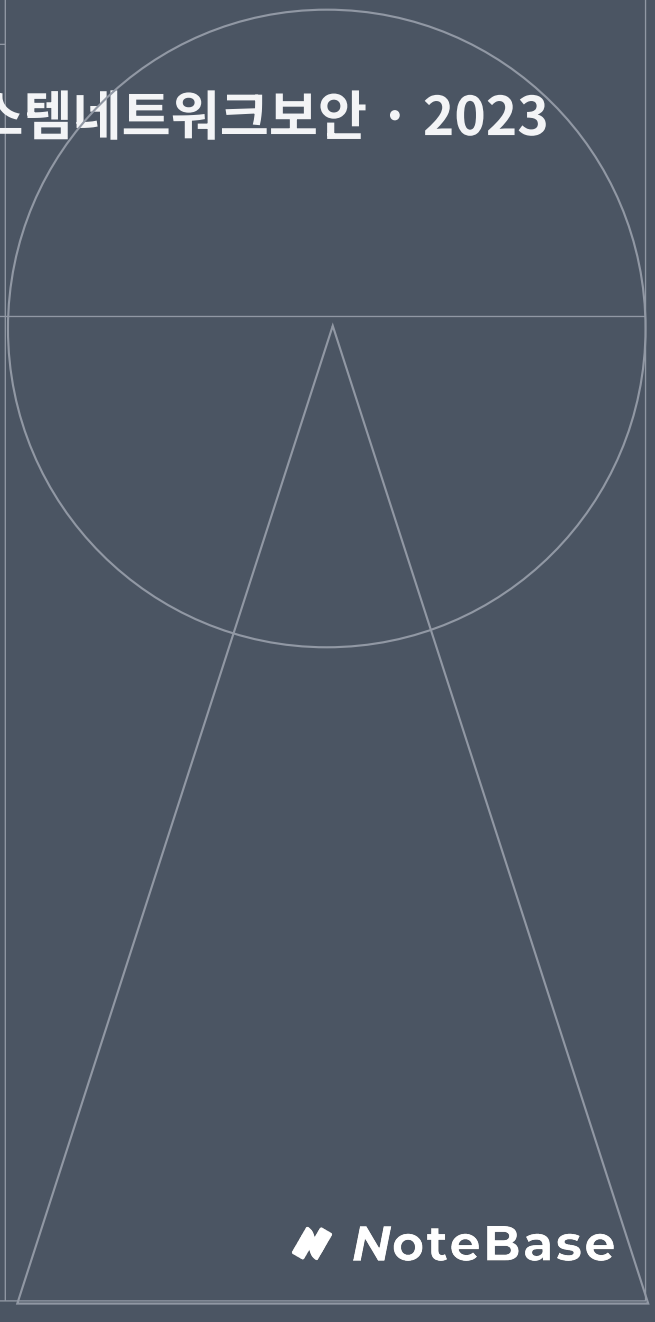
# 기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2023



NoteBase

# 기출OX 해설집

## 공무원/경찰/경력채용 · 시스템네트워크보안 · 2023

### 공무원/경찰/경력채용 · 시스템네트워크보안 · 2023

**문 1. 다음 설명에 해당하는 것으로 가장 적절한 것은?**

라우팅(routing)의 무한루프를 막기 위해 사용되는 것으로 라우터 하나를 지날 때마다 이 값이 1씩 줄어들고 목적지에 도착하기 전에 값이 0이 되면 해당 패킷은 폐기된다.

① HLEN(Header Length)

② TOS(Type Of Service)

③ TTL(Time To Live)

④ TLS(Transport Layer Security)

**정답 3번**

**간단한 해설**

라우터를 지날 때 감소하고 한계에 도달하면 패킷을 폐기하게 하는 값은 **TTL**이다. 이를 통해 잘못된 경로에서 패킷이 무한 순환하는 것을 제한한다.

**개념 구분**

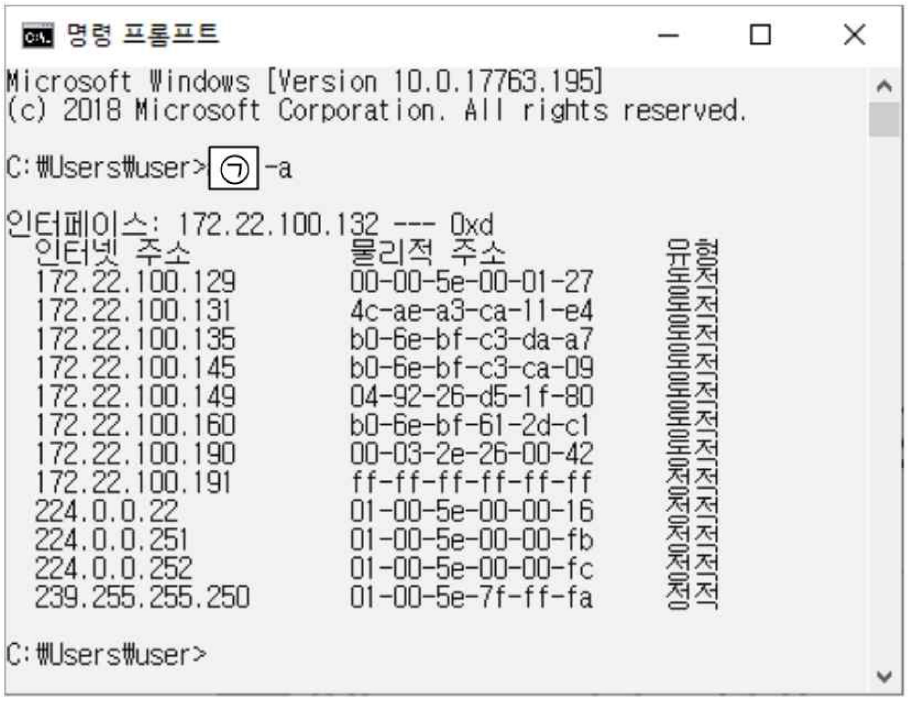
TTL은 IPv4 패킷이 네트워크에서 무한히 순환하지 않도록 전달 범위를 제한하는 필드이다. 라우터가 패킷을 전달할 때 값을 감소시키고, 더 전달할 수 없는 값이 되면 폐기하므로 제시문의 **홉마다 감소·0이면 폐기**라는 조건에 대응한다. 따라서 해당 항목은 ③ TTL이다.

