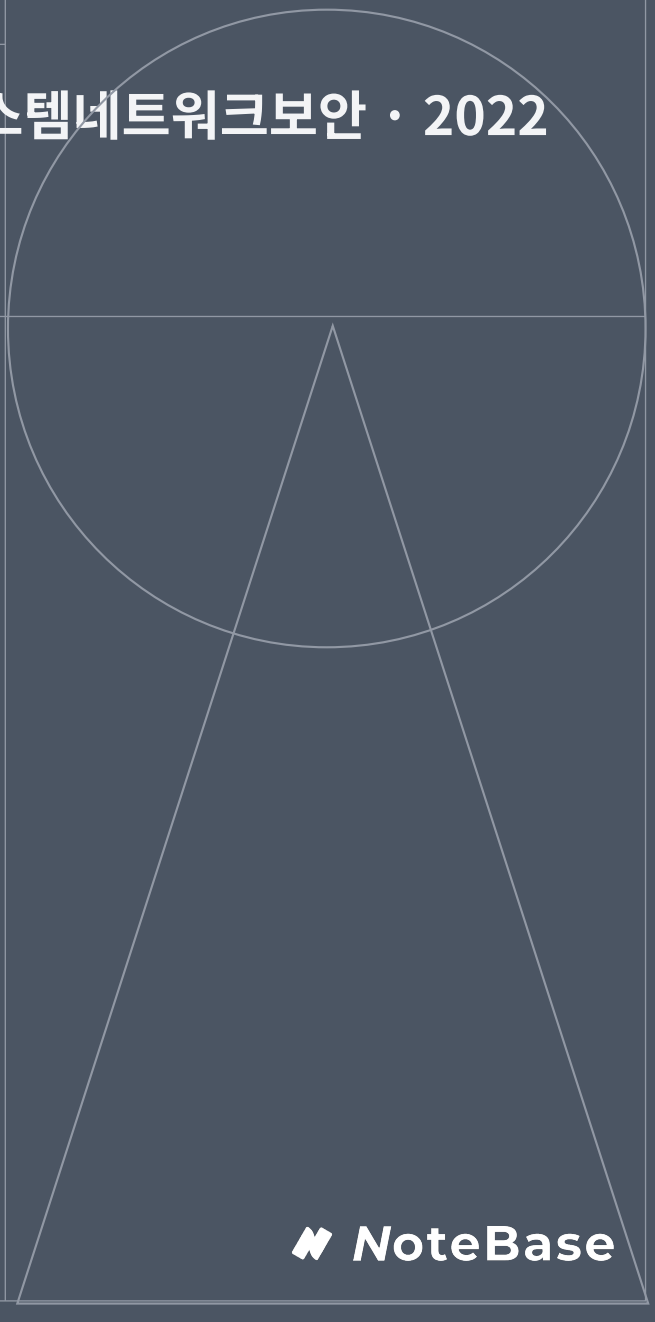
기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2022



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2022

공무원/경찰/경력채용 · 시스템네트워크보안 · 2022

문 1. 윈도우 10에서 부팅 시마다 모든 계정을 대상으로 악성코드 구동을 위해 사용될 수 있는 레지스트리의 위치로 가장 적절한 것은?

① HKLM\Software\Microsoft\Windows NT\CurrentVersion

② HKLM\Software\Microsoft\Windows\CurrentVersion\Run

③ HKCU\Software\Microsoft\Windows\CurrentVersion\Uninstall

④ HKCU\Software\Microsoft\Windows\CurrentVersion\Explore\RunMRU

정답 2번

간단한 해설

모든 사용자에게 적용되는 로그인 자동 실행 위치는 **HKLM 아래의 CurrentVersion\Run**이다. HKCU는 현재 사용자 범위이므로 제시된 조건에는 ②가 맞는다.

핵심 풀이

핵심은 **적용 범위와 자동 실행 기능**이다. HKLM은 컴퓨터 전체에 적용되는 설정 영역이고, HKCU는 현재 사용자에 해당하는 설정 영역이다. 모든 계정을 대상으로 하는 항목은 HKLM 쪽에서 찾는다.

②의 HKLM\Software\Microsoft\Windows\CurrentVersion\Run은 **사용자 로그인 때 반복적으로 실행할 프로그램**을 지정하는 위치이다. 따라서 제시된 위치 중 컴퓨터 전체에 적용되는 자동 실행 항목이라는 조건에 맞는다. 문제의 부팅 시마다는 부팅 후 로그인 과정의 자동 실행이라는 뜻으로 이해해야 하며, Run 항목이 로그인 전의 부팅 단계에서 항상 실행된다는 뜻은 아니다.

①의 Windows NT\CurrentVersion은 Windows 버전 등 시스템 정보를 포함하는 위치로, 제시된 경로 자체가 반복 자동 실행용 Run 키는 아니다.

③의 Uninstall은 프로그램 제거 관련 정보와 연결된다.

④의 RunMRU는 실행 대화상자의 최근 입력 기록과 관련된 이름으로, **기록의 존재와 자동 실행 설정**을 혼동하면 안 된다.

NoteBase

문 2. 다음에서 설명하는 HTTP 요청 방식으로 가장 적절한 것은?

