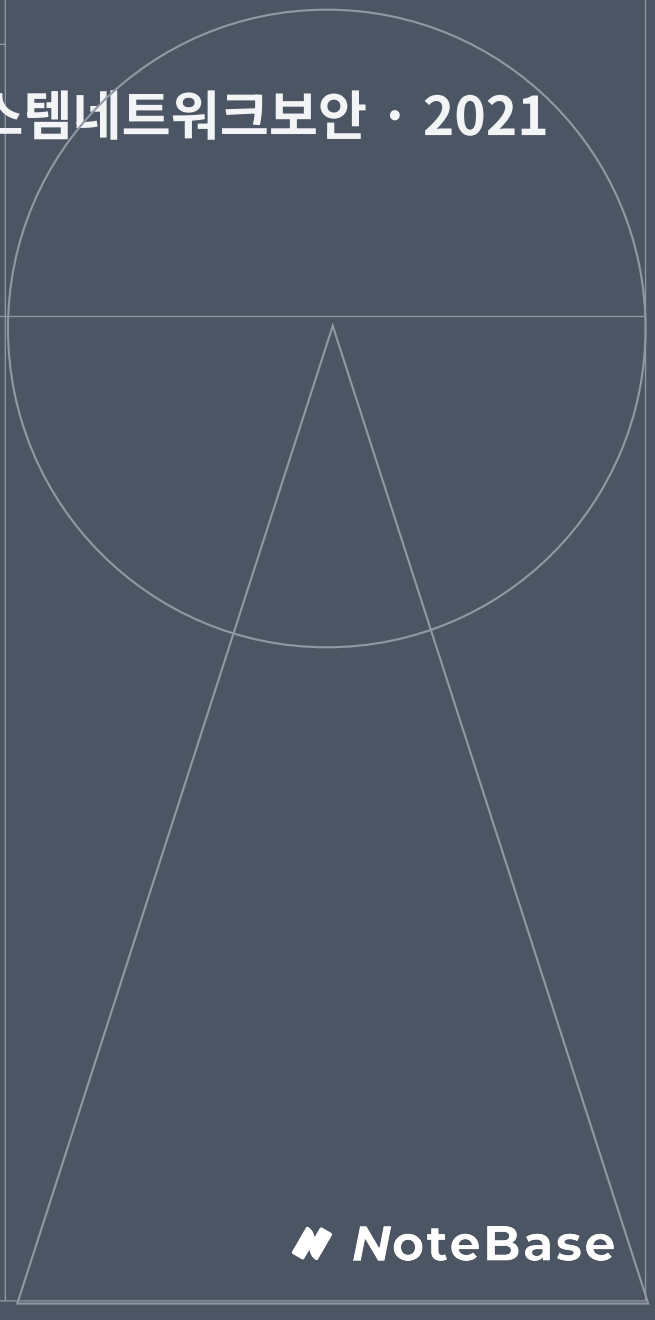
# 기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2021



NoteBase

# 기출OX 해설집

## 공무원/경찰/경력채용 · 시스템네트워크보안 · 2021

### 공무원/경찰/경력채용 · 시스템네트워크보안 · 2021

**문 1. 프로세스의 교착상태(Deadlock) 발생 조건에 대한 설명으로 가장 적절한 것은?**

① 점유와 대기(Hold and Wait): 프로세스가 각각 필요 자원에 대해 배타적 통제권을 요구하는 상태

② 상호배제(Mutual Exclusion): 프로세스가 점유한 자원은 처리가 끝날 때까지 강제로 해제될 수 없는 상태

③ 환형대기(Circular Wait): 프로세스의 순환 사슬이 존재하여 요청 자원에 대해 서로의 꼬리를 물고 있는 상태

④ 비선점(Non-Preemption): 프로세스가 다른 자원을 요구하면서 자신의 점유 자원을 해제하지 않고 대기하는 상태

**정답 3번**

**간단한 해설**

교착상태의 네 가지 필요조건은 상호배제, 점유와 대기, 비선점, 환형대기이다. **환형대기**는 프로세스들이 서로의 자원을 기다리며 **순환 대기 사슬**을 이루는 상태이다.

**선지별 해설**

① X. 제시된 설명은 **상호배제**에 해당한다. 상호배제는 한 자원을 한 번에 하나의 프로세스만 사용할 수 있는 조건이다. 점유와 대기는 이미 자원을 점유한 프로세스가 그 자원을 유지한 채 다른 자원을 기다리는 조건이다.

② X. 점유한 자원을 강제로 빼앗을 수 없다는 설명은 **비선점**에 해당한다. 자원은 점유한 프로세스가 사용을 마치고 자발적으로 반환해야 한다. 상호배제는 자원을 동시에 공유하여 사용할 수 없다는 뜻이다.

③ O. **환형대기**는 프로세스들이 순환 관계를 이루면서 각자 다음 프로세스가 점유한 자원을 기다리는 조건이다. 마지막 프로세스가 다시 첫 번째 프로세스의 자원을 기다리므로 대기 사슬이 닫힌 고리를 이룬다.

④ X. 다른 자원을 요구하면서 기존 점유 자원을 해제하지 않고 기다리는 설명은 **점유와 대기**에 해당한다. 비선점은 다른 프로세스나 운영체제가 점유 중인 자원을 강제로 회수할 수 없다는 조건이다.

따라서 교착상태 발생 조건과 설명이 올바르게 대응하는 것은 ③이다.

NoteBase

**문 2. 다음은 UNIX 디렉터리 구조에 대한 설명이다. <보기 1>의 디렉터리와 <보기 2>의 설명을 가장 적절히 연결한 것은?**

<보기 1>
(가) /var (나) /tmp (다) /etc (라) /home

<보기 2>
㉠ 시스템의 환경설정 파일을 포함하는 디렉터리
㉡ 임시파일을 저장하는 임시 디렉터리
㉢ 시스템 로그가 저장되는 디렉터리
㉣ 사용자의 홈 디렉터리

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

**정답 4번**

**간단한 해설**

/var 아래에는 **시스템 로그**, /tmp에는 임시파일, /etc에는 시스템 설정 파일, /home 아래에는 일반 사용자의 홈 디렉터리가 위치한다. 로그와 설정 파일의 저장 위치를 구별하면 된다.

