1. 다음에 설명하는 보안 솔루션의 유형으로 가장 적절한 것은?

· 해커에게 쉽게 노출된다. · 시스템의 모든 구성 요소를 갖추고 있다. · 통과하는 모든 패킷을 감시한다. · 취약점을 갖고 있는 시스템이다.

① 침입탐지시스템 ② 허니팟
③ 방화벽 ④ 침입차단시스템

2. IPSec 터널 모드에 대한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

가. IP 헤더를 보호하지 않는다. 나. IP 헤더를 포함한 패킷 전체를 보호한다. 다. 두 개의 라우터 간, 호스트와 라우터 간, 또는 라우터와 호스트 간에 사용한다. 라. 전송층에서 네트워크층으로 전달되는 모든 패킷을 보호한다.

① 가, 다 ② 가, 라 ③ 나, 다 ④ 나, 라

3. 버퍼 오버플로(buffer overflow) 공격 대응책에 대한 설명으로 가장 적절한 것은?

① ASLR: 스택에서 실행 권한을 제거함으로써 스택에 로드된 공격자의 공격코드를 실행할 수 없도록 한다.
② Non-Executable Stack: 메모리 공격을 방어하기 위해 스택, 힙, 라이브러리 등의 데이터 영역 주소를 난수화 한다.
③ Stack Guard: 스택에 있는 복귀 주소를 실행 가능한 임의의 주소(libc 영역의 주소)로 돌려 원하는 함수를 수행한다.
④ Stack Shield: 함수를 호출할 때는 복귀 주소를 Global RET Stack이라는 특수 스택에 저장하고 함수를 종료할 때는 Global RET Stack에 저장된 복귀 주소 값과 스택의 복귀 주소 값을 비교하여 일치하지 않으면 프로그램을 종료시킨다.

4. tcpdump에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① Lawrence Berkley Nation Lab의 Network Research Group에서 만들었다.
② 리눅스에서 가장 기본이 되는 spoofing 도구이다.
③ 네트워크 상태를 확인하기 위해 패킷을 캡처하여 분석할 때 사용한다.
④ libpcap 라이브러리를 사용하여 패킷을 캡처한다.

5. 다음은 웹 취약점 보완을 위한 특수 문자 필터링에 대한 특수 문자이다. XSS 취약점 공격에 사용되지 않는 특수 문자를 모두 고른 것으로 가장 적절한 것은?

가. <	나. =	다. ;	라. &	마. ?	바. *

① 가, 나, 다 ② 가, 라, 마
③ 나, 다, 바 ④ 나, 마, 바

6. 포맷 스트링에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① %d: 정수형 10진수 상수
② %s: 문자열
③ %f: 실수형 상수
④ %x: 8진수 양의 정수

7. 침입탐지시스템(IDS)의 기능으로 가장 적절하지 <u>않은</u> 것은?

① 정보 수집 ② 정보 가공 및 축약
③ 침입 방지 및 분석 ④ 보고 및 조치

8. 침입탐지시스템(IDS)의 오용 탐지 기법에 대한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

가. 행위 또는 통계 기반 기법이다. 나. 미리 정의한 rule에 매칭한다. 다. false positive가 낮다. 라. 알려지지 않은 공격에 대응할 수 있다. 마. 대량의 자료를 분석하는 데 부적합하다. 바. false negative가 낮다.

① 가, 다, 라 ② 가, 라, 바
③ 나, 다, 라 ④ 나, 다, 마

9. 일반적인 유닉스 또는 리눅스 주요 로그에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① btmp: 시스템에 현재 로그인한 사용자에 대한 상태 정보를 기록한다.
② syslog: 사용자 인증과 관련된 로그 및 커널, 데몬에서 생성된 모든 로그를 포함하여 기록한다.
③ history: 사용자별로 수행한 명령을 기록한다.
④ secure: telnet, ftp 등 인증과정을 거치는 모든 로그를 기록한다.

10. 다음은 CSRF 공격 단계를 나열한 것이다. 순서가 가장 적절한 것은?

가. 사용자가 CSRF 스크립트가 포함된 게시글을 열람한다. 나. 공격자가 CSRF 취약점이 존재하는 임의의 웹 서버에 CSRF 스크립트가 포함된 게시글을 작성한다. 다. 사용자의 정상적인 요청에 의한 것이 아닌, 공격자가 의도한 동작을 수행한다. 라. 서버에서 CSRF 스크립트가 실행된다.