· 클라이언트에서 서버로 전송될 자료를 URL에 입력 파라미터로 넣어서 요청하기 때문에 패스워드와 같은 보안 정보를 전송하는 것은 위험할 수 있다.
· 많은 데이터를 전송하는 경우 일정 크기에서 잘릴 수 있다.

① GET 방식

② PUT 방식

③ POST 방식

④ DELETE 방식

정답 1번

간단한 해설

웹 폼에서 **입력값을 URL에 붙여 전달**하는 대표적인 요청 방식은 GET이다. URL에 민감한 값이 남을 수 있고 구현별 길이 제한도 있으므로 패스워드나 대량 자료 전송에는 적절하지 않다.

핵심 풀이

핵심 단서는 **입력값을 URL의 질의 문자열에 넣어 요청**한다는 점이다. 웹 폼의 GET 전송은 입력값을 이름과 값의 형태로 URL에 붙이는 대표적인 방식이므로, 제시된 설명은 ① GET 방식에 해당한다. GET의 기본 의미는 대상 자원의 표현을 조회하는 것이다.

URL에 패스워드를 넣으면 브라우저 방문 기록이나 서버·중간 시스템의 로그 등에 남을 수 있다. HTTPS로 통신 구간을 암호화하더라도 URL이 각 끝점의 기록에 저장될 위험까지 없어지는 것은 아니므로, 민감한 정보를 URL로 전달하지 않아야 한다.

많은 데이터가 잘릴 수 있다는 설명은 **브라우저·서버 등의 URL 길이 제한**을 가리킨다. 모든 환경에 동일한 고정 길이가 정해진 것은 아니며, 제한을 넘으면 요청 거절 등으로 처리될 수도 있으므로 GET이 언제나 일정 길이에서 잘린다고 일반화하지 않는다.

POST는 보통 제출 데이터를 요청 본문으로 전달하며, PUT은 지정한 대상 자원을 생성·대체하고 DELETE는 대상 자원과의 연결을 제거하도록 요청하는 데 쓰인다. 본문으로 보낸다는 것만으로 기밀성이 보장되지는 않으며, POST에서도 HTTPS 등 별도의 보안 보호가 필요하다.

NoteBase

문 3. 서브넷 마스크가 255.255.255.240인 경우 연결 가능한 호스트 수는?

① 14

② 16

③ 30

④ 32

정답 1번

간단한 해설

255.255.255.240은 /28이므로 **호스트 비트가 4개**이다. 네트워크 주소와 브로드캐스트 주소를 제외하면 연결 가능한 호스트 수는 $2^4 - 2 = 14$대이다.

계산 과정

255.255.255.240에서 앞의 세 옥텟은 각각 8개의 1로 이루어져 있고, 마지막 240은 이진수로 11110000이다. 따라서 네트워크 부분은 28비트인 /28이며 **호스트 부분은 4비트**이다.

호스트 부분 4비트로 표현할 수 있는 전체 주소 수는 $2^4 = 16$개이다. 일반적인 IPv4 서브넷에서는 호스트 비트가 모두 0인 네트워크 주소와 모두 1인 브로드캐스트 주소를 호스트에 할당하지 않는다.

따라서 할당 가능한 호스트 수는 $2^4 - 2 = 14$대로, **전체 주소 16개에서 예약 주소 2개를 제외**한다. 이는 ① 14와 일치한다.

NoteBase

문 4. 구글(Google)에서 검색어와 예상되는 실행결과에 대한 설명의 조합으로 가장 적절하지 않은 것은?

① 검색어: “경찰공무원 시험” -“채용”, 설명: “경찰공무원 시험”과 “채용” 두 키워드를 포함하는 조건으로 검색하여 출력

② 검색어: “경찰공무원 시험” site:www.police.go.kr, 설명: www.police.go.kr에서 “경찰공무원 시험” 키워드로 검색하여 출력

③ 검색어: “경찰공무원 채용” filetype:pdf, 설명: “경찰공무원 채용” 키워드가 포함된 pdf 파일형식을 검색하여 출력

④ 검색어: “경찰공무원 채용” intitle:공채, 설명: “경찰공무원 채용” 키워드와 웹 페이지 타이틀이 “공채” 문자열이 포함된 것으로 검색하여 출력

정답 1번

간단한 해설

검색어 앞의 **빼기 기호(-)는 제외 조건**이다. 따라서 -“채용”은 “채용”까지 포함하라는 뜻이 아니라 해당 표현을 제외하라는 뜻이다.

선지별 해설

① X: 검색어 앞의 빼기 기호(-)는 해당 단어나 구문을 **검색 결과에서 제외**하는 조건이다. 따라서 “경찰공무원 시험”을 찾되 “채용”을 제외하라는 뜻이며, 두 키워드를 모두 포함하라는 뜻이 아니다.

② O: site:는 검색 범위를 **지정한 사이트**로 제한한다. 여기에 큰따옴표로 묶은 “경찰공무원 시험”을 함께 지정하면 그 사이트 안에서 해당 구문을 찾는 조건이 된다.

③ O: filetype:pdf는 검색 결과의 **파일 형식을 PDF로 제한**한다. 따라서 “경찰공무원 채용” 구문 조건과 PDF 형식 조건을 함께 적용한다.

④ O: intitle:공채는 웹 문서의 **제목에 공채가 포함**되는 조건이다. “경찰공무원 채용” 구문 검색 조건도 함께 적용되지만, 그 구문 전체가 반드시 제목에 있어야 한다는 뜻은 아니다.

