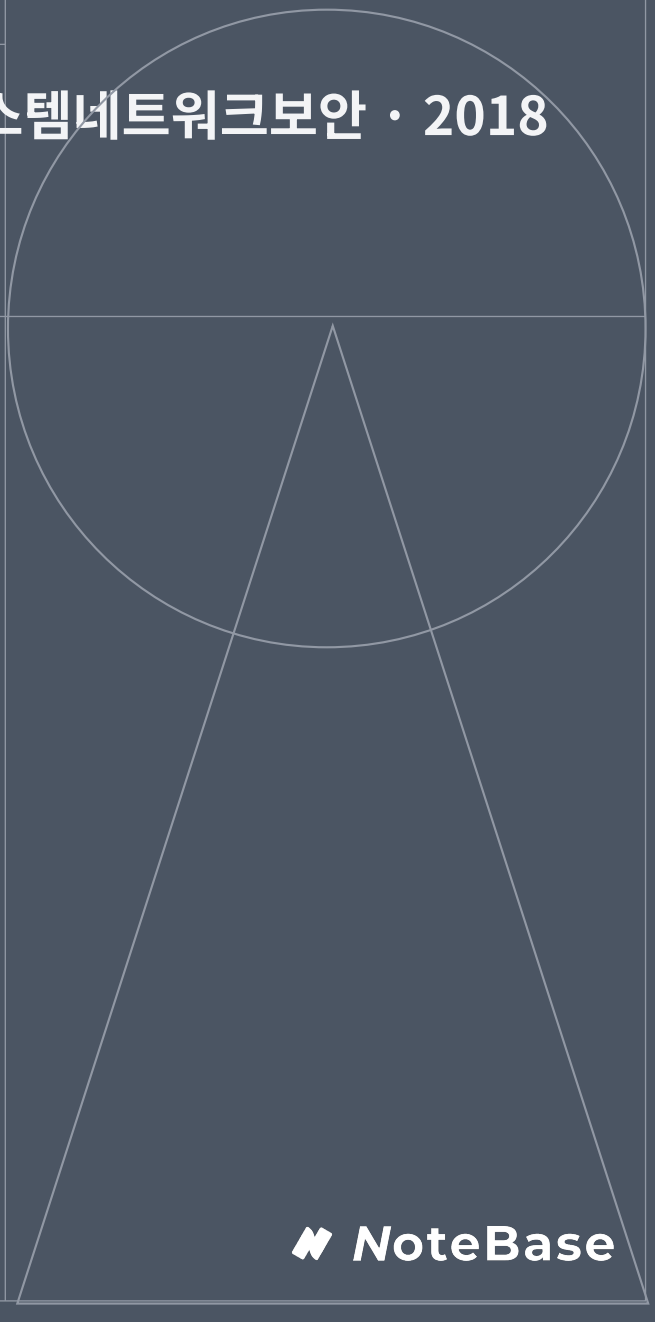
기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2018



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2018

공무원/경찰/경력채용 · 시스템네트워크보안 · 2018

문 1. 192.168.16.0/20의 IPv4 주소 블록을 동일한 크기의 8개 서브넷으로 나누었다. 8개의 서브넷 주소들로 가장 적절하지 않은 것은?

① 192.168.24.0/23

② 192.168.16.0/23

③ 192.168.32.0/23

④ 192.168.28.0/23

정답 3번

간단한 해설

8개로 균등 분할하면 접두사가 /20에서 /23으로 늘어나고, 세 번째 옥텟은 16부터 30까지 2씩 증가한다. **세 번째 옥텟이 32인 주소는 원래 블록 밖**이므로 분할된 서브넷에 포함되지 않는다.

NoteBase

계산 과정

원래 블록의 범위: /20은 32비트 IPv4 주소 중 앞 20비트가 네트워크 부분이라는 뜻이다. 마스크는 255.255.240.0이므로 세 번째 옥텟의 블록 간격은 $256 - 240 = 16$이다. 따라서 192.168.16.0/20의 전체 주소 범위는 **192.168.16.0~192.168.31.255**이다.

8개로 균등 분할: $8 = 2^3$이므로 호스트 부분에서 **3비트를 서브넷 구분에 추가**한다. 새 접두사 길이는 $20 + 3 = 23$이고, 각 서브넷은 $2^{32-23} = 512$개의 주소를 포함한다. 여기서는 사용 가능한 호스트 수가 아니라 전체 주소 블록의 크기를 계산하므로 2를 빼지 않는다.

서브넷 시작 주소: /23의 마스크는 255.255.254.0이고 세 번째 옥텟의 간격은 $256 - 254 = 2$이다. 시작값 16에서 2씩 증가시키면 **16, 18, 20, 22, 24, 26, 28, 30**이 된다. 따라서 8개 서브넷은 192.168.16.0/23, 192.168.18.0/23, 192.168.20.0/23, 192.168.22.0/23, 192.168.24.0/23, 192.168.26.0/23, 192.168.28.0/23, 192.168.30.0/23이다.

선택지 대조: ① 192.168.24.0/23, ② 192.168.16.0/23, ④ 192.168.28.0/23은 위 목록에 포함된다. ③ 192.168.32.0/23은 /23 경계에는 맞지만 **원래 /20 블록의 범위를 벗어난다**. 따라서 적절하지 않은 서브넷 주소는 ③이다.

NoteBase

문 2. 유닉스 시스템의 ‘traceroute’ 프로그램을 이용하여 발신지에서 목적지까지 IPv4 패킷의 전달 경로를 추적하고자 한다. 전달 경로 상의 라우터 장비들이 발신지에게 전달하는 패킷의 종류로 가장 적절한 것은?

① UDP 패킷

② TCP 패킷

③ ICMP 패킷

④ IGMP 패킷

정답 3번

간단한 해설

경로상의 라우터는 TTL이 소진된 탐사 패킷에 대해 **ICMP Time Exceeded**로 응답한다. 발신지가 보내는 UDP 탐사 패킷과 라우터가 돌려주는 오류 응답을 구별해야 한다.