NoteBase

**대응 관계 해설**

(가) /var → ㉣: 실행 중 내용이나 크기가 변하는 데이터를 저장하는 영역이다. 시스템 로그는 보통 그 하위의 **/var/log**에 저장되므로 시스템 로그 디렉터리 설명과 연결된다.

(나) /tmp → ㉡: 프로그램이 작업 도중 사용하는 **임시파일**을 저장한다. 영구 보관용이 아니며 시스템 정책에 따라 정리될 수 있다.

(다) /etc → ㉠: 시스템과 서비스의 **환경설정 파일**을 저장한다. 실행 결과인 로그가 아니라 동작 방식을 지정하는 설정 정보가 중심이다.

(라) /home → ㉢: 일반 사용자의 **홈 디렉터리**를 두는 위치로, 보통 사용자별 하위 디렉터리에 개인 파일과 설정을 저장한다.

따라서 (가)㉣, (나)㉡, (다)㉠, (라)㉢의 대응으로, ④와 일치한다.

NoteBase

**문 3. HTTP 상태 코드에 대한 설명으로 가장 적절하지 않은 것은?**

① 코드: 403, 설명(상태): 요청이 허용되지 않는 자원 요구(Forbidden)

② 코드: 404, 설명(상태): 서버에 요구된 URL을 찾을 수 없음(Not Found)

③ 코드: 500, 설명(상태): 서버 내부오류가 발생하여 더는 진행할 수 없음(Internal Server Error)

④ 코드: 501, 설명(상태): 서버 과부하로 서비스할 수 없음(Service Unavailable)

**정답 4번**

**간단한 해설**

**501은 필요한 기능을 지원하지 않는 Not Implemented**이다. 과부하·점검 등에 따른 일시적 서비스 불가는 503 Service Unavailable이므로 두 코드를 구별해야 한다.

**선지별 해설**

① O. 403 Forbidden은 서버가 요청을 이해했지만 **수행을 거부**했음을 뜻한다. 접근이 허용되지 않는 자원을 요구한 경우라는 설명이 이에 해당한다.

② O. 404 Not Found는 요청 대상 자원의 현재 표현을 찾지 못했거나 그 존재를 공개하지 않는 경우를 나타낸다. 요구된 URL에 해당하는 자원을 찾을 수 없다는 설명은 기본 의미에 맞는다.

③ O. 500 Internal Server Error는 서버에서 **예기치 않은 내부 오류**가 발생하여 요청을 처리하지 못한 경우이다. 서버 내부 문제라는 설명이 맞는다.

④ X. **501은 Not Implemented**로, 요청 수행에 필요한 기능을 서버가 지원하지 않을 때 사용한다. 일시적인 과부하나 점검 때문에 서비스할 수 없는 경우는 503 Service Unavailable이다. 따라서 501과 Service Unavailable을 연결한 설명이 부적절하다.

NoteBase

**문 4. 다음에서 설명하는 서버 공격에 대응하는 방법으로 가장 적절하지 않은 것은?**

C/C++ 컴파일러가 배열의 경계검사를 하지 않기 때문에 선언된 크기보다 더 큰 데이터를 기록하여 버퍼의 용량을 초과하는 것을 이용하는 공격

① 프로그램은 최소 권한으로 실행한다.

② 프로그래밍할 때는 경계값을 검사하는 안전한 함수를 사용한다.

③ 임시파일 사용 시 링크 상태, 파일의 종류, 파일의 소유자, 파일의 변경 여부 등을 점검한다.

④ scanf() 함수는 취약하므로 최대 입력받을 수 있는 문자 길이를 제한한다.

**정답 3번**

**간단한 해설**

제시문은 **버퍼 오버플로**를 설명한다. 버퍼 크기에 맞춘 입력 제한과 경계 검사가 핵심이며, 임시파일의 링크·소유자 점검은 주로 다른 유형의 취약점에 대응한다.

**선지별 해설**

① O: 프로그램을 **필요한 최소 권한**으로 실행하면 버퍼 오버플로가 악용되더라도 공격자가 행사할 수 있는 권한과 피해 범위를 줄일 수 있다. 메모리 경계 초과 자체를 없애는 조치는 아니지만, 공격 영향의 완화 대책에 해당한다.

② O: 입력 길이와 목적지 버퍼 크기를 검증하고 **경계를 초과하여 쓰지 않도록** 하는 함수를 올바르게 사용하면 버퍼 오버플로를 예방할 수 있다. 길이 인수나 종료 문자 처리까지 정확히 지정해야 한다.

③ X: 임시파일의 링크·종류·소유자·변경 여부 확인은 주로 **임시파일 바꿔치기와 경쟁 조건** 등에 대응하는 조치이다. 제시된 버퍼 오버플로의 직접 원인은 메모리 경계를 넘는 쓰기이므로, 입력 길이와 버퍼 용량 검증이 대응의 중심이 되어야 한다. 파일 검사 자체가 불필요하다는 뜻은 아니다.

④ O: scanf()에서 문자열을 길이 제한 없이 입력받으면 버퍼를 넘칠 수 있으므로 **입력 필드 폭**을 제한해야 한다. 특히 %s로 문자열을 저장할 때는 버퍼 크기에서 널 종료 문자 한 자리도 남겨야 한다. scanf()의 모든 사용이 언제나 취약하다는 뜻은 아니다.

NoteBase

**문 5. 윈도우 인증 구성요소 중 LSA(Local Security Authority)의 서비스 기능에 대한 설명으로 가장 적절한 것은?**

① 모든 계정의 로그인에 대한 검증 및 시스템 자원에 대한 접근 권한을 검사한다.

② 사용자, 그룹 계정 정보에 대한 데이터베이스를 관리한다.

③ SID(Security Identifier)를 기반으로 파일이나 디렉터리에 접근 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

④ 사용자 로그인 정보와 SAM(Security Account Manager) 데이터베이스 정보를 비교하여 인증 여부를 결정한다.

**정답 1번**

**출제 포인트**

윈도우 보안 구성요소의 역할을 구분하는 문제이다. LSA는 로그인 인증과 로컬 보안 정책을 담당하고, SAM·SRM·인증 패키지는 각각 계정 정보 관리·자원 접근 검사·인증 정보 검증을 맡는다.