NoteBase

문 5. DHCP(Dynamic Host Configuration Protocol)에 관한 설명으로 가장 적절하지 않은 것은?

① 기본적으로 67, 68번 포트를 사용한다.

② MAC 주소에 IP 주소를 고정·할당하는 방법을 사용할 수 있다.

③ DHCP 서버에서 클라이언트에게 IP 주소를 자동으로 제공해 준다.

④ IP 주소 풀(pool)에서 가용한 IP 주소를 선택하여 클라이언트에게 영구적으로 해당 주소를 할당한다.

정답 4번

간단한 해설

DHCP의 일반적인 **동적 할당은 임대 기간**을 두고 IP 주소를 제공하므로 이를 무조건 영구 할당이라고 설명하면 부정확하다. 다만 DHCP 자체는 예약이나 영구 주소를 제공하는 할당 방식도 지원한다.

선지별 해설

① O. 문항의 DHCPv4는 **UDP 67번을 서버 포트, UDP 68번을 클라이언트 포트**로 사용한다. 클라이언트의 요청은 서버 포트로, 서버의 응답은 클라이언트 포트로 전달된다.

② O. DHCP 서버에 클라이언트의 **MAC 주소와 특정 IP 주소를 대응시키는 예약**을 설정하여 같은 주소를 제공할 수 있다. 따라서 DHCP를 사용한다고 해서 매번 다른 주소가 할당되어야 하는 것은 아니다.

③ O. DHCP 서버는 클라이언트에게 **IP 주소와 네트워크 설정 정보를 자동으로 제공**할 수 있다. 관리자가 각 단말에서 주소를 직접 입력하는 부담을 줄이는 역할을 한다.

④ X. 일반적인 **동적 주소 풀 할당**을 설명하면서 주소가 영구적으로 할당된다고 단정한 점이 적절하지 않다. 동적 할당은 주소를 임대 기간 동안 사용하게 하며, 계속 사용하려면 갱신이 필요하다. 다만 DHCP 표준에는 영구 주소를 주는 자동 할당과 관리자가 주소를 정하는 수동 할당도 있으므로, ‘DHCP는 영구 할당을 전혀 지원하지 않는다’는 뜻은 아니다. 이 문항에서는 일반적인 동적 임대 방식을 기준으로 구분한다.

따라서 일반적인 동적 할당의 설명으로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 6. 다음에서 설명하는 용어로 가장 적절한 것은?

인터넷 사이트에서 신규 회원 등록 시, 사용자가 컴퓨터인지 사람인지를 구별하기 위해 질문을 던져 응답을 확인하는 인증 방식으로, 텍스트나 숫자 등을 컴퓨터가 스스로 해독하기 어렵게 보여주는 방식을 활용한다.

① keypair
② webaholism
③ CAPTCHA
④ typosquatting

정답 3번

간단한 해설

왜곡된 문자나 숫자 등을 이용해 **사람과 자동화된 프로그램을 구별**하려는 장치는 CAPTCHA이다. 따라서 ③이 적절하다.

핵심 풀이

설명의 핵심은 **사람과 자동화된 프로그램을 구별하기 위한 과제**이다. CAPTCHA는 사람은 비교적 쉽게 처리하지만 프로그램은 처리하기 어렵도록 설계한 문제를 제시하여 자동화된 가입이나 요청을 제한하는 데 사용된다. 왜곡된 문자·숫자를 읽게 하는 방식은 전통적인 CAPTCHA의 대표적인 예이다.

따라서 제시된 용어 중에서는 ③ **CAPTCHA**가 맞는다. 이는 이용자가 주장하는 특정 신원을 증명하는 일반적인 계정 인증과 달리, 요청이 사람에게서 왔는지를 판별하려는 장치이다. 모든 CAPTCHA가 문자 입력 방식인 것은 아니며, 자동화 프로그램을 완벽하게 차단한다는 뜻도 아니다.

keypair는 공개키와 개인키처럼 서로 대응하는 암호키 쌍을 뜻한다.

webaholism은 과도한 웹 이용이나 인터넷 중독과 관련된 용어이다.

typosquatting은 사용자의 도메인 입력 오타를 노려 유사 도메인을 이용하는 행위를 뜻하므로, 사람과 프로그램을 구별하는 과제를 가리키지 않는다.

NoteBase

문 8. HTTP에서 클라이언트 상태정보 유지 방식에 관한 설명으로 가장 적절하지 않은 것은?

① 세션 방식은 개별 클라이언트 상태정보를 서버에 저장하는 기술이다.

② 세션 방식은 웹 브라우저를 일정 시간 이상 사용하지 않으면 연결이 종료될 수 있다.

③ 쿠키 방식은 로그온 정보, 방문기록, 방문횟수 등의 정보를 저장하고, 유효기간이 지정되면 만료시간 이후에 자동 삭제된다.

④ 쿠키 방식은 클라이언트 상태정보를 클라이언트에 저장하고 HTTP의 요청과 응답을 헤더에 포함하여 전송하기 때문에 해킹과 스니핑 공격에 안전하다.

정답 4번

간단한 해설

쿠키가 HTTP 헤더로 전달된다고 해서 **자동으로 암호화되거나 도청을 막는 것은 아니다**. 서버 측 세션도 세션 식별자를 쿠키로 주고받을 수 있으므로 식별자의 노출을 방지해야 한다.