핵심 풀이

traceroute는 IPv4 패킷의 TTL(Time To Live)을 작은 값부터 차례로 늘려 탐사 패킷을 보낸다. 라우터는 패킷을 전달할 때 TTL을 줄이며, TTL이 소진되면 해당 패킷을 폐기하고 발신지에 **ICMP Time Exceeded** 메시지를 보낸다. IPv4에서 이 메시지는 Type 11, Code 0이다. 발신지는 응답한 라우터의 주소를 통해 경로의 각 홉을 파악한다.

혼동하기 쉬운 것은 **보내는 탐사 패킷과 돌아오는 오류 응답**이다. 전통적인 유닉스 traceroute는 UDP 탐사 패킷을 사용하지만, 중간 라우터의 TTL 만료 통지는 UDP가 아니라 ICMP이다. TCP도 여기서 묻는 라우터의 TTL 만료 통지 프로토콜에 해당하지 않으며, IGMP는 IPv4 멀티캐스트 그룹 가입 정보를 관리하는 프로토콜이다.

따라서 경로상의 라우터가 발신지로 보내는 응답을 고르면 ICMP 패킷인 ③이다.

NoteBase

문 3. SSL(Secure Socket Layer)에 대한 설명 중 가장 적절하지 않은 것은?

① 메시지 기밀성을 제공하기 위해서 대칭키 암호를 사용한다.

② UDP를 이용하여 신뢰할 수 있는 보안 서비스를 제공한다.

③ 클라이언트와 서버 간에 세션을 연결하고 유지하는 프로토콜이다.

④ HTTPS 프로토콜은 SSL을 사용하는 보안서비스이다.

정답 2번

간단한 해설

SSL은 일반적으로 **UDP가 아니라 TCP와 같은 신뢰성 있는 전송 서비스** 위에서 동작한다. 따라서 UDP를 이용한다고 한 ②가 가장 적절하지 않다.

선지별 해설

① O: SSL은 핸드셰이크에서 정한 비밀키를 바탕으로 **실제 메시지 데이터를 대칭키로 암호화**하여 기밀성을 제공한다. 공개키 방식이 인증이나 키 설정에 쓰일 수 있다는 점과 실제 데이터의 암호화 방식을 구별해야 한다.

② X: SSL은 일반적으로 **TCP와 같은 신뢰성 있는 전송 서비스 위에서** 동작한다. UDP 자체는 순서 보장과 재전송을 제공하지 않으므로, SSL이 UDP를 직접 기반으로 신뢰성 있는 보안 서비스를 제공한다는 설명은 맞지 않는다. 따라서 가장 적절하지 않은 것은 ②이다.

③ O: SSL 핸드셰이크는 클라이언트와 서버 사이에서 암호 알고리즘과 키 등 보안 매개변수를 협의하여 보안 통신을 설정한다. 이후 연결에 적용할 상태를 관리하며, 세션 정보를 이용한 재개도 가능하다. 여기서 세션은 **클라이언트와 서버가 공유하는 보안 매개변수의 연관 관계**를 뜻하며, 단순히 TCP 연결 설정만을 가리키는 것은 아니다.

④ O: HTTPS는 **HTTP 통신을 SSL/TLS로 보호**하는 구조의 보안 웹 통신을 뜻한다. SSL을 사용한 HTTP 보호 방식에서 후속 규격인 TLS를 사용하는 방식으로 발전했으므로, 이 선지는 HTTPS와 SSL 계열 보안 통신의 관계를 설명한 것이다. 구형 SSL 버전의 사용을 권장한다는 의미는 아니다.

문 4. 유닉스 로그 파일에 저장되는 정보로 가장 적절하지 않은 것은?

① wtmp - 사용자 로그인, 로그아웃 정보 및 시스템 부팅 정보

② utmp - 5번 이상 로그인 실패했을 경우의 로그인 실패 정보

③ lastlog - 사용자의 최근 로그인 시간 정보

④ sulog - su 명령어 사용 시 변경 전 사용자 계정과 변경 후 사용자 계정 정보

정답 2번

간단한 해설

utmp는 **현재 로그인 세션**의 정보를 담는다. 선지의 반복 로그인 실패 기록은 utmp가 아니라 Solaris의 전통적인 **loginlog** 설명에 해당한다.

선지별 해설

이 문항은 전통적인 유닉스 계열 로그의 용도를 구별한다. 실제 파일명·경로와 기록 조건은 운영체제와 설정에 따라 달라질 수 있다.

① O: wtmp는 **로그인·로그아웃의 누적 이력**을 보관한다. 시스템의 부팅·재부팅·종료 같은 사건도 기록하므로 사용자 접속 이력과 시스템 가동 이력을 확인하는 데 사용된다.

② X: utmp는 **현재 로그인하여 사용 중인 세션**의 정보를 나타낸다. 반복된 로그인 실패를 기록하는 파일이라는 설명은 맞지 않는다. 선지의 '5번 이상 로그인 실패'는 Solaris의 전통적인 loginlog 기록 방식에 대응한다. loginlog를 사용하도록 준비한 환경에서 같은 login 실행 중 기본 재시도 한도인 5회에 이르면 각 실패 내역이 기록되며, 한도와 기록 여부는 설정에 따라 달라질 수 있다.

③ O: lastlog는 **사용자별 가장 최근 로그인**의 시각 등을 보관한다. 여러 번의 접속 내역을 누적하는 wtmp와 달리, 각 사용자가 마지막으로 언제 접속했는지를 확인하는 데 초점이 있다.

④ O: sulog는 su를 이용한 계정 전환 시도에서 **원래 사용자와 전환 대상 사용자**를 기록한다. 시각·터미널·성공 여부도 함께 기록할 수 있으며, 일반 사용자에서 root로 전환하는 경우에만 한정되지 않는다.

따라서 utmp를 반복 로그인 실패 기록과 연결한 ②가 가장 적절하지 않다.