**핵심 개념**

LSA(Local Security Authority): 로그인 인증을 수행하고 사용자 권한 등 로컬 보안 정책을 관리하는 보안 구성요소이다. 인증은 사용자가 누구인지 확인하는 과정이고, 접근 제어는 그 사용자가 자원을 이용할 권한이 있는지 판단하는 과정이다.
SAM(Security Accounts Manager): 로컬 사용자·그룹의 계정 정보를 저장하고 관리한다.
SRM(Security Reference Monitor): 파일 등 객체에 대한 접근 권한을 검사하고 감사 정책에 따라 감사 이벤트를 생성한다.
인증 패키지: LSA가 호출하여 로그인 정보를 검증하는 모듈이다. MSV1_0은 SAM 정보를 이용하는 인증 패키지의 예이다.

NoteBase

### 선지별 해설

이 문항의 O/X는 가장 적절한 설명으로 선택되는지 여부를 나타낸다.
① O: 로그인 검증과 시스템 자원에 대한 권한 관리를 포괄하여 LSA의 보안 서비스 역할을 가장 잘 설명한다. LSA는 인증을 수행하고 보안 정책과 권한 정보를 관리한다. 다만 개별 파일·디렉터리의 접근 허용 여부를 직접 검사하는 역할은 SRM과 구분한다.
② X: “사용자, 그룹 계정 정보에 대한 데이터베이스를 관리한다”는 내용은 SAM의 역할에 해당한다. 기능 설명 자체가 거짓인 것이 아니라 담당 구성요소가 다르다. 올바른 구분은 SAM이 로컬 계정 데이터베이스를 관리하고, LSA는 이를 인증에 활용한다는 것이다.
③ X: “파일이나 디렉터리에 접근 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다”는 SRM의 역할이다. SID는 사용자·그룹 등을 식별하는 값이며, 실제 접근 검사는 접근 토큰과 객체의 접근 제어 정보를 이용한다. 올바른 구분은 LSA가 보안 정책을 관리하고 SRM이 객체 접근 검사와 관련 감사 이벤트 생성을 수행한다는 것이다.
④ X: “로그인 정보와 SAM 데이터베이스 정보를 비교”하는 것은 LSA가 호출하는 인증 패키지의 구체적 처리에 해당한다. 예를 들어 MSV1_0은 SAM 정보를 확인하고 인증 결과를 LSA에 반환한다. LSA도 이 과정에 관여하므로 전혀 무관한 설명은 아니지만, LSA의 서비스 전반을 설명한 ①보다 범위가 좁다. 올바른 구분은 인증 패키지가 SAM 정보를 이용해 검증하고 LSA가 그 결과를 받아 로그인 인증을 처리한다는 것이다.

### 오답 포인트

④의 “인증 여부를 결정한다”만 보면 LSA로 판단하기 쉽다. 그러나 SAM과 로그인 정보를 비교하는 구체적 검증은 인증 패키지의 역할이며, LSA는 이를 호출하는 상위 보안 구성요소이다. 또한 ①의 포괄적인 권한 관리와 ③의 개별 객체 접근 검사를 같은 수준의 기능으로 혼동하기 쉽다.

### 다시 나오면 이렇게 판단

설명의 중심 기능을 구분한다. 로그인 인증과 보안 정책의 전반적 관리는 LSA, 사용자·그룹 계정 데이터베이스는 SAM, 객체 접근 검사와 감사 이벤트 생성은 SRM, SAM을 이용한 구체적 로그인 정보 검증은 인증 패키지에 연결한다.

### 암기 포인트

LSA는 인증·정책, SAM은 계정 정보, SRM은 접근 검사·감사, 인증 패키지는 로그인 정보 검증이다.

NoteBase

**문 6. 다음에서 설명하는 웹 서비스의 공격 유형으로 가장 적절한 것은?**

사용자가 자신의 의지가 아닌 공격자가 의도한 행위를 특정 웹 사이트에 요청하는 것으로 로그인한 피해자의 웹 브라우저가 취약한 웹 어플리케이션에 피해자의 세션쿠키와 공격자의 변조된 HTTP 요청을 강제로 전송하도록 하는 공격

① XXE(XML External Entities)

② CSRF(Cross-Site Request Forgery)

③ SQL Injection

④ XSS(Cross-Site Scripting)

**정답 2번**

**간단한 해설**

피해자의 브라우저가 **인증된 세션을 이용해 의도하지 않은 요청**을 보내게 하는 공격은 CSRF이다. 세션 쿠키가 함께 전송되는 점을 악용하여 피해자의 권한으로 동작하게 한다.

**핵심 풀이**

CSRF는 **로그인한 사용자의 권한으로 원하지 않는 요청**을 보내도록 유도하는 공격이다. 지문에서는 피해자가 이미 인증되어 있고, 브라우저가 해당 사이트의 세션 쿠키를 요청과 함께 보내므로 서버가 공격자가 의도한 요청을 피해자의 요청으로 처리할 수 있다. 핵심은 세션 쿠키를 훔치는 것이 아니라, 피해자의 브라우저가 가진 인증 상태를 악용한다는 점이다.

XSS는 웹 페이지에 주입된 스크립트가 피해자의 브라우저에서 실행되게 하는 공격이다. CSRF는 **의도하지 않은 인증 요청의 전송**이 핵심이므로, 취약한 사이트 안에서 공격자 스크립트가 실행되어야만 하는 것은 아니다.

XXE는 XML 파서의 외부 엔터티 처리를 악용하는 공격이고, SQL Injection은 입력값을 통해 데이터베이스 질의의 구조나 의미를 바꾸는 공격이다. 지문에는 XML 외부 엔터티나 SQL 질의 조작이 아니라 인증된 브라우저의 요청 위조가 제시되어 있다.

따라서 지문의 공격 유형은 ② CSRF(Cross-Site Request Forgery)이다.

NoteBase

**문 7. UNIX 명령어에 대한 설명으로 가장 적절하지 않은 것은?**

① pwd: 로그인에 필요한 비밀번호를 변경한다.

② cat: 파일 내용을 화면에 출력한다.

③ ps: 현재 시스템에서 실행 중인 프로세스 정보를 출력한다.

④ chmod: 파일에 대한 접근권한을 변경한다.