선지별 해설

① O. 전통적인 서버 측 세션 방식은 **사용자별 상태정보를 서버에 저장**하고 세션 식별자로 구분한다. 클라이언트는 보통 세션 식별자를 쿠키 등으로 전달하므로, 세션과 쿠키는 서로 함께 사용될 수 있다.

② O. 서버에 유휴 시간 제한이 설정되어 있으면 일정 시간 동안 유효한 요청이 없는 세션은 만료될 수 있다. 여기서 연결 종료는 로그인 상태 등 논리적 세션의 종료를 뜻하며, 브라우저 프로그램이나 물리적인 네트워크 연결이 반드시 종료된다는 의미는 아니다.

③ O. 쿠키는 브라우저에 상태를 나타내는 값을 저장하여 로그인 상태 식별이나 방문 정보 관리 등에 사용할 수 있다. 만료 시각이나 최대 수명이 지정된 쿠키는 해당 시점 이후 만료·삭제되어 전송 대상에서 제외된다. 로그인 정보를 저장한다는 것이 비밀번호 원문을 저장하라는 뜻은 아니다.

④ X. 쿠키는 응답의 Set-Cookie 헤더로 설정되고 요청의 Cookie 헤더로 전달되지만, **헤더에 들어간다는 사실만으로 암호화되지는 않는다**. 평문 HTTP에서는 도청될 수 있고 탈취된 세션 쿠키는 세션 도용에 악용될 수 있다. 따라서 해킹·스니핑에 안전하다는 결론이 틀리며, HTTPS와 적절한 쿠키 보안 속성 등 별도 보호가 필요하다.

NoteBase

문 9. UNIX에 대한 설명으로 가장 적절하지 않은 것은?

① 커널은 프로세스 관리, 기억장치 관리, 입·출력 관리 등의 기능을 수행한다.

② 시분할 시스템을 위해 설계된 대화식 운영체제로서 다중 사용자 시스템이다.

③ 쉘은 운영체제와 사용자 간의 인터페이스를 제공하는 부분으로 명령어를 입력받아 해석해 주는 명령어 해석기이다.

④ 파일 시스템의 구조에서 데이터 블록은 전체 파일 시스템에 대한 정보를 저장하고 i-node 블록은 실제 데이터가 파일의 형태로 저장된다.

정답 4번

간단한 해설

파일 시스템 전체의 관리 정보는 **슈퍼블록**, 개별 파일의 속성과 위치 정보는 i-node, 실제 파일 내용은 데이터 블록에 저장된다. 이 세 영역의 역할을 구별해야 한다.

선지별 해설

① O: 커널은 운영체제의 핵심으로서 프로세스 실행과 CPU 배분, 메모리 할당, 장치 입·출력 등을 관리한다. 사용자 프로그램이 하드웨어 자원을 이용할 때 필요한 **자원 관리와 보호**를 담당한다.

② O: UNIX는 여러 사용자가 함께 사용하는 시분할 환경을 전제로 발전한 대화식 운영체제이다. CPU 시간을 나누어 여러 작업을 실행하므로 각 사용자는 시스템과 상호작용하며 작업할 수 있다.

③ O: 쉘은 사용자가 입력한 명령을 해석하고 프로그램 실행 등을 요청하는 **명령어 해석기**이다. 사용자와 운영체제 사이의 인터페이스를 제공하지만, 커널 자체와 동일한 구성 요소는 아니다.

④ X: 전통적인 UNIX 파일 시스템에서 전체 파일 시스템의 크기나 관리 정보는 **슈퍼블록**에 저장된다. i-node에는 파일의 소유자·권한·크기·시간 및 데이터 블록 위치 같은 메타데이터가 저장되고, **실제 파일 내용은 데이터 블록**에 저장된다. 데이터 블록과 i-node의 역할을 잘못 연결한 ④가 가장 적절하지 않다.

NoteBase

문 10. 루프백 주소(loopback address)에 관한 설명으로 가장 적절한 것은?

① 같은 호스트 상에서 서버·클라이언트 프로그램의 서버 주소로 사용할 수 없다.

② 자기 자신을 나타내는 IP 주소로 127.0.0.1은 루프백 주소로 사용할 수 있다.

③ LAN에 연결된 기기에 할당되는 IP 주소로서 인터넷상에서는 사용할 수 없다.

④ 그룹을 구분하기 위한 식별자로써 동일한 네트워크에 연결된 모든 호스트에 대한 통신이 가능하다.

정답 2번

간단한 해설

루프백 주소는 **자기 호스트 내부로 통신을 되돌리는 주소**이다. 127.0.0.1을 이용하면 같은 호스트 안의 서버·클라이언트가 통신할 수 있다.

선지별 해설

① X: 루프백 주소는 **같은 호스트 내부의 서버·클라이언트 통신**에 사용할 수 있다. 서버가 루프백 주소에서 수신하도록 설정되면 같은 호스트의 클라이언트가 그 주소로 접속할 수 있으므로, 사용할 수 없다는 설명은 반대이다.

② O: 루프백 주소는 통신을 **자기 호스트 내부로 되돌리는 주소**이다. IPv4의 127.0.0.1이 대표적이며, 127.0.0.0/8 대역이 루프백 용도로 예약되어 있다.