NoteBase

문 5. IPv6 프로토콜 헤더(Header)의 필드(Field)로 가장 적절하지 않은 것은?

① TTL(Time-To-Live)

② Source address

③ Flow label

④ Version

정답 1번

간단한 해설

IPv6는 IPv4의 TTL에 대응하는 필드로 **Hop Limit**을 사용한다. Source Address, Flow Label, Version은 IPv6 기본 헤더의 필드이다.

개념 구분

TTL(Time-To-Live)은 IPv4 헤더의 필드이다. IPv6에서는 이에 대응하는 **Hop Limit**을 사용한다. 패킷을 전달하는 노드마다 값을 1씩 줄여 패킷이 네트워크에서 끝없이 순환하지 않도록 한다.

Source Address는 패킷을 보낸 출발지의 IPv6 주소를 나타내는 128비트 필드이다.

Flow Label은 같은 흐름에 속하는 패킷을 식별하는 데 사용하는 **20비트 흐름 표지**이다.

Version은 IP 버전을 나타내는 4비트 필드이며 IPv6에서는 값이 6이다.

따라서 IPv6 헤더에 해당 이름으로 포함되지 않는 필드는 TTL인 ①이다.

NoteBase

문 6. 침입탐지시스템(IDS : Intrusion Detection System)에 대한 설명으로 가장 적절하지 않은 것은?

① 알려지지 않은 공격 행위도 이상탐지(Anomaly detection) 방식을 이용하여 탐지할 수 있다.

② IDS는 방화벽과 상호 보완적으로 사용될 수 있다.

③ 기존의 공격 패턴을 분석하여 침입을 탐지하는 오용탐지(Misuse detection) 방식을 사용할 수 있다.

④ IDS를 이용하면 공격 시도를 사전에 예방하고 차단할 수 있다.

정답 4번

간단한 해설

IDS는 침입 징후를 탐지하여 기록하고 경고하는 시스템이다. 탐지에 더해 **공격을 차단하는 기능은 IPS**의 역할이므로 두 시스템을 구별해야 한다.

선지별 해설

① O: 이상탐지는 정상적인 사용자·시스템 활동의 기준을 만들고, 관측된 활동이 그 기준에서 크게 벗어나는지를 분석한다. 이미 알려진 공격 서명과 일치하지 않아도 **정상 행위와의 편차**가 크면 새로운 공격을 탐지할 수 있다. 다만 정상적인 변화도 이상으로 판단할 수 있어 오탐 가능성이 있다.

② O: 방화벽은 접근통제 규칙에 따라 통신의 허용·차단을 수행하고, IDS는 관측된 활동에서 침입 징후를 분석해 경고한다. 방화벽을 통과한 통신이나 내부의 의심 활동을 IDS가 추가로 살피므로 두 장비는 **접근통제와 침입 감시를 보완**할 수 있다.

③ O: 오용탐지는 알려진 공격의 특징을 규칙이나 서명으로 정의하고 관측된 활동과 비교한다. 따라서 **기존 공격 패턴과의 일치**를 이용해 침입을 탐지할 수 있지만, 등록된 패턴으로 표현되지 않은 새로운 공격에는 탐지 한계가 있다.

④ X: IDS의 기본 역할은 침입 징후의 **탐지·기록·경고**이며, 공격의 사전 예방과 차단 자체가 기본 기능인 것은 아니다. 탐지에 더해 공격 트래픽의 차단 등 예방 기능을 수행하는 것은 IPS이다. IDS의 경고를 방화벽 등과 연동해 대응할 수는 있지만, 이를 IDS 자체의 기본 차단 기능과 혼동해서는 안 된다.

NoteBase

문 7. TCP SYN flooding 공격의 대비책으로 가장 적절하지 않은 것은?

① 방화벽이나 IDS/IPS(Intrusion Prevention System) 시스템을 도입하여 침입을 탐지하고 차단한다.

② TCP 연결 타임아웃을 길게 설정한다.

③ CPU 성능이 지원하는 한도 내에서 백로그 큐(Backlog queue)를 늘려준다.

④ SYN cookie 기능을 활성화한다.

정답 2번

간단한 해설

연결 수립 타임아웃을 길게 하면 미완료 연결이 **자원을 더 오래 점유**하여 SYN flooding의 피해가 커질 수 있다. 미완료 연결을 빨리 회수하거나 연결 확인 전 상태 저장을 줄이는 것이 대응 방향이다.

선지별 해설

① O: 방화벽·IPS의 필터링이나 SYN 방어 기능으로 비정상 연결 요청을 차단할 수 있다. IDS는 **탐지·경보**가 중심이므로 차단 장비와 연계한다. 장비를 설치했다는 사실만으로 모든 공격이 방어되는 것은 아니다.

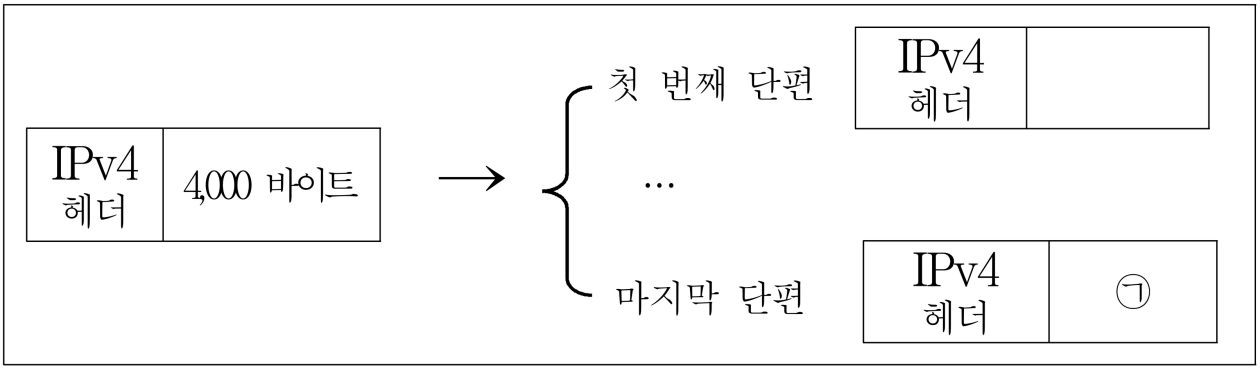
② X: SYN flooding은 연결이 완성되지 않은 반개방 연결을 쌓아 정상 요청을 방해한다. 연결 수립 대기 타임아웃을 늘리면 **미완료 연결이 자원을 더 오래 점유**한다. 이를 줄여 빨리 회수하는 방향이 대응책이지만, 지나치게 짧으면 정상 연결도 실패할 수 있다.