① 가-나-다-라 ② 가-나-라-다
③ 나-가-다-라 ④ 나-가-라-다

11. 응용계층 프로토콜과 잘 알려진 포트번호와의 연결이 가장 적절한 것은?

① HTTPS - 143 ② POP3 - 25
③ TFTP - 21 ④ DNS - 53

12. AAA 중 가장 일반적인 방법인 ID, 패스워드를 입력하여 자신의 신원(identity)을 시스템에 증명하는 과정으로 가장 적절한 것은?

① Audit Trail ② Authorization
③ Accounting ④ Authentication

13. 악성코드에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 런처: 자신 안에 존재하는 데이터로부터 새로운 파일을 생성하여 공격을 수행한다.
② 랜섬웨어: 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성코드를 말한다.
③ 익스플로잇: 운영체제나 특정 프로그램의 취약점을 이용하여 공격한다.
④ 봇: DDoS 공격 시 지정된 공격을 수행하도록 하는 악성코드이다.

14. 어떤 기관의 호스트에 할당된 주소 200.107.16.17/22에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 해당 네트워크 내의 주소 개수는 1024개이다.
② 200.107.16.0/22은 네트워크 주소로서 IP 데이터그램을 목적지로 라우팅하는데 사용된다.
③ 200.107.18.255/22는 마지막 주소로서 해당 네트워크 내 브로드캐스트 주소이다.
④ CIDR을 지원하는 주소 지정 방식이다.

15. TCP 세그먼트(segment)의 순서 번호(sequence number)에 대한 설명으로 가장 적절한 것은?

① 클라이언트-서버 간 연결 설정 후에 임의의 초기 순서 번호가 할당된다.
② 순서 번호는 해당 세그먼트에 포함된 첫 번째 데이터 바이트의 번호로 정의된다.
③ 순서 번호는 0에서 2^{16} - 1의 범위에 있다.
④ 순서 번호의 구조적 문제로 SYN flooding 공격에 영향을 받기 쉽다.

16. SSH-2(Secure Shell ver. 2) 프로토콜에 대한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

가. 클라이언트와 서버 간 보안성 있는 연결을 제공하는 범용 프로토콜이다.
나. SSH는 TCP 또는 UDP 위에 안전한 채널 형성을 위한 별도의 전송 프로토콜을 이용한다.
다. 클라이언트에 대한 인증만을 제공하며, 클라이언트와 서버 간 교환되는 메시지의 데이터 무결성을 보장한다.
라. 포트 포워딩(port forwarding)은 일종의 터널링 기능으로 FTP 응용 등에 보안 연결을 제공할 수 있다.

① 가, 나 ② 가, 라 ③ 나, 다 ④ 다, 라

17. Smurf 공격은 공격자로부터의 패킷을 증폭하는 중간의 경유 네트워크를 필요로 한다. 자신의 네트워크가 Smurf 공격에 이용당하지 않는 방법으로 가장 적절한 것은?

① ICMP echo request 패킷을 필터링한다.
② ICMP echo reply 패킷을 전송하지 않는다.
③ ping 요청에 응답하지 않는다.
④ 외부로부터 수신되는 브로드캐스트 패킷을 필터링한다.

18. IPv6에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① IPv6 헤더의 '페이로드 길이' 필드는 기본 헤더를 뺀 IPv6 데이터그램의 길이를 포함한다.
② IPv6 데이터그램의 단편화(fragmentation)는 발신지 호스트와 라우터에서 수행할 수 있다.
③ IPv6 헤더의 '홉 제한(hop limit)' 필드는 IPv4의 TTL에 대응된다.
④ 같은 자원의 사용, 같은 종류의 보안 등 동일한 특성을 공유하는 일련의 패킷들에 대한 처리를 지원한다.

19. 다음 <보기 1>의 보안을 위한 프로토콜과 <보기 2>의 설명을 순서대로 나열한 것으로 가장 적절한 것은?

