속도 향상 자체가 장점은 아니다**. 장비의 처리 능력과 부하에 따라 지연이나 병목이 생길 수도 있다. 따라서 NAT의 장점으로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 15. 다음과 같이 방화벽을 관리하는 iptables 명령을 이용하여 특정한 조건이 충족될 때만 포트가 동적으로 오픈되도록 하는 기술로 가장 적절한 것은?

```
iptables -A INPUT -p icmp --icmp-type echo-request -m recent --set --name PING
iptables -A INPUT -p tcp --dport 22 -m recent --rcheck --seconds 5 --name PING -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 --dport 22 -j DROP
```

① 포트 포워딩(Port Forwarding)

② 포트 노킹(Port Knocking)

③ 포트 예약(Port Reservation)

④ 포트 할당(Port Assignment)

정답 2번

간단한 해설

ICMP 신호를 보낸 출발지를 기록하고, **5초 이내의 기록이 있을 때만 TCP 22번 접근을 허용**한다. 사전 신호로 접근 조건을 충족시키는 포트 노킹의 예이다.

핵심 풀이

첫 번째 규칙은 ICMP Echo Request가 들어오면 recent 모듈의 PING 목록에 **그 패킷의 출발지 주소와 최근 시각을 기록**한다. '--set'은 기록을 만들거나 갱신하며, 이 줄 자체에 ACCEPT 동작이 지정된 것은 아니다.

두 번째 규칙은 목적지 TCP 포트가 22번인 패킷에 대해 같은 출발지가 PING 목록에 있고 **최근 5초 이내에 기록되었는지**를 검사한다. 조건에 맞으면 ACCEPT하므로 사전 신호를 보낸 출발지의 SSH 접근이 제한된 시간 조건에서 허용된다.

세 번째 규칙은 앞의 허용 조건을 통과하지 못한 TCP 22번 패킷을 모든 출발지에 대해 DROP한다. 따라서 포트를 항상 공개하는 것이 아니라 **선행 신호가 확인된 경우에만 접근을 허용**하는 구조이며, 문항에서는 이를 포트 노킹으로 분류한다.

포트 포워딩은 도착한 트래픽을 다른 주소나 포트로 전달하는 것이고, 포트 예약·할당은 포트 번호의 사용이나 배정을 정하는 개념이다. 여기에는 목적지를 바꾸는 전달 규칙이 아니라 최근 신호의 존재를 확인하는 접근 조건이 있으므로 이들과 구별된다.

따라서 해당 기술은 포트 노킹인 ②이다.

NoteBase

문 16. Windows 레지스트리 루트키에 대한 설명으로 가장 적절한 것은?

① HKEY_CURRENT_USER: 컴퓨터에서 모든 계정에 관한 정보를 저장한다.

② HKEY_USERS: 현재 로그온 된 사용자와 관련된 데이터를 저장한다.

③ HKEY_CLASSES_ROOT: 시스템 관련 정보를 저장한다.

④ HKEY_CURRENT_CONFIG: 현재 하드웨어 프로필에 관한 일부 정보를 저장한다.

정답 4번

간단한 해설

HKEY_CURRENT_CONFIG는 **현재 하드웨어 프로필**의 정보를 제공하며, 표준 구성과 현재 구성의 차이를 나타낸다. 이 설명은 루트키의 고유 역할과 범위를 직접적으로 밝힌다.

선지별 해설

이 문항은 각 진술이 넓은 의미에서 성립하는지만이 아니라, 루트키의 역할을 가장 정확하고 구체적으로 설명한 것을 고르는 문제이다. 아래 O는 진술이 성립한다는 뜻이며, 곧바로 가장 적절한 답이라는 뜻은 아니다.

① X: HKEY_CURRENT_USER는 **현재 사용자**의 환경과 응용 프로그램 설정을 제공하는 루트키이다. 모든 계정의 정보를 저장하는 키가 아니며, HKEY_USERS 아래의 해당 사용자 프로필에 연결된다.