③ O: 백로그 큐를 늘리면 **대기 중인 연결을 더 많이 수용**하여 큐 포화를 늦출 수 있다. 처리 성능과 메모리의 한도 안에서 조정해야 하며, 큐 확대만으로 지속적인 공격을 제거하지는 못한다.

④ O: SYN cookie는 연결 정보를 SYN-ACK의 순서번호에 담고, 최종 ACK가 돌아오면 검증하여 연결 상태를 구성한다. **연결 확인 전 상태 저장을 줄여** 반개방 연결에 의한 자원 고갈을 완화한다.

NoteBase

문 8. MTU(Maximum Transfer Unit)값이 1,500바이트로 설정되어 있는 이더넷(Ethernet)을 통해 그림과 같이 4,000바이트의 IPv4 패킷을 보내려고 한다. MTU값에 의해서 단편화(Fragmentation)된 패킷이 순서대로 전달된다고 가정할 때 마지막 단편으로 전송되는 데이터그램 ㉠의 크기(IPv4헤더는 제외)로 가장 적절한 것은?



① 1,000 바이트

② 1,040 바이트

③ 1,480 바이트

④ 1,500 바이트

정답 2번

간단한 해설

MTU에는 IP 헤더가 포함되므로 기본 헤더 20바이트를 빼면 단편당 데이터는 1,480바이트이다. 그림의 데이터 4,000바이트에서 두 단편의 2,960바이트를 빼면 마지막 데이터는 **1,040바이트**가 남는다.

NoteBase

계산 과정

그림에서는 IPv4 헤더와 4,000바이트 영역을 따로 표시하므로, 나누어 보낼 **데이터 부분이 4,000바이트**이다. 구할 값도 마지막 단편의 헤더를 제외한 데이터 크기이다.

별도 옵션이 없는 기본 IPv4 헤더 20바이트를 기준으로 계산한다. MTU 1,500바이트에는 각 단편의 IP 헤더도 포함되므로 한 단편에 실을 수 있는 데이터는 1,500 − 20 = 1,480바이트이다. 마지막 단편을 제외한 데이터 길이는 8바이트의 배수여야 하며, 1,480은 8의 배수이므로 그대로 사용할 수 있다.

처음 두 단편에 각각 1,480바이트씩 담으면 1,480 × 2 = 2,960바이트를 전송한다. 따라서 마지막 단편에 남는 데이터는 4,000 − 2,960 = **1,040바이트**이다. 마지막 단편에도 별도의 IP 헤더가 붙지만, 문제는 헤더를 제외한 크기를 요구하므로 20바이트를 더하지 않는다.

따라서 ㉠은 1,040바이트이며 ②와 일치한다.

NoteBase

문 9. 네트워크상의 특정 호스트를 발견하고 네트워크 서비스를 탐지하기 위해서 사용하는 포트 스캐닝(Port scanning) 도구로 가장 적절한 것은?

① wireshark

② netstat

③ nmap

④ nslookup

정답 3번

간단한 해설

nmap은 **호스트 발견과 포트·서비스 탐지**를 수행하는 네트워크 탐색 도구이다.

개념 구분

nmap: 호스트에 탐색용 패킷을 보내 응답을 분석하여 **호스트의 존재와 포트 상태, 제공 서비스**를 조사하는 도구이다. 포트 스캐닝은 통신의 접점인 포트가 열려 있는지 등을 확인하여 어떤 서비스가 접근 가능한지 파악하는 작업이다.

wireshark: 네트워크에서 오가는 **패킷을 캡처하고 프로토콜과 내용을 분석**하는 도구이다. 수집한 트래픽을 살펴보는 것이 주된 기능이므로, 문항이 묻는 대표적인 포트 스캐너와 구별된다.

netstat: 실행 중인 컴퓨터의 **현재 연결과 대기 중인 포트**, 네트워크 통계 등을 표시한다. 자신의 연결 상태를 조회하는 기능과 외부 호스트에 탐색 패킷을 보내 포트를 조사하는 기능은 다르다.

nslookup: DNS 서버에 질의하여 **도메인 이름과 IP 주소 등 DNS 정보**를 조회하는 도구이다. 이름 해석을 확인하는 용도이며 포트 스캐닝 도구는 아니다.

따라서 호스트 발견과 서비스 탐지를 위한 포트 스캐닝 도구는 ③ nmap이다.

NoteBase

문 10. 다음 보안 공격의 설명에 포함되지 않은 것으로 가장 적절한 것은?

㉠ 공격자가 자신의 IP주소나 메일 주소를 변조하여 다른 사용자나 시스템인 것처럼 위장하여 공격
㉡ 네트워크상에서 자신이 아닌 다른 시스템들의 패킷 교환을 도청하는 공격
㉢ 공격자가 공격대상의 IP주소로 위장하여 다량의 ICMP echo request 패킷을 브로드캐스팅 함으로써, 공격대상이 다량의 ICMP echo reply 패킷을 받도록 하는 공격

① Smurf attack
② Sniffing
③ Spoofing
④ Teardrop

정답 4번

간단한 해설

주소를 변조한 위장은 스푸핑, 패킷 도청은 스니핑, ICMP 응답을 피해자에게 집중시키는 공격은 스머프이다. **IP 단편 재조립의 취약점을 이용하는 티어드롭**은 설명에 포함되지 않는다.