**정답 1번**

**간단한 해설**

**pwd는 현재 작업 디렉터리의 경로를 출력**하는 명령이다. 비밀번호를 변경하는 passwd와 이름이 비슷하므로 기능을 구별해야 한다.

**선지별 해설**

① X. pwd는 print working directory의 약자로, **현재 작업 디렉터리의 경로**를 출력한다. 로그인 비밀번호를 변경하는 명령은 passwd이므로 두 명령을 혼동한 설명이다.

② O. cat은 파일 내용을 읽어 표준 출력으로 내보낸다. 표준 출력이 화면에 연결된 일반적인 경우 파일 내용이 화면에 표시되며, 여러 파일을 차례로 이어 출력할 수도 있다.

③ O. ps는 **프로세스의 상태 정보를 조회**하는 명령이다. 프로세스 식별자와 실행 명령 등을 표시하며, 어떤 프로세스를 대상으로 어떤 항목을 표시할지는 옵션에 따라 달라진다. 지속적으로 화면을 갱신하는 명령이라는 뜻은 아니다.

④ O. chmod는 파일이나 디렉터리의 접근권한을 변경한다. 소유자·그룹·기타 사용자에 대한 읽기·쓰기·실행 권한 등을 설정할 때 사용하며, 소유자를 바꾸는 chown과 구별한다.

NoteBase

**문 8. UNIX 구성요소 중 커널(Kernel)에 대한 설명으로 적절한 것을 모두 고른 것은?**

㉠ 주기억장치에 상주하여 CPU, 메인 메모리, 하드디스크 등의 하드웨어 자원을 제어한다.
㉡ 프로세스 스케줄링, 기억장치 및 파일관리, 입출력 서비스 기능을 제공한다.
㉢ 운영체제와 사용자가 대화하기 위한 기반을 제공하는 프로그램으로 명령어 해석기 기능을 수행한다.

① ㉠㉡
② ㉠㉢
③ ㉡㉢
④ ㉠㉡㉢

**정답 1번**

**간단한 해설**

커널은 **하드웨어 자원 관리와 프로세스·메모리·파일·입출력 서비스**를 담당한다. 명령어 해석기는 셸이므로 적절한 보기는 **㉠과 ㉡**이다.

**보기별 해설**

㉠ O: 커널은 운영체제의 핵심 부분으로, 실행 중 주기억장치에 상주하며 **CPU·메모리·저장장치 등 하드웨어 자원을 관리**한다. 응용 프로그램은 시스템 호출 등의 인터페이스를 통해 커널이 제공하는 기능을 이용한다.

㉡ O: 커널은 프로세스에 CPU를 배분하는 스케줄링, 메모리 관리, 파일 시스템 관리와 장치 입출력 등의 서비스를 제공한다. 이들은 여러 프로그램이 **시스템 자원을 안전하고 효율적으로 사용**하도록 조정하는 핵심 기능이다.

㉢ X: 사용자 명령을 해석하고 실행을 요청하는 명령어 해석기는 **셸(shell)**이다. 셸은 사용자와 운영체제 사이의 인터페이스 역할을 하고, 커널은 실제 자원 관리와 시스템 서비스를 담당하므로 두 구성요소를 구별해야 한다.

㉠과 ㉡을 함께 고른 조합은 ①이다.

NoteBase

**문 9. 주기억장치 배치전략 기법으로 First-Fit(최초 적합), Best-Fit(최적 적합), Worst-Fit(최악 적합) 방법을 사용할 경우, 다음과 같은 기억장소 리스트에서 25K 크기의 작업이 할당되는 것을 가장 적절하게 연결한 것은? (단, 영역 탐색은 위에서 아래(㉠→㉣)로 한다고 가정)**

| 영역 번호 | 영역 크기 | 상태 |
|---|---|---|
| ㉠ | 25K | 사용 중 |
| ㉡ | 50K | 공백 |
| ㉢ | 20K | 공백 |
| ㉣ | 40K | 공백 |

① First-Fit: ㉠, Best-Fit: ㉣, Worst-Fit: ㉢

② First-Fit: ㉡, Best-Fit: ㉠, Worst-Fit: ㉢

③ First-Fit: ㉠, Best-Fit: ㉠, Worst-Fit: ㉡

④ First-Fit: ㉡, Best-Fit: ㉣, Worst-Fit: ㉡

**정답 4번**

**간단한 해설**

25K 작업이 들어갈 수 있는 빈 영역은 ㉡ **50K와** ㉣ **40K**이다. 최초 적합은 먼저 나오는 ㉡, 최적 적합은 더 작은 ㉣, 최악 적합은 더 큰 ㉡을 선택한다.

NoteBase

**계산 과정**

할당 가능 영역: 요청 크기는 25K이다. ㉠은 크기가 25K여도 **이미 사용 중**이므로 제외하고, ㉢의 20K는 요청보다 작아 제외한다. 빈 영역 중 충분한 공간은 ㉡ 50K와 ㉣ 40K이다.

First-Fit: 위에서 아래로 탐색하여 처음 만나는 할당 가능한 영역을 선택한다. ㉠을 건너뛰면 ㉡ **50K가 처음**이므로 ㉡에 할당한다.

Best-Fit: 할당 가능한 영역 중 요청 크기에 가장 가까운 작은 영역을 선택한다. 남는 공간은 ㉡에서 50K − 25K = 25K, ㉣에서 40K − 25K = 15K이므로 ㉣ **40K**를 선택한다.

Worst-Fit: 할당 가능한 빈 영역 중 가장 큰 영역을 선택한다. 50K가 40K보다 크므로 ㉡ **50K**에 할당한다.

각 전략을 같은 초기 상태에 독립적으로 적용한 결과는 First-Fit ㉡, Best-Fit ㉣, Worst-Fit ㉡이며, 이 연결은 ④이다.

NoteBase

**문 10. ARP 스푸핑(Spoofing) 공격에 대한 설명으로 가장 적절하지 않은 것은?**

① MAC 주소를 변조하여 공격대상이 전송하는 데이터그램을 가로채는 공격이다.

② ARP 응답 메시지가 지속적으로 빈번하게 발생하고 있다면 ARP 스푸핑 공격을 의심할 수 있다.

③ ARP 테이블을 정적(static)으로 설정하면 ARP 스푸핑 공격을 방어할 수 있다.

④ ARP 테이블에 여러 MAC 주소에 대해서 동일한 IP 주소가 중복으로 확인되면 ARP 스푸핑 공격을 의심할 수 있다.

