【시스템네트워크보안】

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

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

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

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 내부오류가 발생하여 더는 진행할 수 없음(Internal Server Error)
④	501	서버 과부하로 서비스할 수 없음(Service Unavailable)

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.

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.

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)

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.

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 ㉠㉡㉢

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	㉡	㉣	㉡

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.

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

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

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

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

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

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

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.

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

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.

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 ㉠㉡㉣

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.

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