HLEN은 **IPv4 헤더 길이**를 나타내며, TOS는 서비스 특성이나 처리 우선순위와 관련된 필드이다. 두 필드는 라우터를 지날 때마다 수명을 줄이는 카운터가 아니다.

TLS는 통신의 기밀성과 무결성 등을 제공하는 **보안 프로토콜**이다. 이름이 TTL과 비슷해도 패킷의 순환 제한을 위한 IP 헤더 필드가 아니다.

NoteBase

**문 2. 다음 그림은 ㉠의 명령어를 실행한 결과이다. ㉠에 들어갈 명령어로 옳은 것은?**




① netstat

② ipconfig

③ arp

④ ping

**정답 3번**

**간단한 해설**

그림의 **인터넷 주소와 물리적 주소의 대응표**는 ARP 캐시이다. Windows에서 이를 표시하는 명령은 arp -a이다.

NoteBase

**도식 해설**

화면에는 '인터넷 주소', '물리적 주소', '유형'이 나란히 표시되어 있다. 예를 들어 172.22.100.129와 00-00-5e-00-01-27이 한 행에 대응하며 유형은 동적이다. 이는 **IP주소와 MAC주소의 대응을 저장한 ARP 캐시**의 출력이다.

Windows에서 **arp -a**는 현재 ARP 캐시 항목을 표시한다. 그림에서 빈칸 뒤에 -a 옵션이 있고 인터페이스 172.22.100.132에 대한 주소 대응표가 출력되므로, ㉠에 들어갈 명령은 ③ arp이다. 동적·정적 표시는 항목의 유형을 나타낸다.

netstat은 네트워크 연결·수신 대기 포트 등의 상태를, ipconfig는 로컬 인터페이스의 IP 구성 정보를 보여준다. ping은 ICMP 에코 요청과 응답으로 도달 가능성 등을 확인한다. 따라서 여러 IP주소와 물리적 주소의 대응표라는 결정적 단서를 설명하는 명령은 arp이다.

NoteBase

**문 3. IPv6에 관한 설명으로 가장 적절하지 않은 것은?**

① 기본 헤더의 길이는 40바이트이다.

② IPv4의 TTL 필드와 같은 목적으로 Hop Limit를 사용한다.

③ IPv4의 주소 32비트 길이를 4배 확장한 128비트 길이의 주소를 사용한다.

④ Traffic Class 필드는 20비트 길이로 응용서비스에 따라 차별화된 QoS를 제공한다.

**정답 4번**

**간단한 해설**

IPv6에서 **Traffic Class는 8비트, Flow Label은 20비트**이다. Traffic Class를 20비트라고 한 ④가 적절하지 않다.

**선지별 해설**

① O: IPv6의 **기본 헤더는 40바이트로 고정**되어 있다. 확장 헤더가 사용되면 기본 헤더 뒤에 별도로 붙으므로, 기본 헤더 길이와 확장 헤더를 포함한 전체 헤더 길이를 구별해야 한다.

② O: Hop Limit는 패킷이 거칠 수 있는 홉 수를 제한하여 **네트워크에서 무한히 순환하는 것을 방지**한다. 라우터가 패킷을 전달할 때 감소시키며, IPv4의 TTL과 같은 목적을 가진다.

③ O: IPv4 주소는 32비트이고 IPv6 주소는 **128비트**이므로 주소의 비트 길이는 4배이다. 다만 가능한 주소의 개수는 단순히 4배가 아니라, 비트 수 증가에 따라 훨씬 크게 늘어난다.

④ X: IPv6의 **Traffic Class는 8비트**이고, 20비트인 필드는 **Flow Label**이다. Traffic Class는 트래픽의 구분과 차등 처리 등에 사용되며, Flow Label은 같은 흐름에 속하는 패킷을 식별하는 데 사용된다. 두 필드의 길이를 혼동한 설명이다.

NoteBase

**문 4. 패스워드 크래킹(password cracking) 도구로 가장 적절하지 않은 것은?**

① Striker

② John the Ripper

③ Pwdump

④ RainbowCrack

**정답 1번**

**간단한 해설**

Striker의 주된 용도는 **정보 수집과 취약점 탐색**으로, 패스워드 크래킹과 다르다. Pwdump는 직접 암호를 찾기보다 크래킹에 사용할 해시를 추출하는 보조 도구라는 점을 구별한다.

**개념 구분**

Striker는 **정보 수집과 취약점 탐색**을 목적으로 하는 도구로, 패스워드 해시를 분석하여 후보 암호를 찾는 크래킹 도구와 구별된다. 도구 이름이 아니라 주된 기능을 기준으로 분류하는 문제이다.

John the Ripper는 여러 형식의 패스워드 해시에 대해 후보 암호를 대입·비교하여 암호를 찾는 대표적인 크래킹 도구이다.

Pwdump는 Windows의 **패스워드 해시 정보를 추출**하는 도구이다. 그 자체가 평문 암호를 알아내는 크래커는 아니지만, 추출한 해시를 크래킹·암호 강도 점검 도구에 제공하므로 이 문제에서는 관련 도구에 포함된다.

RainbowCrack은 미리 계산한 **레인보 테이블**을 이용하여 해시에 대응하는 암호 후보를 찾는 도구이다. 계산 결과를 미리 저장해 두는 시간·공간 절충 방식을 활용한다.

따라서 패스워드 크래킹 도구로 가장 적절하지 않은 것은 ① Striker이다.

NoteBase

**문 5. 방화벽(firewall)의 구축형태에 따른 장점으로 가장 적절하지 않은 것은?**

① 스크리닝 라우터(screening router) 구조는 클라이언트와 서버의 환경변화 없이도 설치가 가능하다.

② 듀얼 홈드 게이트웨이(dual-homed gateway) 구조는 로그 정보 생성 및 관리가 용이하다.

③ 스크린드 호스트 게이트웨이(screened host gateway) 구조는 네트워크 계층과 응용 계층에서 방어하기 때문에 2단계 방어가 가능하다.