**정답 4번**

**간단한 해설**

ARP 스푸핑은 IP–MAC 대응 정보를 속여 통신을 공격자에게 유도한다. 전형적인 테이블 징후는 **여러 IP주소가 같은 공격자 MAC주소를 가리키는 것**이며, 실제 판단에는 정상 구성과 주소 변경 이력도 확인해야 한다.

**선지별 해설**

① O. ARP 스푸핑은 거짓 ARP 정보를 보내 **IP주소에 대응하는 MAC주소 정보를 속이는 공격**이다. 피해자가 보내는 프레임의 목적지를 공격자 쪽으로 바꾸어 데이터그램을 가로챌 수 있다. 여기서 MAC주소 변조는 전달되는 주소 대응 정보의 위조를 뜻하며, 공격자 장치 자체의 MAC주소를 반드시 변경해야 한다는 뜻은 아니다.

② O. 공격자가 거짓 주소 대응을 유지하려고 ARP 응답을 반복해서 보내면 비정상적으로 빈번한 응답이 관찰될 수 있다. 이는 조사할 징후이지, 응답이 많다는 사실만으로 공격이 확정되는 것은 아니다.

③ O. 필요한 상대의 **정확한 IP–MAC 대응을 정적 항목으로 고정**하면 거짓 동적 응답으로 그 항목이 바뀌는 것을 막을 수 있다. 보호할 대상의 대응을 올바르게 설정·관리해야 하며, 한 항목을 고정했다고 네트워크 전체가 보호되는 것은 아니다.

④ X. 이 문제는 전형적인 ARP 테이블 이상 징후의 대응 방향을 거꾸로 설명한 점을 묻는다. 일반적인 같은 인터페이스의 ARP 캐시는 IP주소별로 MAC주소를 보관하며, 대표적인 중간자 공격에서는 **여러 대상 IP주소가 동일한 공격자 MAC주소에 연결**될 수 있다. 다만 실제 조사에서 동일 IP주소의 MAC주소가 바뀌거나 충돌하는 현상도 의심할 수 있으므로, 모든 IP주소 충돌이 공격과 무관하다는 뜻은 아니다. 또한 동일 MAC주소의 반복도 정상 구성에서 가능하므로 추가 확인이 필요하다.

NoteBase

**문 11. OSI 참조모델의 각 계층에서 사용하는 프로토콜로 가장 적절하지 않은 것은?**

① 데이터링크 계층: Ethernet, Token Ring

② 네트워크 계층: IPSec, IGMP

③ 전송 계층: TCP, TLS

④ 응용 계층: PPP, HTTP

**정답 4번**

**간단한 해설**

PPP는 점대점 링크에서 데이터를 전달하는 **데이터링크 계층 프로토콜**이다. HTTP는 응용 계층에 속하지만 PPP까지 응용 계층으로 묶을 수는 없다.

**선지별 해설**

① O: Ethernet과 Token Ring은 근거리 통신망에서 프레임을 주고받고 공유 전송매체에 접근하는 방식을 규정한다. 물리적 전송 규격과도 관련되지만, 이 문항에서는 프레임 처리와 매체 접근 제어라는 **데이터링크 계층 기능**에 따라 분류한다.

② O: IPsec은 IP 패킷에 인증·무결성·기밀성 등의 보안 서비스를 적용하는 네트워크 계층 보안 프로토콜군이다. IGMP는 IPv4 환경에서 호스트의 멀티캐스트 그룹 가입 정보를 인접 라우터에 알리므로 네트워크 계층에 분류한다.

③ O: TCP는 종단 사이의 신뢰성 있는 데이터 전달을 제공하는 전송 계층 프로토콜이다. TLS는 TCP와 같은 신뢰성 있는 전송 위에서 암호화·무결성·인증을 제공하며, **전송 계층의 보안 기능**으로 묶어 설명하는 분류가 있다. 여기서는 그 기능별 분류를 따른다. TLS가 TCP 자체의 전송 기능을 대신한다는 뜻은 아니며, 실제 프로토콜의 적층 위치를 엄격히 나누는 설명에서는 TCP 위의 별도 계층으로 표현하기도 한다.

④ X: HTTP는 웹 자원을 요청하고 응답하는 응용 계층 프로토콜이지만, PPP는 점대점 연결에서 네트워크 계층 데이터그램을 캡슐화하고 링크를 설정·관리한다. 따라서 PPP는 **응용 계층이 아니라 데이터링크 계층**으로 분류해야 한다.

NoteBase

**문 12. 윈도우 운영체제 감사정책에 대하여 <보기 1>의 용어와 <보기 2>의 설명을 가장 적절하게 연결한 것은?**

<보기 1>
(가) 시스템 이벤트 감사 (나) 계정 관리 감사
(다) 개체 액세스 감사 (라) 프로세스 추적 감사

<보기 2>
㉠ 프로세스 생성, 프로세스 종료, 핸들 복제 및 간접적 개체 액세스 등의 이벤트에 대한 추적 정보 감사
㉡ 사용자가 컴퓨터를 시작, 종료할 경우 또는 컴퓨터 보안이나 보안 로그에 영향을 주는 이벤트 감사
㉢ 파일, 폴더, 프린터, 레지스트리 키 등과 같은 개체에 접근하는 사용자의 이벤트 감사
㉣ 사용자나 그룹을 생성, 변경, 삭제, 암호설정 등의 이벤트 감사

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

**정답 2번**

**간단한 해설**

계정의 생성·변경·삭제는 **계정 관리 감사**, 프로세스 생성·종료와 핸들 복제는 **프로세스 추적 감사**에 해당한다. 시스템 상태 변화와 보호 대상 개체 접근도 각각 별도의 감사 범주로 구별한다.

NoteBase

**대응 관계 해설**

(가) 시스템 이벤트 감사 → ㉡: 컴퓨터의 **시작·종료와 시스템 보안 상태**에 관한 사건을 기록하는 범주이다. 보안이나 보안 로그에 영향을 주는 이벤트라는 단서가 이에 해당한다.

(나) 계정 관리 감사 → ㉣: 사용자·그룹의 생성, 변경, 삭제와 암호 설정처럼 **계정 자체를 관리하는 작업**을 대상으로 한다. 단순한 파일 접근이나 프로그램 실행과 구별된다.