<보기 1>

가. IPSec 나. VPN 다. PGP 라. IEEE 802.1X

<보기 2>

㉠ 포트 기반으로 네트워크에의 접근을 통제하기 위한 프로토콜이며 LAN에서 주로 사용한다.
㉡ IP 데이터그램 단위의 암호화/인증을 제공하며 응용의 변경 없이 이용할 수 있다.
㉢ 인터넷을 이용한 가상의 사설망으로 보안을 제공하기 위한 암호와 특별한 프로토콜을 사용하는 컴퓨터들의 집합이다.
㉣ 전자우편에 프라이버시(privacy), 무결성, 인증을 제공하기 위한 프로토콜로서 안전한 전자우편 메시지 생성에 사용할 수 있다.

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

20. 패킷의 발신지 IP 주소를 공격대상의 IP 주소로 변경하여 전송하는 공격들을 모두 고른 것으로 가장 적절한 것은?

가. LAND 공격	나. Smurf 공격
다. DNS spoofing 공격	라. TCP 세션 하이재킹

① 가, 나 ② 가, 나, 다
③ 가, 나, 라 ④ 가, 다, 라

21. 버퍼 오버플로(buffer overflow)에 취약한 함수들을 모두 고른 것으로 가장 적절한 것은?

가. fscanf()　나. gets()　다. strncat()　라. snprintf()

① 가, 나　② 가, 라
③ 나, 다　④ 다, 라

22. 쿠키(cookies)에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?
① 웹 서버는 클라이언트에 대한 정보를 기억할 목적으로 클라이언트로 전송하는 HTTP 응답 메시지의 'Set-Cookie' 헤더에 쿠키를 포함할 수 있다.
② 클라이언트가 웹 서버로부터 쿠키를 받으면, 브라우저는 도메인 서버 이름으로 정렬되는 쿠키 디렉터리에 쿠키를 저장한다.
③ 만료 날짜가 있어 일정 기간이 지나면 자동으로 삭제된다.
④ 쿠키는 XSS, CSRF, HTTP GET flooding 등의 공격에 악용될 수 있다.

23. 다음 용어에 대한 설명 중 가장 적절하지 <u>않은</u> 것은?
① PCB(Process Control Block): 특정 프로세스에 대한 정보를 보관하는 일종의 테이블로서 부모와 자식 프로세스는 PCB를 공유한다.
② 샌드박스(sandbox): 기본적으로 시스템과 다른 애플리케이션에 접근하는 것을 통제하기 위해 사용한다.
③ SetGID: SetGID가 설정된 파일을 실행하면 해당 파일이 실행되는 동안 파일을 소유한 그룹의 권한으로 실행된다.
④ HKEY_CURRENT_USER: 윈도우 운영체제의 레지스트리의 하나로서 윈도우가 설치된 컴퓨터 환경 설정에 대한 정보를 저장한다.

24. 다음 취약점을 갖는 응용 프로토콜과 그 취약점을 이용한 공격을 연결한 것으로 가장 적절한 것은?

제어 명령 전달을 위한 연결과 데이터 전달을 위한 연결이 분리되어 있는 응용 프로토콜이며 파일 전송을 요청한 클라이언트와 실제 파일을 수신하는 클라이언트가 다를 수 있는 취약점이 존재한다.

① HTTP - Anonymous 공격
② FTP - Bounce 공격
③ FTP - Redirect 공격
④ TFTP - Hijacking 공격

25. 웹 서버의 보안을 강화하기 위한 조치로 가장 적절하지 <u>않은</u> 것은?
① Acunetix와 같은 스캐너를 이용하여 웹 서버의 보안취약점을 점검하고 대응한다.
② 웹 서버 관리자는 최소 권한을 갖도록 설정한다.
③ 웹 서버는 사용자가 입력하는 입력 값에 대한 유효성을 검증할 필요가 있다.
④ VPN에 웹 서버를 배치하여 외부의 공격을 최대한 차단한다.

26. 다음에 설명하는 사회공학적기법으로 가장 적절한 것은?

• 사용자가 웹브라우저에 정확한 웹페이지 주소를 입력하였으나 가짜 웹페이지로 유도되어 진짜 사이트로 오인한다. • 사용자가 특별한 의심없이 진짜 사이트로 생각하고 입력하는 모든 개인정보 등은 쉽게 유출될 수 있다.