④ 스크린드 서브넷 게이트웨이(screened subnet gateway) 구조는 다른 방화벽의 구축 형태에 비해 설치와 관리가 쉽고 구축 비용이 적게 든다.

**정답 4번**

**간단한 해설**

**스크린드 서브넷**은 DMZ와 다중 경계를 이용해 방어를 강화하는 대신 **구성·관리의 복잡성과 비용이 증가**하는 형태이다. 설치와 관리가 쉽고 저렴하다는 설명은 대표 장점과 맞지 않는다.

**선지별 해설**

① O. 스크리닝 라우터는 경계의 라우터에서 **주소·포트·프로토콜 등의 조건으로 패킷을 필터링**한다. 클라이언트와 서버의 응용프로그램을 별도로 바꾸지 않고 네트워크 경계에 적용할 수 있다는 장점이 있다.

② O. 듀얼 홈드 게이트웨이는 두 네트워크 인터페이스를 가진 호스트에서 내부와 외부 사이의 직접 전달을 제한하고 중계 기능을 제공한다. 통신을 게이트웨이에서 통제하므로 **중계되는 접근의 로그를 집중적으로 생성·관리**하기 쉽다.

③ O. 스크린드 호스트 게이트웨이는 **스크리닝 라우터와 배스천 호스트**를 결합한다. 라우터의 패킷 필터링과 호스트의 응용 계층 중계를 함께 이용하므로 네트워크 계층과 응용 계층의 두 단계 방어가 가능하다.

④ X. 스크린드 서브넷 게이트웨이는 내부망과 외부망 사이에 **별도의 완충망인 DMZ**를 두고 접근을 여러 경계에서 통제하는 구조이다. 방어 수준을 높일 수 있지만 구성 요소와 정책 관리가 늘어나므로, 일반적으로 단순한 구축 형태보다 설치·관리가 복잡하고 비용도 더 든다. 쉬운 관리와 저렴한 비용을 대표 장점으로 든 설명은 적절하지 않다.

따라서 방화벽 구축 형태의 장점으로 가장 적절하지 않은 것은 ④이다.

NoteBase

**문 6. 다음 대응방법에 관련된 공격으로 가장 적절한 것은?**

· SetUID가 설정되어 있는 파일을 줄여야 한다.
· 가능하면 임시파일을 생성하지 않는다.
· 링크(link) 정보를 검사하여 비정상적인 링크를 제거한다.
· 슈퍼유저(root) 소유의 중요한 파일에 관한 링크는 원천적으로 사용하지 못하게 통제한다.

① 레이스 컨디션(race condition) 공격
② 포맷 스트링(format string) 공격
③ 하트블리드(heartbleed) 공격
④ 시스템 자원 고갈(system resource exhaustion) 공격

**정답 1번**

**간단한 해설**

임시파일과 링크를 바꿔치기하여 높은 권한을 악용하는 상황은 **레이스 컨디션 공격**과 관련된다. 검사와 실제 사용 사이에 대상이 달라지는 틈을 줄이는 것이 핵심이다.

**핵심 풀이**

제시된 대책은 **파일을 검사한 시점과 실제 사용하는 시점 사이의 틈**을 악용하는 레이스 컨디션, 특히 TOCTOU 유형을 겨냥한다. 다른 실행 주체가 그 사이 파일이나 링크 대상을 바꾸면, 프로그램이 검사 때와 다른 대상을 처리할 수 있다. 따라서 ① 레이스 컨디션 공격이 해당한다.

SetUID 프로그램의 불필요한 사용을 줄이면 **높은 권한을 악용할 기회**가 줄어든다. 불필요한 임시파일을 만들지 않고 중요한 파일로 연결되는 비정상 링크를 통제하는 것은 파일 바꿔치기 경로를 줄이는 대책이다. 단순히 링크를 한 번 검사하는 것만으로는 검사 후 변경을 막지 못하므로, 안전한 파일 생성·열기와 원자적 처리도 중요하다.

포맷 스트링 공격은 신뢰할 수 없는 입력을 **서식 문자열**로 해석하는 취약점과 관련되고, 하트블리드는 OpenSSL의 하트비트 처리에서 메모리를 과도하게 읽는 취약점이다. 시스템 자원 고갈은 CPU·메모리 등 자원을 소진시키는 것이므로, 제시된 임시파일·링크·권한 대책의 공통 초점과 다르다.

NoteBase

**문 7. 신뢰 플랫폼 모듈(TPM, Trusted Platform Module)에 관한 설명으로 가장 적절하지 않은 것은?**

① 운영체제가 단계적으로 인증된 절차를 거쳐 부팅되도록 한다.

② 휘발성 메모리 영역에 신뢰 플랫폼 모듈을 위한 신원, 상태 인자를 저장한다.

③ 난수 발생기, 암복호화 엔진, RSA(Rivest-Shamir-Adleman) 키 생성기 등을 포함한다.

④ 훼손방지를 위해 하드웨어칩으로 구현하는 것이 일반적이지만 소프트웨어로 구현하기도 한다.

**정답 2번**

**간단한 해설**

전원을 꺼도 유지해야 하는 TPM의 **신원 및 지속 상태 정보는 비휘발성 영역**에 보관한다. 따라서 이를 휘발성 영역에 저장한다고 한 ②가 적절하지 않다.

**선지별 해설**

① O: TPM은 부팅 과정에서 펌웨어와 소프트웨어의 측정값을 보호하고 증명하여 **단계적인 신뢰 사슬과 무결성 확인**을 지원한다. 이 의미에서 신뢰할 수 있는 부팅 절차를 뒷받침한다. 다만 TPM이 단독으로 모든 부팅 코드를 승인하거나 실행을 차단하는 것은 아니며, 펌웨어·운영체제의 검증 절차와 함께 사용된다.

② X: TPM의 **지속적으로 보존할 신원 정보와 상태 정보**는 전원이 꺼져도 유지되어야 하므로 비휘발성 저장 영역에 보관한다. 이를 휘발성 영역에 저장한다고 한 부분이 틀렸다. TPM에 휘발성 저장 공간이 전혀 없다는 뜻은 아니며, 일시적인 실행 상태 등과 영구 보존 정보를 구별해야 한다.

