2022-경찰경채-시스템네트워크보안-해설-곽후근

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 상호 배제(Mutual Exclusion) : 프로세스가 점유한 자원은 처리가 끝날 때까지 강제로 해제 될 수 없는 상태
③ 환형 대기(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 체크
(3) 프로세스와 자원들이 원형을 이루며 각 프로세스는 자신에게 할당된 자원을 가지고 있으면서 상대방의 자원을 상호 요청하는 경우이다.
오답 체크
(1) 상호배제에 대한 설명이다.
(2) 비선점에 대한 설명이다.
(4) 점유와 대기에 대한 설명이다.

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 환경 설정 파일을 포함하는 디렉터리
㉡ 임시파일을 저장하는 임시 디렉터리
㉢ 시스템 로그가 저장되는 디렉터리
㉣ 사용자의 홈 디렉터리

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

정답 체크
(4) /var : 스풀 디렉토리나 파일, 로그 데이터 그리고 임시파일 같은 가변 데이터 파일들이 저장된다.
/tmp : 프로그램 실행 및 설치 시 생성되는 임시 파일을 담고 있다. 이 디렉토리에 파일을 저장하면 재부팅 시 임의로 삭제될 수 있다.

/etc : 시스템의 환경 설정 및 주요 설정을 담고 있다. passwd, hosts, xinetd, conf 등이 존재한다.
/home : 각 사용자의 작업 디렉토리를 담고 있다. 각 계정으로 로그인할 때 이 디렉토리 밑에 자신의 작업 디렉토리가 시작 디렉토리가 된다.

3. HTTP 상태코드에 대한 설명으로 가장 적절하지 않은 것은?

	코드	설명(상태)
①	403	요청이 허용되지 않는 자원 요구(Forbidden)
②	404	서버에 요구된 URL을 찾을 수 없음(Not Found)
③	500	서버 내부 오류가 발생 하여 더는 진행할 수 없음(Internal Server Error)
④	501	서버 과부하로 서비스할 수 없음(Service Unavailable)

정답 체크
(4) Not Implemented(요청을 수행할 수 있는 기능을 서버가 지원하지 않는다는 것을 의미)이다.
오답 체크
(1) 서버가 허용하지 않는 웹 페이지나 미디어를 사용자가 요청할 때 웹 서버가 반환하는 코드이다.
(2) 요청한 페이지를 찾을 수 없는 것을 의미한다.
(3) 요청을 처리하는 과정에서 서버가 예상하지 못한 상황에 발생하여 요청을 처리할 수 없음을 의미한다.

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

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

① 프로그램은 최소 권한으로 실행한다.
② 프로그래밍 할 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 체크
(3) 레이스 컨디션 공격에 대한 대응을 의미한다.
오답 체크
(1) 공격이 성공해도 권한이 최소이면 피해를 줄일 수 있다.
(2) strcpy 대신 strncpy를 사용한다.
(4) 문자 길이를 제한하면 버퍼 오버플로우 공격을 막을 수 있다.

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 체크
(1) 모든 계정의 로그인에 대한 검증을 수행하고, 시스템 자원 및 파일 등에 대한 접근 권한 검사를 수행한다. 로컬, 원격 모두에 해당하고, 이름과 SID를 매칭하며, SRM이 생성한 감사(audit) 로그를 기록한다.
오답 체크
(2) SAM의 기능에 해당한다.
(3) SRM의 기능에 해당한다.
(4) SAM의 기능에 해당한다.

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

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

① XXE(XML External Entities)
② CSRF(Cross-Site Request Forgery)
③ SQL Injection
④ XSS(Cross-Site Scripting)

정답 체크
(2) 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격이다. 즉, 일단 사용자가 웹 사이트에 로그인한 상태에서 CSRF 공격 코드가 삽입된 페이지를 열면, 이후에는 사용자의 행동과 관계없이 사용자의 웹 브라우저와 공격 대상 웹 사이트 간의 상호 작용이 이루어진다.
오답 체크
(1) XML 입력을 구문 분석하는 애플리케이션에 대한 공격 유형이다. 이 공격은 외부 엔터티에 대한 참조가 포함된 XML 입력이 약하게 구성된 XML 파서에 의해 처리될 때 발생한다. 이 공격은 기밀 데이터의 공개, 서비스 거부(DoS), 서버 측 요청 위조, 파서가 있는 시스템의 관점에서 포트 스캐닝 및 기타 시스템 영향으로 이어질 수 있다.
(3) 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.
(4) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크

립팅이라고 한다.

7. UNIX 명령어에 대한 설명으로 가장 적절하지 않은 것은?
① pwd : 로그인에 필요한 비밀 번호를 변경한다.
② cat : 파일 내용을 화면에 출력한다.
③ ps : 현재 시스템에서 실행 중인 프로세스 정보를 출력한다.
④ chmod : 파일에 대한 접근 권한을 변경한다.