③ X: 루프백 주소는 LAN의 다른 기기에 도달하기 위해 할당하는 주소가 아니라 **자기 호스트 내부용**이다. 사설 주소는 LAN 내부의 서로 다른 장치가 통신하는 데 사용할 수 있지만, 루프백은 그와 용도가 다르다.

④ X: 루프백 주소는 다른 호스트 집단이나 네트워크 전체를 나타내지 않는다. 특정 그룹으로 보내는 것은 **멀티캐스트**, 동일 브로드캐스트 영역의 모든 호스트로 보내는 것은 **브로드캐스트**와 구별하여 이해해야 한다.

NoteBase

문 11. UNIX에서 퍼미션(permission)에 관한 설명 중 가장 적절하지 않은 것은?

① SetUID가 설정된 파일은 모두 해킹 대상이 될 수 있다.

② 파일의 권한이 rw-r-sr-x로 설정된 경우 파일 소유자가 속한 그룹의 권한으로 실행된다.

③ 소유자가 root인 파일의 권한이 rwsr-xr-x로 설정된 경우 root 권한으로 실행된다.

④ Sticky bit가 설정('t')된 디렉터리에서는 root만 파일을 삭제할 수 있다.

정답 4번

간단한 해설

Sticky bit가 설정된 디렉터리에서도 **파일 소유자와 디렉터리 소유자** 등은 필요한 권한이 있으면 파일을 삭제할 수 있다. 따라서 root만 삭제할 수 있다는 ④가 틀렸다.

선지별 해설

① O: SetUID가 적용되는 실행 파일은 실행한 사용자가 아니라 **파일 소유자의 유효 사용자 ID**로 동작할 수 있어, 취약점이 있으면 권한 상승에 악용될 위험이 있다. 따라서 보안 점검 대상이 된다. 다만 SetUID가 있다는 사실만으로 모든 파일에 취약점이 있거나 반드시 침해된다는 뜻은 아니다.

② O: rw-r-sr-x에서 그룹 실행 권한 위치의 s는 **SetGID와 그룹 실행 권한**이 함께 설정되어 있음을 나타낸다. 실행이 허용되고 SetGID가 적용되는 경우 파일의 소유 그룹 ID를 유효 그룹 ID로 사용한다. 정확한 기준은 파일 소유 사용자의 현재 기본 그룹이 아니라 **해당 파일에 기록된 소유 그룹**이다.

③ O: rwsr-xr-x에서 소유자 실행 권한 위치의 s는 **SetUID와 소유자 실행 권한**이 함께 설정되었음을 뜻한다. 파일 소유자가 root라면 정상적으로 SetUID가 적용되는 실행에서 유효 사용자 ID가 root가 된다. 파일 시스템의 nosuid 설정 등으로 특수 비트의 적용이 제한되는 경우는 별도이다.

④ X: Sticky bit가 있는 디렉터리에서는 root만 삭제할 수 있는 것이 아니다. 필요한 디렉터리 접근 권한이 있다는 전제에서 **해당 파일 소유자나 디렉터리 소유자**, 또는 적절한 특권을 가진 사용자가 파일을 삭제할 수 있다. 여러 사용자가 함께 쓰는 디렉터리에서 다른 사용자의 파일을 함부로 삭제하지 못하게 제한하는 기능이다.

NoteBase

문 12. RIP(Routing Information Protocol)에 관한 설명으로 가장 적절한 것은?

① 대규모 네트워크 환경에 적합하다.

② 거리 벡터(distance vector) 라우팅 프로토콜이다.

③ 지연, 대역폭, 회선속도 정보를 라우팅에 반영한다.

④ 최대 16홉까지 가능하다.

정답 2번

간단한 해설

RIP는 **홉 수를 기본 척도로 사용하는 거리 벡터 라우팅 프로토콜**이다. 유효한 경로는 최대 15홉이며 16은 도달 불가를 뜻한다.

선지별 해설

① X. RIP는 **유효한 경로의 최대 홉 수가 15**로 제한되고 네트워크 변화에 대한 수렴이 느린 편이므로 대규모 네트워크보다는 소규모 네트워크에 적합하다. 대규모 환경에 적합하다는 설명은 이러한 확장성 한계를 반대로 설명한 것이다.

② O. RIP는 이웃 라우터와 목적지까지의 거리 정보를 교환하는 **거리 벡터 라우팅 프로토콜**이다. 이웃에게 받은 경로 정보와 비용을 바탕으로 자신의 라우팅 정보를 갱신한다.

③ X. RIP의 기본 경로 선택 척도는 **홉 수**이며, 지연·대역폭·회선속도를 직접 반영하는 복합 척도를 사용하지 않는다. 따라서 빠른 회선인지보다 경유하는 라우터 수가 경로 선택의 기준이 된다.

④ X. RIP에서 도달 가능한 경로의 최대 홉 수는 **15**이고, **16은 도달 불가를 나타내는 값**이다. 16을 정상적으로 사용할 수 있는 최대 홉 수로 해석하면 안 된다.

따라서 RIP에 대한 설명으로 가장 적절한 것은 ②이다.

NoteBase

문 13. 무선랜 통신의 암호화 기술에 관한 설명으로 가장 적절한 것은?