보기별 해설

㉠ Spoofing: IP주소나 메일 주소 등 발신자 식별 정보를 변조하여 **다른 사용자·시스템으로 위장**하는 공격이다. 통신 내용을 엿보는 것이 아니라 상대가 잘못된 신원을 신뢰하게 한다는 점이 핵심이다.

㉡ Sniffing: 네트워크를 지나는 다른 시스템의 패킷을 수집·분석하는 **도청**이다. 발신자 주소를 바꾸어 위장하는 스푸핑과 달리, 관측한 통신에서 정보를 얻는 방식이다.

㉢ Smurf attack: 피해자의 IP주소를 출발지 주소로 위조한 ICMP echo request를 브로드캐스트로 보내 여러 호스트의 응답이 피해자에게 집중되게 한다. **다수의 ICMP echo reply가 피해자에게 반사**되어 네트워크나 시스템 자원을 소모시키는 서비스 거부 공격이다.

포함되지 않은 공격: Teardrop은 IP 단편의 위치 정보가 서로 겹치는 등의 비정상 단편을 이용해 **취약한 시스템의 재조립 처리에 오류**를 일으키는 서비스 거부 공격이다. 위 보기에는 단편 재조립에 관한 설명이 없으므로 정답은 ④이다.

NoteBase

문 11. 다음 <보기>에서 패스워드 해독 공격(Password cracking attack)으로 적절한 것을 모두 고른 것은?

<보기>
㉠ 사전공격(Dictionary attack)
㉡ 무차별 대입 공격(Brute-force attack)
㉢ 레이스 컨디션 공격(Race-condition attack)
㉣ 레인보우 테이블(Rainbow table)을 이용한 공격

① ㉠
② ㉡㉢
③ ㉠㉡㉢
④ ㉠㉡㉣

정답 4번

간단한 해설

사전공격·무차별 대입·레인보우 테이블은 비밀번호 후보를 시험하거나 해시값으로부터 후보를 찾는 방법이다. 레이스 컨디션 공격은 **작업의 실행 순서와 타이밍에 따른 취약점**을 이용하므로 구별된다.

보기별 해설

㉠ O: 사전공격은 자주 쓰는 단어와 예상 비밀번호를 후보로 모아 시험한다. 가능한 모든 문자열을 탐색하기보다 **가능성이 높은 후보를 먼저 대입**하는 패스워드 해독 방법이다.

㉡ O: 무차별 대입 공격은 정한 문자 집합과 길이 범위에서 **가능한 비밀번호 조합을 체계적으로 시도**한다. 후보 공간이 커질수록 필요한 시간이 증가하지만, 패스워드 후보를 직접 시험하는 해독 공격이다.

㉢ X: 레이스 컨디션 공격은 여러 작업의 실행 순서와 타이밍에 따라 결과가 달라지는 취약점을 이용한다. 예를 들어 자원을 검사한 시점과 실제 사용하는 시점 사이에 상태를 바꾸는 방식이다. **동시 실행·시점 차이의 취약점**을 악용하는 공격이지, 비밀번호 후보를 찾아내는 해독 기법 자체는 아니다.

㉣ O: 레인보우 테이블 공격은 미리 계산한 해시·축약 연산의 체인을 이용하여 저장된 해시값에 대응하는 비밀번호 후보를 찾는다. 매번 처음부터 모든 후보를 계산하는 대신 **사전 계산 결과와 저장 공간을 활용**한다. 서로 다른 솔트가 적용된 비밀번호에는 같은 테이블을 그대로 공통 적용하기 어렵다.

패스워드 해독 공격에 해당하는 것은 ㉠·㉡·㉣이므로 ④와 일치한다.

NoteBase

문 12. 유닉스에서 파일의 정보를 <보기>와 같이 확인하였을 때, 파일의 소유자(owner)에게 실행 권한을 부여하는 명령으로 가장 적절한 것은?

<보기>

-rw-rw-rw- 2 user staff 4096 2018-12-25 14:10 test.sh

① chmod u+x test.sh

② chmod o+x test.sh

③ chmod g=x test.sh

④ chmod 444 test.sh

정답 1번

간단한 해설

chmod의 **u+x**는 소유자(u)에게 실행 권한(x)을 추가(+)한다. 기존 읽기·쓰기 권한과 다른 사용자 부류의 권한은 유지한다.

핵심 풀이

권한 문자열 '-rw-rw-rw-'에서 첫 '-'는 일반 파일을, 뒤의 세 묶음은 차례로 소유자·그룹·기타 사용자의 권한을 나타낸다. 현재 소유자 user는 읽기(r)·쓰기(w) 권한만 있고 실행(x) 권한은 없다. staff는 소유 그룹이다.

chmod의 기호 모드에서 **u는 소유자, +는 추가, x는 실행 권한**을 뜻한다. 'chmod u+x test.sh'는 다른 권한을 유지하면서 소유자에게 실행 권한을 더하여 '-rwxrw-rw-'로 바꾼다.

'chmod o+x test.sh'의 o는 소유자가 아니라 **기타 사용자**이다. 'chmod g=x test.sh'는 그룹 권한을 실행만 남도록 지정하여 기존 그룹 읽기·쓰기 권한을 제거한다. 두 명령 모두 소유자에게 실행 권한을 추가하지 않는다.

숫자 모드의 읽기·쓰기·실행은 각각 4·2·1이며, 'chmod 444 test.sh'는 세 사용자 부류 모두에게 읽기 권한만 준다. 실행 권한을 부여하는 명령이 아니다.

따라서 소유자에게 실행 권한을 추가하는 명령은 ① 'chmod u+x test.sh'이다.

NoteBase

문 13. 윈도우즈에서 ARP 스푸핑(spoofing)공격에 대응하기 위하여, 물리적 주소 30-A3-E2-43-12-54와 인터넷 주소 198.12.25.78을 정적으로 연결하는 명령으로 가장 적절한 것은?