② O: HKEY_USERS 아래에는 로드된 사용자 프로필들이 있으므로 현재 로그온한 사용자의 데이터도 포함된다. 따라서 '현재 사용자와 관련된 데이터를 저장한다'는 문장 자체를 거짓으로 볼 수는 없다. 다만 HKEY_USERS의 범위가 현재 사용자 한 명에 한정되는 것은 아니므로, 이 설명만으로는 루트키의 전체 범위를 충분히 구분하지 못한다. 현재 사용자의 설정을 직접 가리키는 루트키는 HKEY_CURRENT_USER이다.

③ O: 파일 형식 연결과 COM 클래스 등록 정보도 넓은 의미에서 시스템 관련 정보에 포함된다. 그러나 HKEY_CLASSES_ROOT의 고유 역할은 **파일 형식·클래스와 그 속성의 등록 정보**를 제공하는 것이다. '시스템 관련 정보'라는 설명은 너무 포괄적이어서 이 키를 다른 루트키와 구별하지 못한다. 컴퓨터 전반의 하드웨어·소프트웨어 구성을 가리키는 대표적인 루트키는 HKEY_LOCAL_MACHINE이다.

④ O: HKEY_CURRENT_CONFIG는 현재 사용 중인 하드웨어 프로필 정보를 제공한다. 특히 표준 하드웨어 구성에 대한 현재 구성의 차이를 나타내므로 '현재 하드웨어 프로필에 관한 일부 정보'라는 설명이 해당 키의 대상과 범위를 구체적으로 나타낸다.

②는 포함되는 데이터의 일부를 말하고 ③은 지나치게 넓은 범주를 말하는 데 비해, ④는 루트키가 다루는 현재 하드웨어 프로필을 정확히 특정한다. 이와 같은 역할 구분을 기준으로 제공된 정답 ④를 선택한다.

NoteBase

문 17. 다음에서 설명하고 있는 전자우편(e-mail) 보안 프로토콜로 가장 적절한 것은?

· 전자우편 에이전트 간 분배단계에서 스팸을 처리하는데 사용할 수 있다.
· 수신측에서 MDA(Message Delivery Agent)는 DNS(Domain Name Service)를 이용해 해당 공개키를 가져와 서명 검증을 할 수 있다.
· 클라이언트 프로그램(MUA: Message User Agent)에서 구현되지 않기 때문에 사용자에 투명하게 동작한다.

① DKIM(DomainKeys Identified Mail)
② IMAP(Internet Mail Access Protocol)
③ PGP(Pretty Good Privacy)
④ S/MIME(Secure/Multipurpose Internet Mail Extension)

정답 1번

간단한 해설

DNS에 게시된 공개키로 도메인 서명을 검증한다는 단서는 DKIM을 가리킨다. 검증 결과를 스팸 처리에 활용할 수 있지만, 서명이 유효하다는 이유만으로 정상 메일이 보장되는 것은 아니다.

핵심 풀이

결정적 단서는 **DNS에서 공개키를 얻어 전자우편의 서명을 검증**한다는 점이다. DKIM은 서명 도메인의 개인키로 메시지에 서명을 붙이고, 수신측은 해당 도메인이 DNS에 게시한 공개키로 검증한다. 따라서 설명에 해당하는 것은 ① DKIM이다.

서명 검증 결과는 메시지에 책임을 표시한 도메인을 확인하고 스팸 처리 정책을 적용하는 데 활용할 수 있다. 다만 **서명 성공이 곧 스팸이 아님을 보장하지는 않는다**. DKIM은 본문을 암호화해 숨기는 기술도 아니다.

사용자에게 투명하다는 설명은 전형적인 메일 서버 측 서명·검증을 가리킨다. 사용자가 MUA에서 직접 키를 관리하지 않아도 송수신 과정에서 처리할 수 있다는 뜻이며, 모든 구현에서 MUA 활용이 기술적으로 금지된다는 뜻은 아니다.

IMAP은 서버에 보관된 전자우편에 접근·관리하는 프로토콜이다. PGP와 S/MIME은 전자우편 내용의 암호화·전자서명에 쓰이지만, 이 문제의 핵심인 도메인 기반 서명과 DNS 공개키 조회의 결합은 DKIM을 가리킨다.