① WEP는 암호화 키와 함께 128bit IV(Initial Vector)를 사용한다.

② WEP는 공유키와 난수 발생기를 이용하여 키스트림을 생성하고 AND 연산을 통하여 암호문을 생성한다.

③ WPA-PSK에서 WPA-1은 TKIP, WPA-2는 CCMP 암호화 방식을 사용한다.

④ 802.1x/EAP에서 802.1x는 무선랜 클라이언트와 RADIUS 서버 간의 통신 프로토콜이다.

정답 3번

간단한 해설

대표적인 데이터 보호 방식은 **WPA1의 TKIP와 WPA2의 AES 기반 CCMP**이다. WEP의 IV는 24비트이고 암호문 생성에는 AND가 아니라 XOR를 사용한다.

선지별 해설

① X. WEP의 초기화 벡터 IV는 **24비트**이다. 흔히 128비트 WEP라고 부르는 구성은 104비트 비밀키와 24비트 IV를 합친 크기이며, IV 자체가 128비트인 것은 아니다.

② X. WEP는 공유 비밀키와 IV를 이용해 RC4 키스트림을 만들고, 평문 및 무결성 검사값에 **XOR 연산**을 적용하여 암호문을 생성한다. AND 연산이라는 부분이 틀리다. XOR는 같은 키스트림을 다시 적용하면 원래 값을 복원할 수 있다.

③ O. 기본적인 세대별 대응은 **WPA1–TKIP, WPA2–AES 기반 CCMP**이다. PSK는 사전 공유키를 사용하는 인증·키 관리 방식의 구분이며, TKIP·CCMP는 데이터 보호 방식의 구분이다. 혼합·호환 설정의 존재와 별개로 이 문제는 각 세대의 대표 방식을 묻는다.

④ X. IEEE 802.1X는 포트 기반 네트워크 접근 제어 체계이다. 무선 클라이언트와 인증 장치인 AP 사이에서는 EAPOL로 EAP 메시지를 전달하고, AP 등 인증 장치와 백엔드 인증 서버 사이에서는 보통 RADIUS로 이를 전달한다. 따라서 클라이언트와 RADIUS 서버 사이의 통신 프로토콜을 단순히 802.1X라고 설명하는 것은 구간별 역할을 혼동한 것이다.

NoteBase

문 14. 프러미스큐어스(promiscuous) 모드를 사용하는 스니핑(sniffing) 공격의 탐지 방법에 관한 설명으로 가장 적절하지 않은 것은?

① 네트워크에 존재하지 않는 MAC 주소를 이용하여 의심이 가는 호스트에 ping을 보낸다.

② 테스트 대상 네트워크로 ping sweep을 보내고 들어오는 forward-DNS lookup을 감시한다.

③ 네트워크에 존재하지 않는 IP 주소를 이용하여 ARP request를 보낸다.

④ MAC 주소와 IP 주소의 매핑(mapping) 초기값을 저장하고 ARP 트래픽을 모니터링한다.

정답 2번

간단한 해설

스니퍼가 수집한 IP 주소의 호스트 이름을 확인할 때 발생하는 것은 **역방향 DNS 조회**이다. 따라서 forward-DNS가 아니라 reverse-DNS lookup을 감시한다.

선지별 해설

① O: 목적지 IP는 의심 호스트로 두되 **목적지 MAC 주소를 존재하지 않는 값**으로 지정한 ping을 보내는 탐지 방법이다. 정상적인 MAC 필터링이라면 버릴 프레임을 수신·처리하여 응답하는지를 관찰한다. 다만 운영체제의 추가 필터링 등에 따라 응답하지 않을 수 있으므로 탐지를 보장하지는 않는다.

② X: 일부 스니퍼는 수집한 IP 주소를 호스트 이름으로 바꾸기 위해 **역방향 DNS 조회**를 수행한다. 따라서 ping sweep으로 유인 트래픽을 만든 뒤 감시할 것은 reverse-DNS lookup이다. 이름에서 IP 주소를 찾는 forward-DNS lookup으로 제시한 ②가 가장 적절하지 않다.

③ O: 존재하지 않는 IP 주소를 담은 ARP 요청을 유인 자료로 보내고, 그 주소에 대한 역방향 DNS 조회 같은 스니퍼의 부수 동작을 관찰할 수 있다. 이는 **없는 IP에도 모든 스니퍼가 ARP 응답을 한다는 뜻은 아니다**. 주소 해석을 하지 않는 수동 스니퍼는 이러한 반응을 보이지 않을 수 있다.

④ O: 초기 IP·MAC 대응과 이후 ARP 트래픽을 비교하면 주소 대응의 비정상적인 변화를 발견할 수 있다. 이는 **ARP 스푸핑을 이용한 트래픽 가로채기**의 단서를 찾는 방법이며, 프러미스큐어스 모드 자체나 모든 수동 스니핑을 직접 검출하는 방법은 아니다.

NoteBase

문 15. ping 명령에 관한 설명 중 가장 적절하지 않은 것은?

① ICMPv4(Type 2)를 이용하는 유틸리티이다.

② 원격 호스트까지의 네트워크 속도를 측정할 수 있다.

③ 원격 호스트의 운영체제를 구분할 수 있다.

④ 원격 호스트까지의 라우터 수를 알 수 있다.