③ O: TPM은 **난수 생성, 암호 연산, 키 생성 및 보호** 등의 기능을 제공한다. RSA 키 생성기와 암복호화 기능은 전통적인 TPM의 대표적인 구성 기능이며, 지원 알고리즘과 세부 구성은 TPM 버전 및 구현에 따라 달라질 수 있다.

④ O: TPM은 물리적 변조에 대한 보호를 고려한 전용 칩 형태로 구현할 수 있으며, **보호된 실행 환경의 펌웨어나 소프트웨어 방식**으로도 구현된다. 구현 형태에 따라 격리와 변조 저항성 등 보안 특성이 같지는 않으므로, 일반 응용 프로그램과 동일한 보호 수준이라는 뜻은 아니다.

NoteBase

**문 8. 다음에서 시스템 취약점 점검 및 탐지 도구로 옳은 것만을 모두 고른 것은?**

㉠ Netbus
㉡ Nmap(Network mapper)
㉢ SAINT(Security Administrator’s Integrated Network Tool)
㉣ SATAN(Security Analysis Tool for Auditing Networks)

① ㉡㉢
② ㉡㉣
③ ㉡㉢㉣
④ ㉠㉡㉢㉣

**정답 3번**

**간단한 해설**

Nmap, SAINT, SATAN은 **네트워크 조사·취약점 점검에 활용하는 도구**이다. Netbus는 원격 제어·백도어 계열로 구별한다.

**보기별 해설**

㉠ Netbus: X. Netbus는 원격 시스템 제어 기능으로 알려진 도구이며, 악용될 경우 백도어·트로이목마로 사용된다. 이 문제에서 묻는 **취약점 점검·탐지 도구**의 분류에는 해당하지 않는다.

㉡ Nmap: O. 네트워크의 호스트와 열린 포트, 제공 서비스 등을 조사하는 도구이다. 이러한 정보를 이용해 노출된 서비스를 점검하고 보안 감사에 활용하며, 스크립트 기능으로 특정 취약점 탐지도 수행할 수 있다.

㉢ SAINT: O. 네트워크에 연결된 시스템의 **알려진 취약점을 검사하고 결과를 분석·보고**하는 취약점 평가 도구이다. 관리자가 취약한 자산을 찾아 조치 우선순위를 정하는 데 활용할 수 있다.

㉣ SATAN: O. 네트워크 서비스와 보안상 약점을 조사하는 취약점 분석 도구이다. 원격 제어를 주 기능으로 하는 Netbus와 달리 보안 점검을 위한 정보 수집·취약점 확인에 해당한다.

따라서 점검·탐지 도구에 해당하는 것은 ㉡·㉢·㉣이며, 이 조합은 ③이다.

NoteBase

**문 9. 스푸핑(spoofing) 공격 유형에 관한 설명으로 가장 적절하지 않은 것은?**

① IP 스푸핑 : 공격자가 정보를 얻거나 접근하기 위해 다른 컴퓨터의 IP 주소를 사용한다.

② E-Mail 스푸핑 : 이메일의 수신자를 위조하여 보내는 방식이다.

③ ARP 스푸핑 : MAC 테이블을 static으로 설정하여 막을 수 있다.

④ DNS 스푸핑 : 실제 DNS 서버보다 빨리 공격대상에게 DNS Response 패킷을 보내 공격대상이 잘못된 IP 주소로 접속하도록 유도하는 공격이다.

**정답 2번**

**간단한 해설**

E-Mail 스푸핑은 **발신자 정보를 위조**하여 다른 사람이 보낸 것처럼 가장하는 방식이다. 수신자를 위조하는 공격으로 설명한 부분이 잘못되었다.

**선지별 해설**

① O. IP 스푸핑은 패킷의 **출발지 IP 주소를 다른 호스트의 주소처럼 위조**하여 상대를 속이는 공격이다. 단순히 다른 IP 주소를 정상적으로 할당받는 것이 아니라 신원을 가장한다는 점이 핵심이다.

② X. E-Mail 스푸핑은 수신자가 아니라 **발신자 주소나 발신자 표시 정보를 위조**하여 다른 사람이 보낸 메일처럼 보이게 하는 방식이다. 따라서 '수신자'를 '발신자'로 고쳐야 한다.

③ O. 다만 원문의 'MAC 테이블'은 표현이 모호하며, 이 문항에서는 **ARP의 IP–MAC 주소 대응표**를 뜻하는 것으로 이해해야 한다. 신뢰할 수 있는 대응을 정적으로 고정하면 위조 ARP 메시지로 그 항목이 바뀌는 것을 방지할 수 있다. 스위치의 MAC–포트 대응표인 CAM 테이블만 정적으로 설정하면 ARP 스푸핑이 해결된다는 뜻은 아니다.

④ O. DNS 스푸핑의 한 방식은 **위조 DNS 응답을 정상 응답보다 먼저 보내** 잘못된 IP 주소가 채택되도록 유도하는 것이다. 실제로 받아들여지려면 질의에 대응하는 응답으로 인정되어야 하므로, 빠르게 보내기만 하면 반드시 성공한다는 의미는 아니다.

따라서 스푸핑 유형의 설명으로 가장 적절하지 않은 것은 발신자와 수신자를 뒤바꾼 ②이다.

NoteBase

**문 10. UNIX 시스템의 로그(log)에 관한 설명으로 가장 적절한 것은?**

① dmesg는 원격지 접속 로그 등 인증과정을 거치는 모든 로그를 저장한다.

② history는 시스템 운영에 관련한 전반적인 로그로 /var/log/messages 파일에 저장한다.

③ utmp는 텍스트(text) 형태로 로그가 저장되며 w, who, users 명령어로 내용을 확인할 수 있다.

④ wtmp는 사용자들의 로그인과 로그아웃, 시스템 재부팅에 관한 정보를 담고 있으며 last 명령어로 내용을 확인할 수 있다.

**정답 4번**

**간단한 해설**

UNIX 계열의 로그는 커널 메시지, 셸 명령 이력, 로그인 기록처럼 목적에 따라 구별한다. wtmp는 **로그인·로그아웃 및 재부팅 이력**을 기록하며 last 명령으로 확인한다.