① arp - v 198.12.25.78 30-A3-E2-43-12-54

② arp - d 198.12.25.78 30-A3-E2-43-12-54

③ arp - g 198.12.25.78 30-A3-E2-43-12-54

④ arp - s 198.12.25.78 30-A3-E2-43-12-54

정답 4번

간단한 해설

ARP 명령의 **-s 옵션은 IP 주소와 MAC 주소의 정적 대응을 추가**한다. 인수는 IP 주소, MAC 주소 순서이다.

핵심 풀이

정적 연결: ARP 캐시는 IP 주소와 물리적 주소인 MAC 주소의 대응을 저장한다. **-s 옵션은 정적 ARP 항목을 추가**하므로, 알려진 올바른 주소 대응을 고정하는 데 사용한다.

주소의 순서: -s 뒤에는 **IP 주소 다음에 MAC 주소**를 지정한다. 따라서 198.12.25.78을 먼저, 30-A3-E2-43-12-54를 다음에 두어 두 주소를 연결한다.

다른 옵션: -v는 ARP 항목의 상세 표시, -d는 지정한 항목의 삭제, -g는 -a와 같은 ARP 항목 표시 기능이다. 이들은 **정적 대응을 추가하는 옵션이 아니다**.

따라서 -s와 IP 주소·MAC 주소를 차례로 제시한 ④가 요구한 명령에 해당한다.

NoteBase

문 14. 다음은 웹 클라이언트가 웹 서버에 접속할 때 발생하는 오류에 대한 설명이다. 이 설명의 상태코드로 가장 적절한 것은?

웹 클라이언트에서 웹 서버로 페이지를 요청 했을 때, 요청된 URL이 변경되거나 요청한 주소의 페이지가 없을 경우에 발생하는 오류이다.

① 204 No Content

② 304 Not Modified

③ 404 Not Found

④ 500 Internal Server Error

정답 3번

간단한 해설

요청한 주소에서 **페이지를 찾을 수 없는 경우**에는 404 Not Found가 해당한다. 서버 내부 처리 오류인 500과 구별한다.

개념 구분

지문은 요청한 주소에 해당하는 **페이지를 찾을 수 없는 상황**을 설명한다. URL이 바뀌었더라도 새 주소로 안내하는 리다이렉션이 아니라, 기존 주소에서 자원을 찾지 못한 경우이므로 404 Not Found에 해당한다.

204 No Content는 요청 처리는 성공했지만 응답 본문으로 보낼 내용이 없다는 뜻이다. 페이지를 찾지 못한 오류와는 다르다.

304 Not Modified는 조건부 GET·HEAD 요청에서 기존에 저장된 표현을 다시 사용할 수 있어 본문을 재전송할 필요가 없다는 뜻이다. **캐시의 유효성 확인**과 관련되며, 페이지가 없다는 뜻이 아니다.

404 Not Found는 요청 대상 자원의 현재 표현을 찾지 못했음을 나타낸다. 이 지문에서는 요청 주소에 페이지가 없다는 단서가 결정적이다.

500 Internal Server Error는 서버 내부의 예상하지 못한 문제 때문에 요청을 처리하지 못했음을 나타낸다. **서버 내부 처리 실패**와 요청 자원의 부재를 구별해야 한다.

따라서 지문에 가장 적절한 상태코드는 ③ 404 Not Found이다.

NoteBase

문 15. <보기 1>의 윈도우즈 레지스트리(Registry) 루트키와 <보기 2>의 설명을 연결한 것들 중에 가장 적절한 것은?

<보기 1>
(가) HKEY_USERS
(나) HKEY_CLASSES_ROOT
(다) HKEY_CURRENT_USER
(라) HKEY_LOCAL_MACHINE
<보기 2>
㉠ 시스템 관련 정보를 저장한다.
㉡ 컴퓨터에서 모든 계정에 관한 정보를 저장한다.
㉢ 현재 로그온 된 사용자와 관련된 데이터를 저장한다.
㉣ 파일 연관성과 COM(Component Object Model) 개체 등록 정보를 저장한다.

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

정답 3번

간단한 해설

HKEY_USERS는 사용자별 프로필, HKEY_CURRENT_USER는 **현재 사용자**의 설정을 구분한다.
HKEY_CLASSES_ROOT는 파일 연결·COM 등록, HKEY_LOCAL_MACHINE은 **컴퓨터 전체의 구성**에 해당한다.

NoteBase

대응 관계 해설

(가) HKEY_USERS → ㉡: 사용자 계정별 프로필 정보를 구분하여 보관하는 영역이다. 문항의 '모든 계정'은 현재 사용자 한 명만을 가리키는 HKEY_CURRENT_USER와 대비하는 설명이며, 실제로는 **로드된 사용자 프로필의 하이브**가 하위에 나타난다.

(나) HKEY_CLASSES_ROOT → ㉣: **파일 확장자·파일 형식의 연결과 COM 개체 등록** 정보를 제공한다. 파일을 어떤 프로그램으로 열지와 개체 클래스를 어떻게 처리할지에 관련된 정보를 다룬다.

(다) HKEY_CURRENT_USER → ㉢: **현재 로그온한 사용자의 설정**을 나타낸다. 해당 사용자의 환경과 응용프로그램 설정 등을 다루며, HKEY_USERS 아래의 해당 사용자 프로필을 참조한다.

(라) HKEY_LOCAL_MACHINE → ㉠: 특정 사용자 한 명의 설정이 아니라 **컴퓨터 전체의 시스템 구성**을 다룬다. 하드웨어·시스템·설치 소프트웨어 등 기계 단위의 정보를 저장한다.

따라서 (가)㉡, (나)㉣, (다)㉢, (라)㉠의 연결이므로 ③과 일치한다.