(다) 개체 액세스 감사 → ㉢: 파일, 폴더, 프린터, 레지스트리 키 등 **보호 대상 개체에 대한 접근**을 기록한다. 실제 기록에는 감사 정책과 해당 개체의 SACL 등 감사 설정이 적용된다.

(라) 프로세스 추적 감사 → ㉠: 프로세스의 생성·종료, 핸들 복제, 간접적 개체 액세스 등 **프로그램 실행 과정의 상세 동작**을 추적한다. 개체에 접근했는지만 보는 범주와 달리 프로세스 활동의 흐름이 중심이다.

따라서 (가)㉡, (나)㉣, (다)㉢, (라)㉠으로 연결되며, ②와 일치한다.

NoteBase

**문 13. <보기 1>의 공격 기법과 <보기 2>의 설명을 가장 적절하게 연결한 것은?**

<보기 1>
(가) HTTP GET Flooding Attack (나) DNS Spoofing Attack
(다) Smurf Attack (라) SYN Flooding Attack
<보기 2>
㉠ 접속하려는 웹 서버의 IP 주소를 조작된 IP 주소로 알려주어 공격대상자가 악의적인 사이트로 접속하게 하는 공격
㉡ TCP SYN 패킷을 넘치게 전달하여 정상적인 서비스를 받지 못하도록 하는 공격
㉢ 여러 에이전트가 특정 웹 페이지를 동시에 요청하여 웹 서버가 감당하기 어렵게 하는 공격
㉣ 대량의 ICMP echo reply를 수신하도록 하는 공격

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

**정답 1번**

**간단한 해설**

각 공격의 핵심은 **웹 요청, DNS 주소 위조, ICMP 응답, TCP SYN**이다. 이 단서를 구분하면 HTTP GET Flooding은 ㉢, DNS Spoofing은 ㉠, Smurf는 ㉣, SYN Flooding은 ㉡과 연결된다.

NoteBase

**대응 관계 해설**

(가) HTTP GET Flooding Attack → ㉢. 여러 에이전트가 특정 웹 페이지에 **HTTP GET 요청을 대량으로 보내** 웹 서버의 처리 자원을 소모시키는 공격이다. 웹 페이지를 동시에 요청하여 서버가 감당하기 어렵게 한다는 설명과 대응한다.

(나) DNS Spoofing Attack → ㉠. 도메인 이름에 대한 **DNS 응답의 IP 주소를 위조**하여 사용자가 의도한 서버 대신 다른 주소로 접속하게 만드는 공격이다. 조작된 IP 주소를 알려 악의적인 사이트로 유도한다는 설명과 대응한다.

(다) Smurf Attack → ㉡. ICMP를 이용하는 반사·증폭 공격으로, 여러 호스트의 **ICMP Echo Reply가 피해자에게 집중**되도록 하여 자원을 소모시킨다. 핵심은 피해자가 대량의 응답 패킷을 수신한다는 점이다.

(라) SYN Flooding Attack → ㉡. TCP 연결 수립을 시작하는 **SYN 패킷을 대량 전송**하여 서버의 연결 대기 자원을 소모시키고 정상적인 연결을 어렵게 만드는 공격이다. TCP SYN 패킷이 넘치게 전달된다는 설명과 대응한다.

따라서 (가)–㉢, (나)–㉠, (다)–㉡, (라)–㉡으로 연결한 ①이 적절하다.

NoteBase

**문 14. 다음은 어떤 라우터가 갖고 있는 포워딩 테이블이다. 이 라우터에 목적지 주소로 “192.168.7.200”인 패킷이 수신되었을 때 라우터가 수행하는 동작으로 가장 적절한 것은?**

| 네트워크 주소 | 네트워크 마스크 | 다음홉(nexthop) 주소 | 인터페이스 |
|---|---|---|---|
| 192.168.7.128 | 255.255.255.192 | - | eth0 |
| 192.168.7.0 | 255.255.255.0 | - | eth1 |
| 0.0.0.0 | 0.0.0.0 | 192.168.8.1 | eth2 |

① eth0 인터페이스로 전송

② eth1 인터페이스로 전송

③ eth2 인터페이스로 전송

④ 수신된 패킷을 폐기

**정답 2번**

**간단한 해설**

목적지 192.168.7.200은 eth0의 /26 범위에는 없고, **eth1의 192.168.7.0/24**와 일치한다. 기본 경로보다 /24 경로가 우선하므로 eth1로 전송한다.

**계산 과정**

1. 목적지 주소는 192.168.7.200이다. eth0의 경로는 192.168.7.128/26으로, 마스크 255.255.255.192의 주소 범위는 **192.168.7.128~192.168.7.191**이다. 목적지의 마지막 옥텟 200은 이 범위 밖이므로 eth0 경로와 일치하지 않는다.

2. eth1의 경로는 192.168.7.0/24이며 마스크는 255.255.255.0이다. 목적지와 마스크를 비트 AND하면 **192.168.7.0**이므로 이 경로와 일치한다.

3. eth2의 0.0.0.0/0은 모든 목적지와 일치하는 기본 경로이다. 라우터는 일치한 경로 중 **접두사 길이가 가장 긴 경로**를 선택하므로, /0보다 구체적인 /24 경로를 사용한다. 따라서 eth1 인터페이스로 전송하는 ②가 적절하다.

NoteBase

**문 15. IPv6에 대한 설명으로 가장 적절하지 않은 것은?**

① IPv6는 128비트의 주소 필드를 갖고 있어서 IPv4보다 더 많은 주소를 사용할 수 있다.

② 네트워크의 신뢰도가 높아져서 IPv4 헤더의 checksum 필드가 IPv6 헤더에서는 삭제되었다.

③ IPv6에서 기본 헤더의 길이는 40바이트로 고정된다.

④ IPv6에서 라우터는 크기가 큰 데이터그램을 여러 개의 작은 데이터그램으로 단편화할 수 있다.

**정답 4번**

**간단한 해설**

IPv6 단편화는 **출발지 노드가 수행**하며 중간 라우터는 수행하지 않는다. 너무 큰 패킷은 라우터가 폐기하고 출발지에 크기 초과를 알린다.

**선지별 해설**

① O: IPv6 주소의 길이는 **128비트**로, 32비트인 IPv4보다 훨씬 큰 주소 공간을 제공한다. 주소 길이와 기본 헤더 전체 길이를 혼동하지 않아야 한다.