**선지별 해설**

① X: dmesg는 **커널 링 버퍼의 메시지**를 출력·제어하는 명령이다. 부팅이나 장치 인식 등의 커널 메시지를 확인하는 데 쓰이며, 모든 인증 로그를 저장하는 로그 자체가 아니다. 인증 기록은 시스템의 로깅 설정에 따라 별도로 관리된다.

② X: history는 셸에서 실행한 **명령 이력**을 확인하는 기능이다. Bash에서는 보통 HISTFILE이 지정하는 파일에 이력을 저장하며 기본값은 ~/.bash_history이다. 시스템 전반의 메시지를 기록하는 /var/log/messages와 구별해야 한다.

③ X: utmp는 현재 로그인 세션 등의 정보를 담는 **바이너리 형식**의 파일이다. w, who, users 등으로 로그인 사용자 정보를 확인할 수 있다는 부분이 아니라, 텍스트 형태로 저장된다는 부분이 틀렸다.

④ O: wtmp는 사용자의 **로그인·로그아웃 이력**과 시스템 재부팅 등의 기록을 남긴다. last 명령은 이 파일을 읽어 접속 이력을 보여 주므로, 현재 세션 정보를 중심으로 하는 utmp와 구별된다.

NoteBase

**문 11. 해커의 정보를 얻기 위한 시스템인 허니팟(honeypot)에 관한 설명으로 가장 적절하지 않은 것은?**

① 허니팟을 통과하는 패킷(packet)에 대해서 감시하지 않는다.

② 허니팟은 쉽게 해킹이 가능한 것처럼 취약해 보여야 한다.

③ 허니팟은 해커에게 쉽게 노출되어야 한다.

④ 허니팟은 시스템의 모든 구성 요소를 갖추고 있어야 한다.

**정답 1번**

**출제 포인트**

허니팟의 공격자 유인 기능과 공격 정보를 수집하기 위한 감시 기능을 구분하는 문제이다.

**핵심 개념**

허니팟은 공격자가 관심을 갖고 접근하도록 마련한 미끼 시스템 또는 자원이다. 공격자의 접속, 전송 패킷, 실행 행위 등을 관찰하고 기록하여 공격 방법과 도구에 관한 정보를 얻는다.

**선지별 해설**

O/X는 이 문항에서 설명의 상대적 적절성을 나타내며, X는 가장 적절하지 않은 설명이다.
① X: “감시하지 않는다”가 잘못된 표현이다. 공격을 유도해도 패킷과 공격 행위를 관찰하지 않으면 해커의 정보를 얻기 어렵다. 올바르게는 허니팟에 들어오고 나가는 패킷과 공격 행위를 감시·기록한다.
② O: 공격자가 공격할 만한 대상으로 판단하도록 취약해 보이는 서비스를 제공하거나 모방한다. “취약해 보여야 한다”는 유인을 위한 외관을 뜻하며, 실제로 모든 보안 통제를 없애야 한다는 뜻은 아니다.
③ O: 공격자가 미끼 시스템을 발견하고 접근할 수 있어야 공격 정보를 수집할 기회가 생긴다. 여기서 노출은 공격 대상이 될 수 있게 한다는 의미이며, 허니팟이라는 정체까지 드러내라는 의미는 아니다.
④ O(상대적 판단): 실제 시스템처럼 보이는 구성과 동작을 갖춰 공격자가 의심하지 않고 활동하도록 한다는 취지에서는 ①보다 적절하다. 다만 “모든 구성 요소를 갖추고 있어야 한다”는 표현은 일반적인 필수조건으로 단정할 수 없다. 고상호작용 허니팟은 실제 운영체제와 서비스를 제공하지만, 저상호작용 허니팟은 일부 서비스만 모방할 수도 있다. 정확한 일반 설명은 목적과 상호작용 수준에 맞는 구성 요소를 제공하거나 모방한다는 것이다.

**오답 포인트**

공격자가 접근하도록 허용한다는 사실을 감시하지 않는다는 뜻으로 혼동하기 쉽다. 접근 허용은 유인 수단이고, 감시·기록은 정보 수집 수단이다. ④의 “모든”을 모든 허니팟에 적용되는 절대조건으로 암기하는 것도 피한다.

NoteBase

**다시 나오면 이렇게 판단**

공격자를 유인하는 설명인지, 유인한 공격을 관찰하는 설명인지 구분한다. 정보 수집 목적을 직접 부정하는 “감시하지 않는다”는 가장 부적절하다. 구현 범위를 묻는 경우에는 저상호작용의 서비스 모방과 고상호작용의 실제 시스템 제공을 구분한다.

**암기 포인트**

허니팟은 유인하고 관찰한다. 취약해 보이는 외관과 감시·기록은 함께 작동한다.

NoteBase

**문 12. 다음에서 버퍼 오버플로우(buffer overflow) 공격에 대응하는 방법으로 옳은 것만을 모두 고른 것은?**

㉠ 스택 가드(stack guard)
㉡ 스택 쉴드(stack shield)
㉢ Non-Executable Stack
㉣ ASLR(Address Space Layout Randomization)

① ㉠㉡
② ㉠㉡㉢
③ ㉡㉢㉣
④ ㉠㉡㉢㉣

**정답 4번**

**간단한 해설**

네 방법은 각각 **변조 탐지, 반환 주소 보호, 실행 제한, 주소 무작위화**를 통해 버퍼 오버플로우 악용에 대응한다. 따라서 ㉠·㉡·㉢·㉣을 모두 고른 ④가 맞는다.

**보기별 해설**

㉠ O: 스택 가드는 스택의 주요 제어 정보 앞에 **카나리 값**을 두고 함수가 반환하기 전에 변조 여부를 검사한다. 버퍼를 넘어서 쓴 데이터가 카나리를 손상시키면 이를 탐지하여, 변조된 반환 주소를 사용하는 공격을 막는 데 도움을 준다.

㉡ O: 스택 쉴드는 **반환 주소를 별도의 영역에 보관하여 보호**하는 방식으로 스택의 반환 주소 덮어쓰기에 대응한다. 일반 스택에 저장된 값만을 그대로 신뢰하지 않도록 하여 공격자가 제어 흐름을 바꾸기 어렵게 한다.