정답 1번

간단한 해설

IPv4 ping의 기본 메시지는 **Echo Request Type 8과 Echo Reply Type 0**이다. Type 2를 사용한다는 설명은 이에 맞지 않는다.

선지별 해설

① X: IPv4의 ping은 ICMP **Echo Request(Type 8)**를 보내고 **Echo Reply(Type 0)**를 받는 방식으로 동작한다. 따라서 사용하는 메시지 유형을 Type 2라고 한 설명이 명백히 잘못되었다.

② O: ping은 요청과 응답 사이의 **왕복 시간(RTT)**을 측정하여 원격 호스트와의 응답 속도와 지연 상태를 살펴볼 수 있다. 다만 이는 전송 대역폭이나 실제 파일 다운로드 처리량을 직접 측정한다는 뜻은 아니다.

③ O: 응답 패킷의 TTL 등은 운영체제 계열을 **추정하는 단서**로 활용될 수 있다. 그러나 초기 TTL은 변경할 수 있고 여러 운영체제가 같은 값을 사용할 수 있으므로, ping 결과만으로 운영체제를 확정할 수는 없다.

④ O: 응답의 초기 TTL을 알고 있다면 수신 TTL과의 차이로 해당 경로의 **경유 홉 수를 추정**할 수 있다. 초기값을 모르면 확정하기 어렵고 왕복 경로가 다를 수도 있다. 라우터별 경로를 직접 조사하려면 traceroute나 tracert가 더 적합하다.

NoteBase

문 16. hosts 파일에 관한 설명으로 가장 적절하지 않은 것은?

① 시스템에 등록된 DNS 서버가 다운되더라도 hosts 파일에 등록된 사이트에 접속할 수 있다.

② hosts 파일에 등록된 닉네임(임의의 명칭)으로 사이트에 접속할 수 있다.

③ DNS 스푸핑(spoofing) 공격을 회피하기 위하여 hosts 파일을 이용할 수 있다.

④ 윈도우 10에서는 '운영체제 설치 디렉터리\System\drivers\etc\hosts'에 있다.

정답 4번

간단한 해설

hosts 파일은 호스트 이름과 IP 주소를 로컬에서 대응시키는 파일이다. Windows 10의 기본 경로에는 **System이 아니라 System32**가 들어간다.

선지별 해설

① O. hosts 파일은 **호스트 이름과 IP 주소의 대응을 로컬에 저장**한다. 올바른 주소가 등록되어 있고 해당 파일을 이용해 이름을 해석하면 DNS 서버가 응답하지 않아도 목적지 주소를 얻을 수 있다. 다만 실제 접속에는 네트워크와 서버가 정상 동작해야 한다.

② O. hosts 파일에 호스트 이름이나 **별칭을 IP 주소와 연결**해 등록하면 그 이름을 이용해 해당 주소를 찾을 수 있다. 다만 이름 해석이 가능하다는 뜻이며, 웹 서버의 호스트 이름 설정이나 HTTPS 인증서가 임의의 별칭까지 자동으로 지원하는 것은 아니다.

③ O. 신뢰할 수 있는 IP 주소를 hosts 파일에 등록해 로컬 매핑으로 이름을 해석하면 **위조된 DNS 응답에 의존하지 않도록** 할 수 있다. 이는 해당 이름에 대한 DNS 스푸핑 회피 수단이며, hosts 파일 자체의 변조나 모든 종류의 공격을 막는다는 의미는 아니다.

④ X. Windows 10의 기본 경로는 **운영체제 설치 디렉터리\System32\drivers\etc\hosts**이다. 일반적인 설치에서는 C:\Windows\System32\drivers\etc\hosts이며, 선지의 System이 아니라 System32가 들어가야 한다.

따라서 hosts 파일에 대한 설명으로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 17. UNIX에서 TCP Wrapper에 관한 설명으로 가장 적절하지 않은 것은?

① IP 주소와 포트번호에 기반한 접근통제가 가능하다.

② tcpd는 hosts.allow 및 hosts.deny 파일을 참조하여 접근통제를 수행한다.

③ SSH, FTP 서비스에 대한 접근통제가 가능하다.

④ 네트워크 접속에 대한 로그 생성이 가능하다.

정답 1번

간단한 해설

TCP Wrapper는 **서비스 데몬과 클라이언트 호스트 정보**를 기준으로 접근을 제어한다. 포트번호를 직접 조건으로 사용하는 패킷 필터 방식과 혼동한 ①이 적절하지 않다.

선지별 해설

① X: TCP Wrapper의 기본 접근통제 규칙은 **서비스 데몬 이름과 접속 클라이언트의 호스트명·IP 주소** 등을 대응시킨다. 패킷 필터 방화벽처럼 포트번호를 직접 조건으로 지정하는 방식이 아니므로, IP 주소와 포트번호를 기준으로 한다는 설명은 적절하지 않다. 서비스가 특정 포트를 사용한다는 사실과 규칙이 포트번호를 직접 검사한다는 것은 구별해야 한다.

② O: 전통적인 TCP Wrapper의 tcpd는 **hosts.allow와 hosts.deny**의 접근통제 규칙을 이용한다. 일반적으로 허용 목록과 먼저 일치하면 허용하고, 그렇지 않으면 거부 목록을 확인하며, 어느 쪽에도 일치하지 않으면 허용한다.