NoteBase

문 18. Windows 파일 시스템에는 FAT(File Allocation Table) 방식과 NTFS(New Technology File System) 방식이 있다. 다음에서 FAT 방식과 비교하여 NTFS 방식의 장점으로 가장 적절한 것을 모두 고른 것은?

㉠ 호환성 우수
㉡ 강력한 보안 기능
㉢ 자동 압축 및 안정성
㉣ 디스크의 효율적 사용

① ㉠㉡
② ㉠㉢
③ ㉠㉢㉣
④ ㉡㉢㉣

정답 4번

간단한 해설

NTFS는 FAT에 비해 **접근 통제·압축·복구와 공간 관리 기능**이 강화되어 있다. 여러 구형 운영체제와 기기에 걸친 호환성은 오히려 FAT 계열의 대표적인 장점이다.

보기별 해설

㉠ X: 다양한 구형 운영체제와 기기에서 폭넓게 지원되는 **호환성은 FAT 계열의 장점**으로 보는 것이 일반적이다. NTFS의 고급 기능은 이를 지원하지 않는 환경에서는 그대로 이용할 수 없으므로, FAT보다 호환성이 우수하다고 일반화할 수 없다.

㉡ O: NTFS는 파일·디렉터리별 접근 권한과 보안 설명자 등을 지원하여 **사용자별 접근 통제**가 가능하다. 이러한 파일 시스템 수준의 보안 기능은 FAT와 비교되는 장점이다.

㉢ O: NTFS는 설정한 파일·폴더에 대해 투명한 **압축·해제**를 지원하며, 로그 기반 복구로 파일 시스템의 일관성과 안정성을 높인다. 자동 압축은 모든 파일이 기본적으로 압축된다는 뜻이 아니고, 로그 복구도 모든 사용자 데이터의 손실 방지를 보장하는 것은 아니다.

㉣ O: 파일 압축과 희소 파일 등의 기능을 활용하면 **실제 저장 공간의 낭비를 줄일 수 있다**. 다만 효율은 파일 특성·할당 단위·기능 설정에 따라 달라지므로 모든 경우에 동일한 절약 효과가 생기는 것은 아니다.

따라서 NTFS의 장점에 해당하는 보기는 ㉡·㉢·㉣이며, 이 조합은 ④이다.

NoteBase

문 19. 다음 중 Linux의 시스템 로그에 대한 설명으로 가장 적절하지 않은 것은?

① lastlog: 사용자의 IP 주소별로 가장 최근에 로그인한 시간, 접속 장소, 사용자 이름, IP 주소정보 등을 기록

② wtmp: 파일이 생성되는 순간부터 로그인/로그아웃 정보 기록

③ btmp: 시스템에 현재 로그인한 사용자에 대한 상태 정보 기록

④ syslog: 사용자 인증과 관련된 로그 및 커널, 데몬에서 생성된 모든 로그를 포함하여 기록

정답 3번

출제 포인트

Linux 로그인 로그를 사용자별 마지막 로그인, 누적 로그인 이력, 로그인 실패, 현재 접속 상태로 구분하는 문제이다.

핵심 개념

lastlog는 사용자별 마지막 로그인 정보를 저장한다. wtmp는 로그인·로그아웃 이력을 누적하고, btmp는 실패한 로그인 시도를 기록한다. utmp는 현재 로그인한 사용자의 상태를 기록한다. syslog는 인증, 커널, 데몬 등에서 발생하는 시스템 메시지를 처리하는 로그 체계이다.

선지별 해설

이 문항의 O는 가장 적절하지 않은 설명으로 선택한다는 뜻이며, X는 선택하지 않는다는 뜻이다.
① X: lastlog가 가장 최근 로그인 정보를 기록한다는 핵심은 맞다. 다만 “IP 주소별”은 정확하지 않으며, 올바르게는 “사용자별”이다. 접속 호스트 정보는 로그인 기록의 내용이지 기록을 구분하는 기준이 아니다. 이러한 표현상의 문제는 있지만, 로그의 기록 목적 자체를 다른 로그와 바꾼 ③이 더 부적절하다.
② X: wtmp는 로그인과 로그아웃 기록을 누적하므로 현재 접속 상태만 보여 주는 utmp와 구분된다. “파일이 생성되는 순간부터”는 기록 파일이 마련된 이후 이력이 쌓인다는 취지이다. 파일 생성 자체가 로그인 기록을 발생시키는 것은 아니다.
③ O: “시스템에 현재 로그인한 사용자에 대한 상태 정보”는 utmp의 설명이다. btmp의 올바른 설명은 “실패한 로그인 시도를 기록한다”이다. 로그인 실패 기록과 현재 접속 상태를 혼동했으므로 가장 적절하지 않다.
④ X: syslog는 인증, 커널, 데몬 등 여러 종류의 시스템 메시지를 처리하므로 설명의 핵심이 맞다. 다만 “모든 로그”가 한 파일에 무조건 저장된다는 뜻은 아니다. 실제 저장 대상과 위치는 로그 설정에 따라 달라진다.