② O: IPv6 기본 헤더에는 **헤더 체크섬 필드가 없다**. 링크 계층과 상위 계층의 오류 검출을 활용하면서 중복 검사와 라우터의 재계산 부담을 줄이는 설계이다. 네트워크 신뢰도가 높아졌다는 표현은 이러한 배경을 요약한 것이며, 모든 전송 오류가 사라졌다는 의미는 아니다.

③ O: IPv6의 **기본 헤더는 40바이트**로 고정되어 있다. 추가 기능은 확장 헤더로 표현할 수 있으므로, 확장 헤더와 데이터까지 포함한 전체 패킷 길이가 항상 40바이트라는 뜻은 아니다.

④ X: IPv6에서 단편화는 **출발지 노드만** 수행하며, 전달 경로상의 라우터는 패킷을 단편화하지 않는다. 전송할 링크의 MTU보다 큰 패킷을 만나면 라우터는 이를 폐기하고 ICMPv6 Packet Too Big 메시지로 출발지에 알린다.

NoteBase

**문 16. UNIX 시스템에서 다음과 같이 출력하기 위한 명령어로 가장 적절한 것은?**

| 프로토콜 | 로컬주소 | 외부주소 | 상태 |
|---|---|---|---|
| TCP | 192.168.0.2:5223 | 112.51.2.150:6211 | ESTABLISHED |
| TCP | 192.168.0.2:6122 | 220.12.3.4:5134 | TIME_WAIT |
| TCP | 192.168.0.2:7742 | 220.12.3.4:7785 | CLOSE_WAIT |

① nslookup

② nmap

③ netstat

④ traceroute

**정답 3번**

**간단한 해설**

**netstat**은 네트워크 연결의 주소·포트와 상태를 확인하는 명령이다. 제시된 **ESTABLISHED, TIME_WAIT, CLOSE_WAIT**는 TCP 연결 상태를 나타낸다.

**핵심 풀이**

표에는 **프로토콜, 로컬 주소와 포트, 외부 주소와 포트, TCP 상태**가 나란히 표시되어 있다. 예를 들어 첫 행은 로컬 192.168.0.2:5223과 외부 112.51.2.150:6211 사이의 TCP 연결을 나타낸다. 이처럼 현재 시스템의 네트워크 연결을 주소·포트·상태별로 보여 주는 명령은 netstat이다.

표의 **ESTABLISHED**는 연결이 성립된 상태이고, TIME_WAIT는 연결 종료 과정에서 지연된 패킷 등에 대비해 일정 시간 기다리는 상태이다. CLOSE_WAIT는 상대방의 연결 종료 요청을 받은 뒤 로컬 응용프로그램이 연결을 닫기를 기다리는 상태이다. 이러한 연결 상태 열이 명령어를 식별하는 핵심 단서이다.

nslookup은 DNS 정보를 조회하고, nmap은 대상 호스트와 포트 등을 조사하며, traceroute는 목적지까지의 경유 경로를 확인한다. 이들은 로컬 시스템의 TCP 연결 현황을 보여 주는 표의 용도와 구별된다.

따라서 가장 적절한 명령어는 netstat인 ③이다.

NoteBase

**문 17. 보안 솔루션에 대한 용어설명으로 가장 적절하지 않은 것은?**

① 방화벽(Firewall)은 외부 네트워크와 내부 네트워크 사이에 위치하여 트래픽을 통제하는 시스템이다.

② 침입방지시스템(IPS: Intrusion Prevention System)은 공격을 탐지하여 자동으로 대응조치를 수행하는 예방적 통제 시스템이다.

③ 비정상탐지(Anomaly Detection) 방법은 미리 학습된 공격 패턴과 유사한 활동을 차단하여 내부 시스템을 보호한다.

④ 허니팟(Honeypot)은 비정상적인 접근을 탐지하려고 의도적으로 설치해 둔 시스템으로 공격자를 유인하여 정보를 얻는 용도로 활용한다.

**정답 3번**

**간단한 해설**

비정상 탐지는 **정상 행위의 기준에서 벗어난 활동**을 찾아낸다. 알려진 공격 패턴과의 일치·유사성을 찾는 방법은 시그니처 기반 탐지이다.

**선지별 해설**

① O: 방화벽은 서로 다른 신뢰 영역 사이에서 보안 정책에 따라 **트래픽을 허용하거나 차단**한다. 외부망과 내부망의 경계에 배치하는 것은 대표적인 구성이다.

② O: IPS는 침입 시도를 탐지하는 데 그치지 않고 패킷 차단이나 연결 종료 같은 **자동 대응**을 수행하여 공격의 진행을 막는다. 따라서 예방적 통제 기능을 갖는다.

③ X: 알려진 공격 패턴과 현재 활동을 비교하는 것은 **오용 탐지 또는 시그니처 기반 탐지**이다. 비정상 탐지는 정상적인 행위의 기준을 만들고 **정상 기준에서 벗어나는 정도**로 이상을 판단한다. 따라서 학습된 공격 패턴과의 유사성을 비정상 탐지의 기준으로 제시한 ③이 가장 적절하지 않다.

④ O: 허니팟은 공격자의 관심을 끌도록 준비한 유인 시스템이다. 정상 업무용 자원과 구분해 접근을 관찰함으로써 공격 시도와 수법에 관한 정보를 수집하는 데 활용한다.

NoteBase

**문 18. VPN(Virtual Private Network)에 대한 설명으로 적절한 것을 모두 고른 것은?**

㉠ VPN은 인터넷과 같은 공중망을 이용하여 사설망을 구성하는 기술이다.
㉡ L2TP나 PPTP와 같은 2계층 터널링 프로토콜을 사용할 수 있다.
㉢ IPSec VPN을 활용하기 위해서는 응용 계층의 수정이 필요하다.
㉣ SSL VPN은 대부분의 웹 브라우저가 이미 지원하고 있어서 site-to-site 연결에서 주로 활용한다.

① ㉡㉢
② ㉠㉡
③ ㉠㉢㉣
④ ㉠㉡㉣

**정답 2번**

**간단한 해설**

VPN에는 2계층 터널링 방식도 사용할 수 있으며, IPsec은 응용 프로그램의 수정을 일반적으로 요구하지 않는다. 브라우저 기반 SSL VPN의 대표 용도는 **사용자 원격 접속**이지 지점 간 연결이 아니다.