정답 체크
(1) 현재 디렉토리를 알려주는 명령어이다.
오답 체크
(2) 파일의 모든 내용을 출력한다.
(3) 대부분의 유닉스 계통 운영 체제에서 현재 실행되고 있는 프로세스들을 표시한다(process status).
(4) 파일의 모드(권한)를 변경하는 명령어이다.

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 체크
(1) ㄱ : 운영체제의 기능인 자원 관리를 제공한다.
ㄴ : 파일 관리, 메모리 관리, 프로세스 스케줄링 등을 제공한다.
오답 체크
(2), (3), (4) ㄷ : 커널이 아닌 쉘에 대한 설명이다.

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

	First-Fit	Best-Fit	Worst-Fit
①	㉠	㉣	㉢
②	㉡	㉠	㉢

③ ㉠ ㉠ ㉡
④ ㉡ ㉣ ㉡

정답 체크
(4) ㄴ : 처음 검색된 50K에 할당한다.
ㄹ : 할당 후 공간이 제일 적게 남는 40K에 할당한다.
ㄴ : 할당 후 공간이 가장 많이 남는 50K에 할당한다.
Tip! 25K가 사용 중이라는 것이 함정이다.

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 체크
(4) 동일한 IP 주소에 하나의 MAC 주소가 확인된다.
오답 체크
(1) 중간자 공격 기법이다.
(2) 공격자가 자신의 MAC을 계속적으로 응답한다.
(3) 상대방의 MAC을 고정하면 된다.

11. OSI 참조모델의 각 계층에서 사용하는 프로토콜로 가장 적절하지 않은 것은?
① 데이터 링크 계층: Ethernet, Token Ring
② 네트워크 계층: IPSec, IGMP
③ 전송 계층: TCP, TLS
④ 응용 계층: PPP, HTTP

정답 체크
(4) PPP는 데이터 링크 계층 프로토콜이다.
오답 체크
(1) HDLC, 프레임 릴레이 등이 존재한다.
(2) ICMP, ARP, OSPF 등이 존재한다.
(3) RTP, RSVP 등이 존재한다. (TLS는 표현 계층으로 보는 견해도 존재. 2022-국회직)

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 감 사
㉢ 파일, 폴더, 프린터, 레지스트리 키 등과 같은 개체에 접근하는 사용자의 이벤트 감사
㉣ 사용자나 그룹을 생성, 변경, 삭제, 암호 설정 등의 이벤트 감사

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

정답 체크
(2) 시스템 이벤트 감사 : 시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.
계정 관리 감사 : 신규 사용자·그룹 추가, 기존 사용자·그룹 변경, 사용자 활성화·비활성화, 계정 패스워드 변경 등을 감사한다.
개체 액세스 감사 : 특정 파일이나 디렉터리, 레지스트리 키, 프린터 등과 같은 객체에 대해 접근을 시도하거나 속성 변경 등을 탐지한다.
프로세스 추적 감사 : 사용자 또는 응용 프로그램이 프로세스를 시작하거나 중지할 때 해당 이벤트가 발생한다.

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 접 속하게 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

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

정답 체크

(1) HTTP GET Flooding Attack : 서버에 TCP 3-웨이 핸드셰이킹 과정을 통해 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것이다.
DNS Spoofing Attack : 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.
Smurf Attack : 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.
SYN Flooding Attack : 존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서버의 서비스를 제공받지 못하게 하는 공격이다.

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 체크
(2) eth0 조건이 맞지 않아 그 다음으로 작은 서브넷이 eth1이 해당 패킷을 처리한다.
오답 체크
(1) 192.168.7.128부터 192.168.7.191인 패킷을 처리한다.
(3), (4) eth1에서 처리된다.

15. IPv6에 대한 설명으로 가장 적절하지 않은 것은?
① IPv6는 128 비트의 주소 필드를 갖고 있어서 IPv4 보다 더 많은 주소를 사용할 수 있다.
② 네트워크의 신뢰도가 높아져서 IPv4 헤더의 checksum 필드가 IPv6 헤더에서는 삭제되었다.
③ IPv6에서 기본 헤더의 길이는 40 바이트로 고정된다.
④ IPv6에서 라우터는 크기가 큰 데이터그램을 여러 개의 작은 데이터그램으로 단편화할 수 있다.

정답 체크
(4) 보내는 곳에서 미리 단편화가 되어 중간 라우터에서 단편화가 발생하지 않는다.
오답 체크
(1) IPv4는 32비트이고, IPv6는 128비트이다.
(2) 체크섬 필드가 없다.
(3) IPv4는 20바이트 가변이다.

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 체크

(3) netstat의 실행 결과이다.