㉢ O: Non-Executable Stack은 **스택 메모리에서 코드 실행을 금지**한다. 버퍼 오버플로우로 스택에 코드를 주입하더라도 그 위치에서 실행하는 것을 제한한다. 다만 메모리가 덮어써지는 오류 자체를 제거하거나 모든 코드 재사용 공격을 막는 것은 아니다.

㉣ O: ASLR은 실행 파일·라이브러리·스택 등 대상 메모리 영역의 배치를 무작위화하여 **공격에 필요한 주소를 예측하기 어렵게**한다. 버퍼 오버플로우 악용의 성공 가능성을 낮추지만, 취약점 자체를 수정하는 기법은 아니다.

네 보기 모두 대응 방법이므로 조합은 ④이다. 각 방법의 보호 범위가 다르므로 함께 적용하고, 근본적으로는 안전한 메모리 처리로 결함을 수정해야 한다.

NoteBase

**문 13. 다음 IDS(Intrusion Detection System)의 탐지 실행단계를 순서대로 나열한 것은?**

㉠ 분석 및 탐지
㉡ 보고 및 대응
㉢ 데이터 수집
㉣ 데이터 가공 및 축약

① ㉢-㉣-㉠-㉡
② ㉢-㉣-㉡-㉠
③ ㉠-㉡-㉢-㉣
④ ㉠-㉡-㉣-㉢

**정답 1번**

**간단한 해설**

IDS는 **분석에 사용할 자료가 먼저 준비되어야** 침입 여부를 판단할 수 있으며, 보고와 대응은 탐지 결과를 바탕으로 이루어진다.

**올바른 순서**

**㉢ 데이터 수집 → ㉣ 데이터 가공 및 축약 → ㉠ 분석 및 탐지 → ㉡ 보고 및 대응**

먼저 ㉢ 데이터 수집 단계에서 네트워크 패킷, 시스템 로그, 감사 기록 등 판단에 필요한 관측 자료를 확보한다. 분석할 입력이 있어야 하므로 수집이 출발점이다.

다음 ㉣ 데이터 가공 및 축약 단계에서 수집 자료를 분석 가능한 형식으로 정리하고 필요한 항목을 추려낸다. 중복·불필요한 정보를 줄이고 특징을 추출하여 탐지에 사용할 입력을 준비한다.

이어 ㉠ 분석 및 탐지 단계에서 준비한 데이터를 알려진 공격 패턴이나 정상 행위 기준 등과 비교하여 침입 징후를 판단한다. 전처리한 자료를 해석하는 단계이므로 가공 및 축약 뒤에 온다.

마지막 ㉡ 보고 및 대응 단계에서 탐지 결과를 기록·경고하고 관리자나 연계 시스템의 대응으로 이어지게 한다. IDS가 항상 직접 차단한다는 뜻은 아니며, 대응 방식은 구성과 정책에 따라 다르다. 탐지 결과가 먼저 나와야 그 결과에 대한 보고·대응을 할 수 있다.

NoteBase

**문 14. 블루투스의 보안 위협 유형에 관한 설명으로 가장 적절하지 않은 것은?**

① 블루프린팅(blueprinting) : 공격대상장치에 연결하여 임의의 파일을 삭제할 수 있다.

② 블루스나핑(bluesnarfing) : 공격대상장치에 있는 주소록이나 달력 등의 내용을 요청하여 열람하거나 취약한 임의의 파일에 접근할 수 있다.

③ 블루버깅(bluebugging) : 공격대상장치를 원격에서 연결하여 전화걸기, 불특정 번호로 SMS 보내기 등 임의의 동작을 실행시킬 수 있다.

④ 블루재킹(bluejacking) : 블루투스를 이용해 스팸 메시지를 익명으로 퍼트릴 수 있다.

**정답 1번**

**간단한 해설**

블루프린팅은 블루투스 장치의 정보를 분석하여 **장치의 종류와 특성을 식별**하는 기법이다. 파일 삭제가 아니라 공격 대상의 정보를 수집하는 핑거프린팅에 해당한다.

**선지별 해설**

① X: 블루프린팅은 블루투스 장치가 제공하는 정보를 분석하여 **제조사·모델·펌웨어 등을 식별**하는 기법이다. 임의의 파일을 삭제하는 공격이라는 설명은 잘못되었으며, 장치의 특성을 파악하는 핑거프린팅으로 이해해야 한다.

② O: 블루스나핑은 취약한 블루투스 장치에 무단으로 접근하여 **저장된 정보를 열람·탈취**하는 공격이다. 주소록이나 달력 등 개인 정보와 접근 가능한 파일이 대상이 될 수 있다.

③ O: 블루버깅은 장치의 취약점을 악용하여 **명령을 실행하고 기능을 원격 제어**하는 공격이다. 단순한 정보 열람을 넘어 전화 걸기나 SMS 전송과 같은 동작을 수행하게 할 수 있다.

④ O: 블루재킹은 블루투스를 통해 상대방이 원하지 않는 **메시지를 전송**하는 행위이다. 스팸성 메시지를 보내는 것이 대표적이며, 저장된 정보의 탈취나 장치 제어와 구별된다.

NoteBase

**문 15. 분산반사 서비스 거부(DRDoS, Distributed Reflection Denial of Service) 공격에 관한 설명으로 가장 적절하지 않은 것은?**

① TCP에서 사용하는 3way-handshake의 취약점을 이용한다.

② 출발지의 IP 주소를 위조하는 공격이다.

③ 악성 봇(bot)의 감염을 통해서만 공격이 가능하다.

④ 공격트래픽이 수많은 반사서버를 경유하므로 역추적이 어렵다.

**정답 3번**

**간단한 해설**

DRDoS는 **출발지 주소를 위조**하여 여러 서버의 응답이 피해자에게 모이게 하는 공격이다. 반사 서버는 정상 서버일 수 있으므로 **악성 봇 감염이 필수는 아니다**.