NoteBase

문 16. 다음 <보기>에서 버퍼 오버플로(Buffer overflow)에 취약한 C언어의 함수들을 모두 고른 것으로 가장 적절한 것은?

<보기>
㉠ strcat() ㉡ fgets() ㉢ sprintf()
㉣ strncpy() ㉤ strcmp() ㉥ realpath()

① ㉠㉢㉥
② ㉡㉢㉤
③ ㉠㉣㉤
④ ㉡㉣㉥

정답 1번

간단한 해설

strcat(), sprintf(), 호출자 버퍼를 사용하는 realpath()는 **목적지의 실제 크기를 인수로 받지 않는 쓰기 방식**에 주의해야 한다. 크기 제한을 지정하는 fgets()·strncpy()와 문자열을 비교하는 strcmp()를 구별한다.

NoteBase

보기별 해설

㉠ strcat(): 취약 함수에 해당한다. 목적지 문자열 뒤에 원본 문자열을 이어 붙이지만 **목적지 버퍼의 크기를 인수로 받지 않는다**. 기존 문자열과 추가 문자열, 종료 널 문자를 모두 담을 공간이 없으면 버퍼 경계를 넘어 쓸 수 있다.

㉡ fgets(): 이 문항의 취약 함수 묶음에 해당하지 않는다. 크기 인수 n을 받아 최대 n−1개의 문자를 읽고 종료 널 문자를 붙인다. **n을 실제 버퍼 크기 이하로 지정**하면 입력 길이를 제한할 수 있다. 잘못된 크기를 넘겨도 안전하다는 뜻은 아니다.

㉢ sprintf(): 취약 함수에 해당한다. 서식화한 결과를 문자열 버퍼에 쓰지만 **출력 버퍼 크기를 제한하는 인수가 없다**. 결과가 버퍼보다 길면 오버플로가 발생할 수 있다. 크기 제한 인수가 있는 snprintf()와 구별한다.

㉣ strncpy(): 이 문항의 취약 함수 묶음에 해당하지 않는다. n바이트 범위로 복사·널 채움을 제한하므로 n을 목적지 크기 이하로 지정해야 한다. 다만 원본 길이가 n 이상이면 **종료 널 문자가 자동 보장되지 않는다**. 따라서 크기와 문자열 종료를 관리하지 않으면 후속 처리에서 문제가 생길 수 있다.

㉤ strcmp(): 이 문항의 취약 함수 묶음에 해당하지 않는다. 두 문자열을 비교하여 대소 관계를 반환하며 **결과 문자열을 목적지 버퍼에 쓰지 않는다**. 유효하게 널 종료된 문자열을 전달해야 한다는 전제는 별개이다.

㉥ realpath(): 호출자가 제공한 버퍼에 정규화된 절대 경로를 저장하는 사용 방식에서는 **그 버퍼의 실제 크기를 전달하는 인수가 없다**. 충분한 경로 저장 공간을 확보하지 않으면 문제가 되므로 이 문항은 취약 함수로 분류한다. 충분한 크기를 확보하거나 지원되는 명세에서 널 포인터를 전달해 필요한 버퍼를 할당받는 안전한 사용 방식까지 불가능하다는 뜻은 아니다.

따라서 크기 제한 없는 쓰기 방식에 주의해야 하는 함수 묶음은 ㉠·㉢·㉥이며, ①과 일치한다.

NoteBase

문 17. 리눅스에서 각종 서비스들을 제공하기 위한 데몬(Daemon)에 대한 설명으로 가장 적절하지 않은 것은?

① syslogd - 로그기록 서비스를 제공한다.

② ntpd - 네트워크 파일시스템 서비스를 제공한다.

③ crond - 주기적으로 실행하도록 예약한 명령을 실행한다.

④ systemd - 시스템의 상태를 종합적으로 관리하는 역할을 수행한다.

정답 2번

간단한 해설

ntpd는 네트워크 파일시스템이 아니라 **NTP를 통한 시스템 시간 동기화**를 담당한다. 네트워크 파일시스템은 NFS와 관련된다.

선지별 해설

① O: syslogd는 프로그램 등이 보내는 로그 메시지를 받아 설정에 따라 파일 등에 기록하는 **시스템 로그 서비스**를 제공한다. 기록된 로그는 시스템 동작이나 오류를 확인하는 자료가 된다.

② X: ntpd는 NTP를 이용하여 기준 시각에 맞게 **시스템 시계를 동기화**하는 데몬이다. 네트워크 파일시스템 서비스는 NFS에 해당하며, ntpd의 시간 동기화 기능과 구별해야 한다. 따라서 가장 적절하지 않은 설명은 ②이다.

③ O: crond는 예약표에 지정한 시간 조건을 확인하여 해당 시각에 명령이나 프로그램을 실행하는 데몬이다. 매일·매주 같은 **주기적 작업의 예약 실행**에 사용한다.

④ O: systemd는 리눅스의 시스템·서비스 관리자이다. 부팅 과정에서 서비스를 시작하고 서비스의 실행 상태와 의존 관계 등을 관리하므로, **시스템과 서비스의 상태를 종합적으로 관리**한다는 설명에 해당한다.

NoteBase

문 18. Apache 웹 서버를 사용할 때 웹 로그에 기록되는 정보로 가장 적절하지 않은 것은?

① 클라이언트 호스트 명 또는 IP 주소

② 클라이언트 운영체제 및 브라우저 버전 정보

③ 클라이언트 요청에 대한 처리 상태를 나타내는 상태코드

④ 클라이언트 요청을 처리하는데 소요된 시간과 메모리 사용량

정답 4번

간단한 해설

통상적인 Apache 접근 로그에는 요청별 **메모리 사용량이 기본 항목으로 기록되지 않는다**. 처리 시간은 별도 로그 형식 설정으로 기록할 수 있으므로, 시간도 기록 불가능하다고 단정하지 않는다.

선지별 해설

① O: 접근 로그는 요청을 보낸 클라이언트의 IP 주소나 호스트명을 기록할 수 있다. 호스트명 조회 설정 등에 따라 표시가 달라지며, 프록시를 거치면 **접속한 프록시의 주소**가 기록될 수도 있다.