① 보이스 피싱　② 메신저 피싱
③ 스미싱　④ 파밍

27. SSL에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?
① SSL은 IPSec과는 달리 HTTP에만 적용 가능하여 HTTPS 프로토콜의 구현에 사용된다.
② SSL은 Handshake, Change Cipher Spec, Alert, Record 프로토콜 등으로 구성된다.
③ SSL Handshake 프로토콜은 RSA 공개키 암호 알고리즘을 사용한다.
④ SSL Record 프로토콜은 TCP 위에서 동작하며 응용 데이터를 암호화한다.

28. 리눅스 보안에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?
① nmap은 로컬 호스트나 원격의 서버가 사용 중인 포트와 운영체제를 스캔할 수 있다.
② 시스템 관리자는 날짜가 오래된 로그 파일을 백업 후 삭제할 필요가 있다.
③ nmap은 네트워크 주소를 지정하여 특정 네트워크 전체를 스캔할 수 없다.
④ 일반 사용자 계정에서의 로그 파일에 대한 접근은 보안상 제한하는 것이 바람직하다.

29. SSO(Single Sign On)에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?
① 사용자가 한 번의 인증으로 인터넷 및 인트라넷 간 응용 프로그램을 별도의 인증 없이 이용할 수 있다.
② 사용자는 먼저 인증 서버에 접속하여 인증을 받은 후 응용 서버에 서비스를 요청한다.
③ 인증 서버에서 응용 서버로 사용자 인증정보를 전달할 때 보안 취약점이 발생할 수 있다.
④ 중앙집중관리를 통한 효율적인 관리가 가능하다.

30. 다음 용어에 대한 설명 중 가장 적절하지 <u>않은</u> 것은?
① TCB(Trusted Computing Base): 컴퓨터 시스템의 신뢰성, 안전성, 효율성을 높이기 위해 시스템을 종합적으로 분석/평가하는 솔루션이다.
② DLP(Data Loss Prevention): 조직 내의 중요한 자료가 외부로 빠져나가는 것을 탐지하여 차단하는 보안 솔루션이다.
③ NAC(Network Access Control): 단말기가 조직 내부 네트워크에 접속을 시도할 때 사용자 인증을 수행하고 백신 설치와 관련한 무결성을 점검한다.
④ Salt: 패스워드의 해시에 사용하는 난수의 일종으로 운영체제별로 다양한 알고리즘이 존재한다.

31. 윈도우 운영체제에서의 네트워크 관리 명령어에 대한 설명으로 가장 적절하지 않은 것은?

① ipconfig /flushdns: dns 캐시 정보를 삭제한다.
② netstat -r: 로컬 호스트의 라우팅 테이블을 보여준다.
③ ping -f 사이트 주소: 'Ctrl+c'로 중지할 때까지 사이트 주소에 ping을 실행한다.
④ tracert 사이트 주소: 최종 수신지에 도달하기까지 중간에 경유하는 라우터 경로 및 응답 시간을 보여준다.

32. 다음 윈도우XP 운영체제 부팅에 대한 설명으로 가장 적절한 것은?

- 기본 파일 시스템 정보가 들어있다.
- 저장 매체의 첫 번째 섹터(LBA)에 위치하는 512 바이트 영역이다.
- 부팅 가능한 파티션이 없으면 미리 정의된 오류 메시지를 출력한다.
- 운영체제를 부팅할 때 저장 매체의 첫 번째 섹터를 호출하면 해당 부트 코드를 수행한다.
- 부트 코드의 주 역할은 파티션 테이블에서 부팅 가능한 파티션을 찾아 해당 파티션의 부트 섹터를 호출한다.

① CMOS 로딩
② MBR 로딩
③ POST 실행
④ WBM(Window Boot Manager) 실행

33. 윈도우 운영체제에서 백도어가 이용하는 csrss.exe 프로세스에 대한 설명으로 가장 적절한 것은?

① 작업표시줄, 바탕화면 등 사용자 셸을 지원하는 프로세스이다.
② 시스템 백업이나 업데이트 등을 작업하는 스케줄러 프로세스이다.
③ winlogin 서비스에 필요한 인증 프로세스이다.
④ 윈도우 콘솔을 관장하고 스레드를 생성 및 삭제하며 32비트 가상 MS-DOS 모드를 지원하는 프로세스이다.