**선지별 해설**

① O. **TCP를 이용하는 반사 공격**에서는 연결 수립 과정에서 SYN 요청에 SYN/ACK 응답을 보내는 동작을 악용할 수 있다. 다만 DRDoS가 항상 TCP 3-way handshake만 이용하는 것은 아니며, DNS 등 UDP 기반 서비스의 응답을 반사시키는 방식도 있다. 이 설명은 TCP 기반 유형에 해당한다.

② O. 반사 요청의 **출발지 IP 주소를 피해자의 주소로 위조**하면 반사 서버의 응답이 피해자에게 향한다. 공격 요청을 보낸 주체와 응답을 받는 대상이 달라지는 점이 핵심이다.

③ X. DRDoS의 반사 서버는 **악성 봇에 감염되지 않은 정상 서버**일 수 있다. 정상적인 응답 기능이 악용되는 것이므로 봇 감염이 필수 조건은 아니다. 감염된 봇이 공격에 동원될 수 있다는 사실과, 감염을 통해서만 공격할 수 있다는 주장은 구별해야 한다.

④ O. 피해자에게 보이는 응답의 출발지는 다수의 반사 서버이고, 공격자가 처음 보낸 요청에는 위조된 출발지 주소가 사용된다. 따라서 **반사 서버와 실제 공격자를 바로 동일시할 수 없어** 공격 근원 추적이 어려워진다.

따라서 DRDoS 공격에 대한 설명으로 가장 적절하지 않은 것은 ③이다.

NoteBase

**문 16. SecaaS(Security as a Service)에 관한 설명으로 가장 적절하지 않은 것은?**

① 인터넷을 사용해서 안전한 보안 서비스를 제공한다.

② IT 인프라 서비스를 제공하는 IaaS(Infrastructure as a Service)로 분류된다.

③ 서비스 제공자가 제공하는 보안 서비스 패키지이다.

④ 방화벽, 메일 보안, 신원 및 접근관리 등의 서비스를 제공한다.

**정답 2번**

**간단한 해설**

SecaaS는 **보안 기능 자체를 서비스로 제공**하는 개념이다. 서버·저장장치 같은 인프라 자원을 제공하는 IaaS와 동일하게 분류한 ②가 적절하지 않다.

**선지별 해설**

① O: SecaaS는 인터넷 등 네트워크를 통해 **보안 기능을 서비스로 제공**하는 방식이다. 이용자는 보안 기능을 직접 구축하는 대신 제공자의 서비스를 이용할 수 있다. 여기서 안전한 서비스라는 표현은 보안을 제공하려는 목적을 뜻하며, 모든 위험이 사라진다는 보장은 아니다.

② X: IaaS는 가상 서버, 저장장치, 네트워크 등 **기반 인프라 자원**을 제공하는 모델이다. SecaaS는 보안 기능 자체를 서비스로 제공하는 개념으로, 이를 IaaS로 분류하는 것은 적절하지 않다. 보안 소프트웨어 기능을 구독하는 SaaS 형태 등이 대표적이며, 서비스가 내부적으로 IaaS를 이용하는 것과 서비스 자체의 분류는 구별해야 한다.

③ O: 제공자가 보안 기능을 운영하여 고객에게 **보안 서비스 또는 서비스 묶음**으로 제공한다는 설명이다. 고객은 계약한 기능과 범위에 따라 이를 이용하므로, 모든 보안 업무가 항상 제공자에게 이전되는 것은 아니다.

④ O: SecaaS에는 **네트워크 보안, 이메일 보안, 신원 및 접근관리** 등이 포함될 수 있다. 방화벽 기능을 서비스로 제공하거나 스팸·악성 메일을 걸러 내고 사용자 접근을 관리하는 방식이 이에 해당한다.

NoteBase

**문 17. 서버 보안용 점검 도구인 Tripwire에 관한 설명으로 가장 적절하지 않은 것은?**

① 파일의 기밀성을 보장하는 것이 목적인 도구이다.

② 해커의 침입으로 인한 시스템 파일이나 디렉터리 변경을 쉽게 검출할 수 있다.

③ fcheck와 AIDE(Advanced Intrusion Detection Environment)도 비슷한 기능을 한다.

④ MD5(Message Digest 5), SHA(Secure Hash Algorithm), CRC-32(Cyclic Redundancy Check-32) 등의 해시 함수를 제공한다.

**정답 1번**

**간단한 해설**

Tripwire는 정상 상태와의 비교로 **파일·디렉터리 변경을 탐지하는 무결성 점검 도구**이다. 파일 내용을 비밀로 유지하는 기밀성 보호와는 목적이 다르다.

**선지별 해설**

① X. Tripwire의 핵심 목적은 파일 내용을 숨기는 기밀성이 아니라 **파일·디렉터리의 무결성 검사**이다. 정상 상태의 기준값과 현재 상태를 비교하여 변경을 탐지하며, 파일을 암호화해 열람을 막는 도구와 구별한다.

② O. 기준 데이터베이스에 기록한 파일의 내용 요약값과 속성 등을 현재 값과 비교하여 추가·삭제·변경을 검출할 수 있다. 다만 변경이 발견되었다고 모두 침입은 아니므로 정상적인 업데이트인지도 확인해야 하며, 기준 데이터 자체도 보호해야 한다.

③ O. fcheck와 AIDE 역시 파일·디렉터리의 상태를 기준 정보와 비교하는 **무결성 점검** 도구 계열이다. 이러한 변경 감시는 침입으로 인한 시스템 변조를 알아내는 데 활용된다.

④ O. Tripwire가 MD5·SHA·CRC-32 등 여러 변경 검출용 요약값·체크섬 방식을 제공해 왔다는 취지로 타당하다. 다만 엄밀히 **CRC-32는 암호학적 해시가 아니라 비암호학적 체크섬**이다. 이 선택지의 포괄적인 '해시 함수' 표현을 모든 알고리즘의 암호학적 안전성이 같다는 뜻으로 받아들이면 안 되며, MD5나 오래된 SHA 계열의 지원 이력도 현재 안전한 사용을 권장한다는 의미는 아니다.