③ O: TCP Wrapper를 지원하도록 연동된 SSH·FTP 등의 서비스는 **데몬 단위로 접근통제**할 수 있다. 모든 구현이나 버전에서 지원되는 것은 아니다. 예를 들어 OpenSSH는 6.7에서 tcpwrappers/libwrap 지원을 제거했으므로, 이 설명을 현대의 모든 SSH 서버에 적용해서는 안 된다.

④ O: TCP Wrapper는 네트워크 서비스 접속에 대해 **접속 기록을 남기는 기능**을 제공한다. 로그를 통해 접속 출처나 서비스 접근을 확인할 수 있으며, 실제 기록 위치와 범위는 시스템의 로깅 설정에 따라 달라진다.

NoteBase

문 18. 전자봉투의 기밀성을 유지하는 방법으로 가장 적절한 것은?

① 송신자가 메시지의 해시값을 전송한다.

② 송신자가 메시지를 송신자의 개인키(비대칭키)로 암호화한다.

③ 송신자가 메시지를 수신자의 공개키(비대칭키)로 암호화한다.

④ 송신자가 메시지를 비밀키(대칭키)로 암호화한다.

정답 4번

간단한 해설

전자봉투에서는 **메시지 본문을 대칭키로 암호화**하고, 그 대칭키를 수신자의 공개키로 보호해 전달한다. 본문과 세션키에 각각 어떤 키를 사용하는지 구별해야 한다.

핵심 풀이

전자봉투는 대칭키 암호와 공개키 암호의 역할을 나누는 혼합 방식이다. **메시지 본문은 대칭키인 세션키로 암호화**하므로, 본문의 기밀성을 유지하는 방법을 묻는 이 문제의 답은 ④이다.

송신자는 본문을 암호화한 뒤 그 세션키를 수신자의 공개키로 암호화하여 함께 보낸다. 수신자는 자신의 개인키로 세션키를 복원하고, 복원한 대칭키로 본문을 복호화한다. 즉 **본문 보호에는 대칭키, 세션키 전달 보호에는 수신자 공개키**를 사용한다.

①의 해시값 전송은 원문을 암호화하지 않으므로 그 자체로 기밀성을 제공하지 않는다.

②의 송신자 개인키를 사용하는 설명은 서명·송신자 확인 쪽 개념과 혼동한 것으로, 수신자만 본문을 읽게 하는 방법이 아니다.

③처럼 수신자 공개키로 데이터를 암호화하는 것은 일반적으로 기밀성 확보에 이용할 수 있다. 다만 이 문제의 전자봉투 구성에서는 공개키로 보호하는 대상이 메시지 본문이 아니라 **본문 암호화에 사용한 세션키**라는 점을 구별해야 한다.

NoteBase

문 20. 아래의 방화벽 패킷 필터링 규칙(㉠~㉣)에 대한 설명으로 가장 적절하지 않은 것은? (단, 방화벽을 기준으로 192.168.1.2는 내부 네트워크에 위치한 서버이고, 10.10.20.3과 10.10.20.4는 외부 네트워크에 위치한 서버이다)

	From	Service	To	Action
㉠	External	25	Internal	Deny
㉡	Any	53	10.10.20.3	Allow
㉢	192.168.1.2	110	Any	Allow
㉣	Internal	143	10.10.20.4	Deny

① ㉠: 외부에서 내부로 SMTP 패킷 전송을 거부한다.

② ㉡: 모든 IP 주소에서 10.10.20.3으로 DNS 패킷 전송을 허용한다.

③ ㉢: 192.168.1.2에서 모든 IP 주소로 POP3S 패킷 전송을 허용한다.

④ ㉣: 내부에서 10.10.20.4로의 IMAP4 패킷 전송을 거부한다.

정답 3번

간단한 해설

표의 **110번은 POP3**의 기본 서비스 포트이며 **POP3S는 995번**을 사용한다. 규칙은 출발지, 서비스, 목적지, 허용·거부 동작을 함께 읽어야 한다.

NoteBase

선지별 해설

① O. ㉠의 출발지 From은 External, 목적지 To는 Internal, Service는 **25번**, Action은 Deny이다. 25번은 SMTP의 기본 서비스 포트이므로 외부에서 내부로 향하는 SMTP 패킷을 거부하는 규칙이다.

② O. ㉡은 From이 Any, To가 10.10.20.3, Service가 **53번**, Action이 Allow이다. 53번은 DNS 서비스 포트이며 Any는 출발지 제한이 없다는 뜻이므로 모든 출발지 IP에서 해당 외부 서버로 향하는 DNS 패킷을 허용한다.

③ X. ㉢은 내부 서버 192.168.1.2에서 모든 목적지로 향하는 **110번 서비스**를 허용한다. 110번은 POP3이고, **POP3S의 기본 포트는 995번**이다. 따라서 출발지·목적지·허용 동작은 맞지만 서비스 이름을 POP3S가 아니라 POP3로 고쳐야 한다.

④ O. ㉣은 From이 Internal, To가 외부 서버 10.10.20.4, Service가 **143번**, Action이 Deny이다. 143번은 IMAP4의 기본 포트이므로 내부에서 해당 서버로 향하는 IMAP4 패킷을 거부한다.

따라서 방화벽 규칙에 대한 설명으로 가장 적절하지 않은 것은 ③이다.

NoteBase