34. 어셈블리 명령어에 대한 설명으로 가장 적절하지 않은 것은?

① CMP: 산술 연산 명령이며 데이터의 두 값을 비교할 때 사용한다.
② JMP: 제어 전송 명령이고 점프 명령(분기)이며 프로그램 실행 주소 또는 레이블로 이동할 때 사용한다.
③ LEA: 데이터 전송 명령이며 스택에서 데이터를 삭제할 때 사용한다.
④ STC: 프로세서 제어 명령이고 피연산자 없이 사용하며 EFLAGS 레지스터의 CF 값을 설정할 때 사용한다.

35. 랜섬웨어에 대한 설명으로 가장 적절한 것은?

① CryptoLocker: 감염되면 파일 확장자가 .locker로 변경되며 바탕화면과 텍스트 파일로 복구 관련 메시지를 출력한다.
② CryptXXX: 정상 rundll32.exe를 svchost.exe 이름으로 복사한다.
③ Locky: 윈도우 운영체제의 SMB(Server Message Block)를 이용하여 악성코드를 감염시킨다.
④ WannaCry: 실행 파일이 아닌 동적 링크 라이브러리(DLL) 형태로 유포한다.

36. 보안 커널의 기능 중 참조 모니터(reference monitor)에 대한 설명으로 가장 적절하지 않은 것은?

① 프로세스와 파일의 정보 흐름을 감시하는 보안 모듈이다.
② 객체에 대한 접근통제 기능을 수행한다.
③ 액세스 권한을 변경하는 등 보안 관리기능을 수행할 때 신뢰할 수 있는 경로를 제공해야 한다.
④ 감사, 식별, 인증 및 보안 매개변수 설정 등과 같은 다른 보안 메커니즘과 데이터를 교환하면서 상호작용을 한다.

37. 블루투스 보안 취약점에 대한 설명으로 가장 적절한 것은?

① blueprinting: 블루투스 장치가 서로 한 번 연결되면 그 이후에는 별다른 인증절차 없이 자동으로 서로 연결되는 인증 취약점을 악용한 것으로 10미터 이내의 거리에서 블루투스 기기에 전화 걸기, 불특정 번호로 SMS 보내기, 주소록 읽기 및 쓰기 등을 실행할 수 있다.
② bluejacking: 서비스 발견 프로토콜(SDP:Service Discovery Protocol)을 통해 블루투스 장치를 검색하고 모델을 확인한다.
③ bluebugging: 사용자들은 블루투스를 통해서 스팸 메시지들을 보낸다. 메시지들은 피해가 없는 광고와 스팸메시지 등이다.
④ bluesnarfing: 블루투스 장치끼리 인증없이 간편하게 정보를 교환하도록 개발된 OPP 기능을 사용하여 블루투스 장치에 있는 주소록 등의 내용을 요청하여 열람하거나 취약한 장치의 파일에 접근할 수 있다.

38. 윈도우 운영체제에서 ARP spoofing 공격을 막기 위하여 MAC 주소를 고정하는 네트워크 명령어로 가장 적절한 것은?

- IPv4 주소: 203.237.128.40
- MAC 주소: AA-BB-CC-DD-A0-B0

① route ADD 203.237.128.40 AA-BB-CC-DD-A0-B0
② route CHANGE 203.237.128.40 AA-BB-CC-DD-A0-B0
③ arp -d 203.237.128.40 AA-BB-CC-DD-A0-B0
④ arp -s 203.237.128.40 AA-BB-CC-DD-A0-B0

39. HTTP Response의 상태 코드 '301'에 대한 설명으로 가장 적절한 것은?

① bad request
② moved permanently
③ not modified
④ not implemented

40. 다음에 설명하는 구글검색엔진의 검색 파라미터를 제시한 것들로 가장 적절한 것은?

- 특정 도메인으로 지정한 사이트에서 검색하려는 문자열이 포함된 사이트를 찾는다.
- 페이지 제목에 검색하는 문자가 들어있는 사이트를 찾는다.
- 특정 파일 유형에 한해 검색하는 문자가 들어있는 사이트를 찾는다.

① cache, inurl, link
② cache, filetype, intitle
③ filetype, link, site
④ filetype, intitle, site