NoteBase

**문 18. 다음에서 설명하는 시스템으로 가장 적절한 것은?**

빅데이터 분석 기술 등을 바탕으로 전자금융거래에 사용되는 단말기 정보, 접속정보, 거래내용 등의 정보들을 분석하여 이상 금융거래를 탐지하고 차단하는 시스템을 의미한다. 정보수집 기능, 분석 및 탐지 기능, 대응 기능, 모니터링 및 감사 기능으로 구성되며, 보안 프로그램에서 방지하지 못하는 전자금융사기에 대한 이상거래를 탐지하여 조치할 수 있도록 지원하는 시스템을 말한다.

① NMS(Network Management System)

② IPS(Intrusion Prevention System)

③ IDS(Intrusion Detection System)

④ FDS(Fraud Detection System)

**정답 4번**

**간단한 해설**

**FDS**는 단말기·접속·거래 정보를 분석해 **이상금융거래를 탐지하고 대응**하는 시스템이다. 제시문의 판단 대상이 네트워크 침입 자체가 아니라 전자금융거래라는 점이 핵심이다.

**핵심 풀이**

제시문은 단말기 정보, 접속정보, 거래내용을 종합해 **전자금융거래의 이상 징후**를 판별하는 시스템을 설명한다. 거래 패턴을 분석하여 부정 사용이나 금융사기가 의심되는 거래를 찾아내는 것이 핵심이므로 FDS, 즉 이상금융거래 탐지시스템에 해당한다.

FDS의 **정보수집**은 거래와 이용 환경의 자료를 모으는 기능이고, **분석 및 탐지**는 수집된 정보를 비교·분석하여 이상 징후를 찾는 기능이다. 대응 기능은 의심 거래의 차단이나 추가 확인 등의 조치를 지원하며, 모니터링 및 감사 기능은 탐지·대응 현황과 이력을 점검할 수 있게 한다.

일반적인 보안 프로그램이 단말기 악성코드나 침입을 막더라도 거래 자체의 비정상 패턴까지 모두 확인하는 것은 아니다. FDS는 **거래 정보 중심의 분석**으로 이러한 전자금융사기 대응을 보완한다.

NMS는 네트워크 장비·성능·장애를 관리하는 시스템이다.

IDS는 침입 징후를 탐지하고 알리는 데, IPS는 침입 트래픽의 탐지와 차단에 초점이 있다. 단순히 '탐지·차단'이라는 말이 아니라 전자금융거래와 부정 거래 분석이라는 대상까지 보아야 구별할 수 있다.

따라서 설명에 해당하는 시스템은 FDS인 ④이다.

NoteBase

**문 19. 다음 UNIX 시스템의 /etc/shadow 파일에 관한 설명으로 가장 적절하지 않은 것은?**

police:$5$De3h9deY$5u78Fd~중략~T4e3rfG:13123:0:90:5:7:0:

① 패스워드(password) 만료 5일 전부터 사용자에게 경고한다.
② 사용자 패스워드는 SHA-512 일방향 해시 알고리즘이 적용되어 저장되었다.
③ 현재 사용 중인 패스워드를 변경하지 않고 사용할 수 있는 기간은 90일이다.
④ 패스워드가 마지막으로 변경된 날짜는 1970년 1월 1일을 기준으로 13,123일이 지났다.

**정답 2번**

**간단한 해설**

패스워드 해시 앞의 **$5$는 SHA-256 기반 방식**을 뜻한다. SHA-512 기반 방식은 $6$으로 표시하므로 두 식별자를 구별해야 한다.

**선지별 해설**

① O: /etc/shadow의 필드는 콜론(:)으로 구분된다. 여섯 번째 필드인 **5는 패스워드 만료 경고 기간**으로, 만료 5일 전부터 사용자에게 경고하도록 설정한 것이다.

② X: 두 번째 필드의 맨 앞에 있는 **$5$는 SHA-256 기반 패스워드 해시 방식**을 나타낸다. SHA-512 기반 방식의 식별자는 $6$이므로, 제시된 값을 SHA-512로 해석한 것은 잘못이다.

③ O: 다섯 번째 필드인 **90은 패스워드의 최대 사용 기간**이다. 마지막 변경일부터 90일이 지나면 패스워드를 변경하도록 하는 설정이며, 이는 계정 자체의 만료일과 구별된다.

④ O: 세 번째 필드인 **13123은 패스워드의 마지막 변경일**을 나타낸다. 1970년 1월 1일을 기준으로 경과한 일수로 기록하므로, 그 기준일부터 13,123일이 지난 날짜에 마지막으로 변경되었다는 뜻이다.

NoteBase

**문 20. 다음에서 설명하는 무선 LAN 프로토콜은?**

IEEE 802.11n의 후속 버전으로 Wi-Fi 5라고 부르며, 정보를 최대 6.9Gbps의 속도로 전송하고 5GHz 주파수에서 높은 대역폭 (80MHz⊠160MHz)을 지원한다.

① IEEE 802.11b

② IEEE 802.11g

③ IEEE 802.11i

④ IEEE 802.11ac

**정답 4번**

**간단한 해설**

**Wi-Fi 5는 IEEE 802.11ac**를 가리킨다. 5GHz 대역과 넓은 채널 폭을 이용하는 특징이 일치하므로 ④가 맞는다.

**핵심 풀이**

설명의 결정적인 단서는 **Wi-Fi 5, 5GHz, 80~160MHz 채널 폭**이다. 이 특징을 갖는 무선 LAN 규격은 IEEE 802.11ac이며, 802.11n보다 넓은 채널과 고차 변조, 다중 공간 스트림 등을 이용해 전송률을 높였다. 따라서 ④가 적절하다.

약 6.9Gbps는 최대 구성에서의 **이론적인 물리계층 전송률**이다. 모든 단말이나 공유기가 이 속도를 지원하거나 실제 데이터가 항상 이 속도로 전달된다는 뜻은 아니다. 실제 속도는 채널 폭, 공간 스트림 수, 신호 상태 및 프로토콜 오버헤드 등의 영향을 받는다.

802.11b와 802.11g는 2.4GHz 대역의 이전 무선 LAN 규격으로 Wi-Fi 5를 가리키지 않는다.

802.11i는 **무선 LAN 보안 강화**를 위한 규격이므로, 제시된 고속 무선 전송 규격과 구별한다.

NoteBase