프로토콜	로컬 주소	외부 주소	상태
TCP	111.111.111.111:49217	222.222.222.221:ms-sql-s	ESTABLISHED
		(중략)	
TCP	111.111.111.111:49216	222.222.222.222:ftp	TIME_WAIT

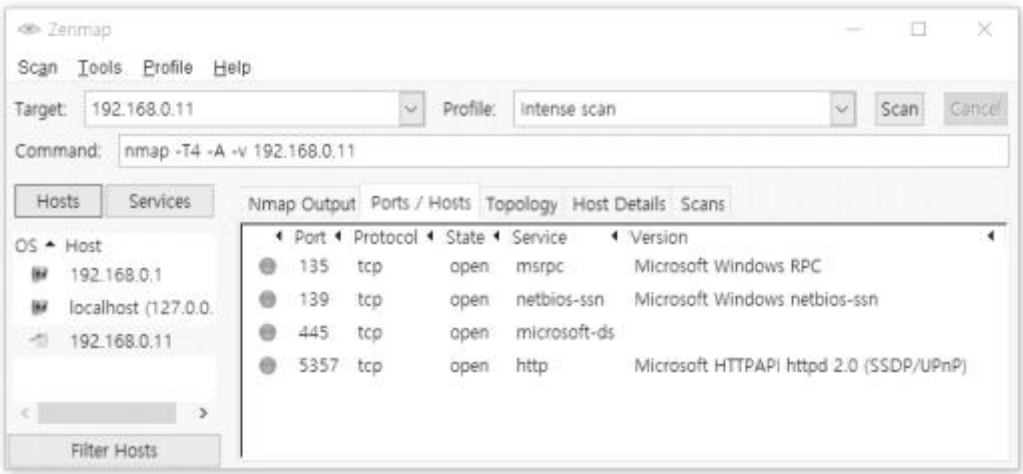
오답 체크

(1) nslookup의 실행 결과이다.

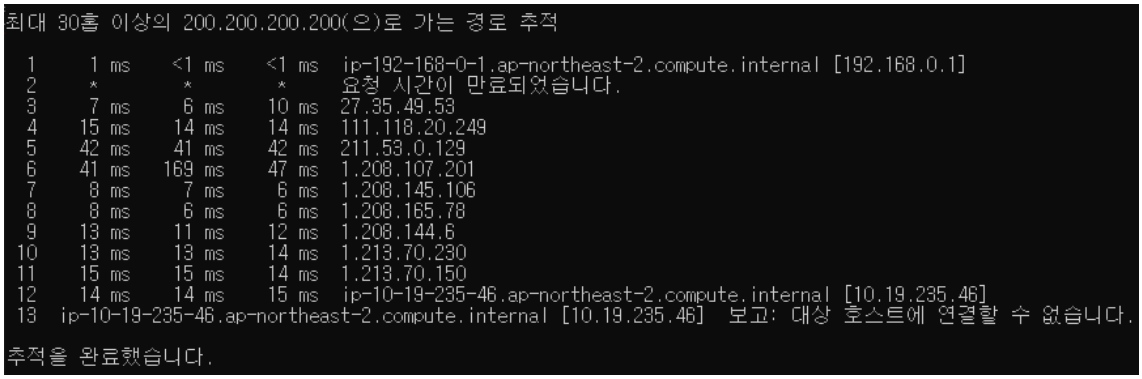
```
서버:    ip-10-80-0-53.ap-northeast-2.compute.internal
Address:  10.80.0.53

권한 없는 응답:
이름:    naver.com
Addresses:  125.209.222.142
          223.130.195.200
          223.130.195.95
          125.209.222.141
```

(2) nmap의 실행 결과이다.



(4) tracert의 실행 결과이다.



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 대응 조치를 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 체크

(3) 오용탐지(misuse detection)에 대한 설명이다.

오답 체크

(1) 인트라넷을 보호한다.

(2) 능동적 보안 장비이다.

(4) 크래커를 유인하는 함정을 꿀단지(곰을 유인)에 비유한 것에서 명칭이 유래한다. 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 한다. 침입자를 오래 머물게 하여 추적이 가능하므로 능동적으로 방어할 수 있고, 침입자의 공격을 차단할 수 있다. 직접적인 공격을 수행하지는 않는다.

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 체크

(2) ㄱ : 공중망과 사설망의 장점을 결합한다.

ㄴ : L2TP, PPTP, L2F 등을 사용한다.

오답 체크
(1), (3), (4) ㄷ : 3계층에서 동작하므로 7계층의 수정이 필요하지 않다.
ㄹ : client-to-site 연결에 주로 활용한다.

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 체크
(2) 암호화키를 가변한다.
오답 체크
(1) WPA2를 사용한다.
(3) AES와 CCMP를 사용한다.
(4) 전사공격이 가능하다.

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 체크
(2) 여러개의 포트로 접속하는 것을 알 수 있다.
오답 체크
(1) ping이 여러 개 보여야한다.
(3) 출발지 IP와 목적지 IP가 같아야 한다.
(4) 연결을 끊고 재설정하는 과정이 있어야 한다.