② O: 일반적으로 사용하는 Combined Log Format은 **User-Agent 요청 헤더**를 기록한다. 여기에는 클라이언트가 알리는 운영체제·브라우저 및 버전 정보가 포함될 수 있다. 다만 클라이언트가 보내는 값이므로 실제 환경을 독립적으로 검증한 정보는 아니다.

③ O: HTTP 상태코드는 요청 처리 결과를 나타내는 로그 항목이다. 예를 들어 200은 성공, 404는 요청한 자원을 찾지 못했음을 나타내며, 로그에서 **응답 결과**를 확인하는 데 쓰인다.

④ X: 통상적인 접근 로그가 요청별 처리 시간과 메모리 사용량을 모두 기본 기록하는 것은 아니다. 특히 **요청별 메모리 사용량은 일반적인 접근 로그 항목이 아니다**. 처리 시간 자체는 LogFormat에 %D나 %T를 지정하여 기록할 수 있으므로, Apache가 처리 시간을 전혀 기록할 수 없다는 뜻으로 이해하면 안 된다.

NoteBase

문 19. 다음 <보기> 중 허니팟(Honeypot)에 대한 설명으로 적절한 것을 모두 고른 것은?

<보기>
㉠ 공격자의 행동 패턴에 관한 정보를 수집한다.
㉡ 비정상적인 접근을 탐지하기 위하여 의도적으로 설치해 둔 시스템이다.
㉢ 허니팟이 공격자에게 쉽게 해킹당하지 않도록 취약점을 제거하는 보안조치를 취한다.
㉣ 침입자가 허니팟을 사용하는 동안 감시하는 역할을 한다.

① ㉠
② ㉡㉢
③ ㉢㉣
④ ㉠㉡㉣

정답 4번

간단한 해설

허니팟은 공격자를 유인하여 **침입 행위와 행동 패턴을 관찰**하는 시스템이다. 취약점을 모두 없애 접근을 막는 것과는 목적이 다르지만, 주변 시스템을 보호하기 위한 격리·통제는 필요하다.

NoteBase

보기별 해설

허니팟은 실제 서비스처럼 보이는 유인용 시스템을 두어 침입 시도와 공격 행위를 관찰하는 보안 수단이다. 운영 시스템을 보호하는 조치와, 공격자를 관찰 대상으로 유인하는 허니팟의 목적을 구별해야 한다.

㉠ O: 허니팟에서 발생하는 접근과 행동을 기록하면 공격 도구·명령·진행 순서 등 **공격자의 행동 패턴**을 분석할 수 있다. 수집한 정보는 탐지와 대응 방법을 개선하는 자료가 된다.

㉡ O: 정상 업무용 서비스가 아니라 의도적으로 마련한 유인 시스템이므로, 여기에 들어오는 의심스러운 접근을 관찰하여 비정상적인 활동을 탐지할 수 있다.

㉢ X: 허니팟의 핵심은 취약점을 모두 제거해 공격자가 접근하지 못하게 하는 것이 아니라, 공격자가 관심을 갖는 서비스나 취약한 환경을 제공·모사하여 **침입 시도를 관찰**하는 데 있다. 다만 허니팟이 다른 시스템을 공격하는 거점이 되지 않도록 격리와 통신 통제 등은 필요하다. 관찰 대상의 유인성과 주변 시스템 보호를 혼동하면 안 된다.

㉣ O: 침입자가 허니팟과 상호작용하는 동안 접속·명령·변경 사항 등을 감시하고 기록하여 공격의 진행 방식과 목적을 파악한다. 단순히 설치하는 것만이 아니라 **지속적인 관찰과 기록**이 중요하다.

따라서 적절한 보기는 ㉠·㉡·㉣이며, 이를 모두 포함한 ④와 일치한다.

NoteBase

문 20. 다음 <보기>에서 가상 사설망(VPN : Virtual Private Network)이 제공하는 보안 서비스로 적절한 것을 모두 고른 것은?

<보기>
㉠ 인증
㉡ 터널링
㉢ 패킷 필터링
㉣ 데이터 암호화

① ㉠㉢
② ㉡㉣
③ ㉡㉢㉣
④ ㉠㉡㉣

정답 4번

간단한 해설

보안 VPN은 상대를 **인증**하고, 터널로 논리적 통신 경로를 구성하며, 암호화로 내용을 보호한다. 패킷 필터링은 VPN 장비에 함께 들어갈 수 있지만 **방화벽의 접근 통제 기능**과 구별된다.

보기별 해설

㉠ O: 인증은 VPN 접속 사용자나 통신 상대의 신원을 확인하여 **허가된 주체가 연결하도록** 하는 기능이다. 공중망을 통해 사설망에 접근하므로 접속 상대를 확인하는 절차가 필요하다.

㉡ O: 터널링은 원래 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 공중망을 가로지르는 **논리적인 사설 통신 경로**를 만든다. 터널링 자체가 반드시 암호화를 뜻하는 것은 아니며, 보안 VPN은 암호화·인증과 함께 사용한다.

㉢ X: 패킷 필터링은 출발지·목적지 주소, 포트, 프로토콜 등의 규칙으로 패킷을 허용하거나 차단하는 **방화벽의 대표적인 접근 통제 기능**이다. VPN 장비에 함께 구현될 수 있지만, 이 문항에서 구별하는 VPN의 기본 기능인 인증·터널링·암호화 자체와는 다르다.

㉣ O: 데이터 암호화는 공중망에서 전송되는 데이터를 암호문으로 바꾸어 제3자가 내용을 쉽게 읽지 못하도록 한다. 보안 VPN에서 **전송 내용의 기밀성**을 보호하는 기능이다.

따라서 문항에서 VPN의 보안 기능으로 고르는 항목은 ㉠·㉡·㉣이며 ④와 일치한다.

NoteBase