**보기별 해설**

㉠ O. VPN은 인터넷 등 공유된 통신 기반 위에 **논리적인 사설 통신 경로**를 구성하는 기술이다. 물리적인 전용 회선을 새로 설치하지 않고도 조직의 내부망이나 원격 사용자를 연결할 수 있다.

㉡ O. L2TP와 PPTP는 2계층 터널링 프로토콜로 분류하며 VPN 구성에 사용될 수 있다. 터널링과 암호화는 구별해야 하며, L2TP는 자체적인 기밀성 보호를 위해 통상 IPsec과 결합한다. 여기서는 프로토콜의 분류와 사용 가능성을 묻는 것이지, 오래된 PPTP를 안전한 신규 구성으로 권장하는 것은 아니다.

㉢ X. IPsec은 **네트워크 계층에서 IP 패킷을 보호**하므로 일반적으로 응용 프로그램 자체를 수정할 필요가 없다. VPN 장비·운영체제의 보안 기능과 정책을 설정하는 것과 응용 계층 프로그램 코드를 변경하는 것은 다르다.

㉣ X. 브라우저의 SSL/TLS 기능을 활용하는 SSL VPN은 주로 **개별 사용자의 원격 접속**에 활용된다. 브라우저 지원이라는 앞부분의 특성으로부터 지점 간 site-to-site 연결이 주 용도라는 결론이 나오지는 않는다. 지점 간 네트워크 연결에는 IPsec VPN이 널리 쓰인다.

적절한 설명은 ㉠과 ㉡이므로 해당 조합은 ②이다.

NoteBase

**문 19. 무선랜 보안기법에 대한 설명으로 가장 적절하지 않은 것은?**

① IEEE 802.11i는 무선랜의 보안성을 강화한 표준이다.

② WAP-EAP는 무선랜 연결 세션들이 미리 설정한 공통의 암호화 키를 재사용한다.

③ WPA2는 AES 암호화 알고리즘을 사용하여 강력한 보안 기능을 제공한다.

④ WEP는 무선랜의 가장 기본적인 암호화 기술이지만 보안성이 높지 않아서 지금은 권장되지 않는다.

**정답 2번**

**간단한 해설**

②의 원문 표기는 WAP-EAP이나 문맥상 **WPA-EAP의 오기로 추정**된다. EAP 기반 Enterprise 방식은 사용자·세션별 키를 동적으로 관리하므로, 미리 설정한 공통 트래픽 암호화 키를 세션들이 그대로 재사용한다는 설명은 적절하지 않다.

**선지별 해설**

① O: **IEEE 802.11i**는 무선 LAN의 인증과 키 관리, 데이터 보호를 강화한 보안 표준이다. 기존 WEP의 취약점을 보완하는 보안 구조와 TKIP·CCMP 등의 메커니즘을 규정하였다.

② X: 원문은 **WAP-EAP**라고 표기하지만, 무선랜과 EAP라는 문맥상 **WPA-EAP를 의도한 오기로 추정**된다. 이를 정상적인 명칭으로 단정하거나 원문을 고친 것은 아니다. WPA의 Enterprise/EAP 방식은 인증 결과를 바탕으로 사용자·세션별 키를 동적으로 관리하므로, 모든 연결 세션이 미리 정한 하나의 공통 트래픽 암호화 키를 그대로 재사용한다는 설명은 맞지 않는다. 또한 사전 공유 자격정보와 실제 통신용 파생 키는 구별해야 하며, 그룹 트래픽용 키가 존재하지 않는다는 뜻도 아니다.

③ O: WPA2는 **AES 기반 CCMP**를 사용하는 강력한 무선랜 데이터 보호를 제공한다. 이는 WEP보다 개선된 암호화와 무결성 보호를 뜻하며, 취약한 비밀번호나 구현 결함까지 모두 없어진다는 의미는 아니다.

④ O: **WEP**는 초기 무선랜 보호 기술이지만 키 관리와 암호 설계상의 약점으로 보안성이 충분하지 않다. 따라서 안전한 무선랜 보호 수단으로 권장되지 않으며, 더 강화된 보안 방식을 사용해야 한다.

NoteBase

**문 20. 다음 로그로 유추할 수 있는 상황으로 가장 적절한 것은?**

Aug 8 01:11:38 localhost in.rlogind[4747]: connect from 192.168.1.10
Aug 8 01:11:38 localhost in.ftpd[4748]: connect from 192.168.1.10
Aug 8 01:11:38 localhost in.telnetd[4750]: connect from 192.168.1.10
Aug 8 01:11:38 localhost in.tftpd[4752]: connect from 192.168.1.10

① Ping of Death
② Port Scan
③ Land Attack
④ TCP Session Hijacking

**정답 2번**

**간단한 해설**

**동일한 출발지**가 같은 시각에 **여러 서비스로 접속**한 기록은 열린 포트와 서비스를 탐색하는 포트 스캔을 시사한다. 로그만으로 침입 성공을 단정할 수는 없다.

**핵심 풀이**

네 로그는 모두 **동일한 출발지 192.168.1.10**에서 **같은 초인 Aug 8 01:11:38**에 발생했다. 접속 대상은 in.rlogind, in.ftpd, in.telnetd, in.tftpd로 서로 다른 서비스이며, 각각 원격 로그인, FTP, Telnet, TFTP 관련 데몬이다.

한 출발지가 짧은 시간에 여러 서비스로 접속을 시도하는 패턴은 **열린 포트와 동작 중인 서비스를 탐색하는 포트 스캔**을 시사한다. 로그의 핵심은 특정 서비스 하나의 반복 사용이 아니라 여러 서비스에 걸친 동시다발적 접근이다. 다만 이 기록만으로 악의성이나 침입 성공까지 확정할 수는 없다.

Ping of Death는 비정상적으로 큰 패킷의 처리 문제를 악용하는 공격이며,

Land Attack은 출발지와 목적지 주소·포트가 같게 조작된 패킷을 이용한다.

TCP Session Hijacking은 이미 성립된 TCP 세션을 탈취하는 공격이다. 제시된 로그에는 이러한 패킷 특성이나 기존 세션 탈취를 보여 주는 정보가 없다.

따라서 로그로 유추할 수 있는 가장 적절한 상황은 Port Scan인 ②이다.

NoteBase