오답 포인트

③의 “현재 로그인한 사용자”를 보면 utmp와 연결해야 한다. btmp는 접속에 성공해 사용 중인 사람이 아니라 로그인에 실패한 시도를 기록한다. ①의 “IP 주소별”과 ④의 “모든 로그”를 그대로 일반화하는 것도 피해야 한다.

NoteBase

다시 나오면 이렇게 판단

현재 접속 상태이면 utmp, 로그인·로그아웃의 누적 이력이면 wtmp, 로그인 실패이면 btmp, 사용자별 마지막 로그인이면 lastlog로 구분한다. 여러 구성 요소의 시스템 메시지를 다루는 체계는 syslog이다.

암기 포인트

utmp는 현재, wtmp는 이력, btmp는 실패, lastlog는 사용자별 마지막 로그인이다.

NoteBase

문 20. Windows 운영체제에서 감사정책은 어떤 로그를 기록할지 정의한 규칙을 말한다. 다음 감사정책의 설명으로 가장 적절하지 않은 것은?

① 로그인 이벤트 감사: 시스템 액세스 제어 목록(SACL)이 지정되어 있는 액티브 디렉터리(Active Directory) 개체에 접근하는 사용자에 대한 감사 로그를 제공한다.

② 권한 사용 감사: 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.

③ 계정 관리 감사: 신규 사용자, 그룹의 추가, 기존 사용자 그룹의 변경, 사용자의 활성화나 비활성화, 계정 패스워드 변경 등을 감사한다.

④ 정책 변경 감사: 사용자 권한 할당 정책, 감사 정책 또는 신뢰 정책의 변경과 관련된 사항을 로깅한다.

정답 1번

간단한 해설

SACL이 설정된 Active Directory 개체에 대한 접근은 **디렉터리 서비스 액세스 감사**의 대상이다. 이를 로그인 이벤트 감사라고 한 ①이 적절하지 않다.

선지별 해설

① X: SACL이 설정된 Active Directory 개체에 대한 접근은 **디렉터리 서비스 액세스 감사**에 해당한다. 로그인 이벤트 감사는 컴퓨터에 로그인하거나 로그오프하는 활동을 다루므로, 두 감사 범주를 바꾸어 설명한 것이다.

② O: 권한 사용 감사는 사용자가 **특권을 실제로 행사하는 행위**를 감사한다. 예를 들어 개체의 소유권을 가져오거나 개체별 감사 설정을 지정할 때 사용하는 특권이 해당할 수 있다. 이 선지의 권한 설정 변경은 이러한 특권 사용을 수반하는 작업이라는 범위에서 이해해야 한다. **사용자 권한 할당 정책 자체의 변경**은 ④의 정책 변경 감사에 속하며, 모든 관리자 작업이나 모든 권한 변경이 이 범주에서 자동으로 기록되는 것은 아니다.

③ O: 계정 관리 감사는 사용자·그룹의 생성 및 변경, 계정의 활성화·비활성화, 암호 변경 등 **계정과 그룹의 관리 활동**을 대상으로 한다. 단순 로그인 활동이나 개체 접근 감사와 구별한다.

④ O: 정책 변경 감사는 **사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경** 등을 다룬다. 권한을 누구에게 부여하거나 회수할지를 정하는 정책을 바꾸는 것과, 이미 부여받은 특권을 실제 작업에서 사용하는 것은 구별해야 한다.

NoteBase