1. 다음에서 설명하는 윈도우 로그로 가장 적절한 것은?

> 도메인 계정 사용으로 생성되고, 이 감사의 실패 이벤트 추적에서는 패스워드 크래킹 시도 등을 확인할 수 있고, 성공 이벤트 추적에서는 사후 문제를 확인할 수 있다.

① 개체 액세스 감사
② 계정 로그온 이벤트 감사
③ 로그온 이벤트 감사
④ 계정 관리 감사

2. 다음에서 설명하는 용어로 가장 적절한 것은?

> 전자상거래 당사자들의 신뢰성과 안전성을 위하여 사용자 및 판매자의 신원 인증, 거래 정보의 비밀성, 지불 데이터의 부인 방지 등의 보안 기능과 이질적인 환경에서의 상호운용성을 제공한다.

① SET
② PGP
③ OTP
④ SSO

3. 리눅스 디렉터리의 주요 기능에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?

① /dev : 장치 파일이 담긴 디렉터리이다.
② /opt : 추가 패키지가 설치되는 디렉터리이다.
③ /sys : 시스템의 환경설정 및 주요 설정 파일을 담고 있다.
④ /var : 시스템 운영 중에 발생하는 데이터나 로그 등 내용이 자주 바뀌는 파일이 저장된다.

4. SSH에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① Telnet이나 보안을 제공하지 않는 다른 원격 로그인 방식을 대체하기 위해 개발되었다.
② 원격 로그인과 X-터미널에 채택되어 사용되었으며 현재도 가장 널리 사용되는 응용 기술이다.
③ Alert 프로토콜과 Record 프로토콜을 정의하여 암호화를 한다.
④ 안전하지 않은 TCP 연결을 포트 포워딩을 사용하여 안전한 연결로 변환시킬 수 있다.

5. 다음에서 설명하는 공격기법으로 가장 적절한 것은?

> 통신을 연결하는 두 사람 사이에 침입하여, 두 사람이 상대방에게 연결됐다고 생각하도록 조작하고, 공격자는 한쪽에서 전달된 정보를 도청하거나 조작한 후 다른 쪽으로 전달하는 공격기법이다.

① 부채널 공격
② 살라미 공격
③ 무차별 공격
④ 중간자 공격

6. 리눅스에서 exam이라는 파일에 SetUID를 설정하는 명령으로 가장 적절한 것은?

① chmod u+t exam
② chmod g+s exam
③ chmod 2755 exam
④ chmod 4755 exam

7. VPN에서 사용하는 터널링 프로토콜 중에서 가장 적절하지 <u>않은</u> 것은?

① L2F
② PPTP
③ L2TP
④ P2P

8. 다음에서 설명하는 공격기법으로 가장 적절한 것은?

> TCP 3중 연결(3-way handshaking)의 취약점과 반사 서버(라우터 등)를 이용한 공격으로, 공격자는 출발지 IP를 공격 대상의 IP로 위조하여 SYN 패킷을 다수의 반사 서버로 전송하여 응답하는 SYN-ACK 패킷을 공격 대상이 받도록 한다.

① LAND
② Port Scan
③ DRDoS
④ ARP Spoofing

9. IDS의 비정상(Anomaly) 행위 탐지에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 신경망, 통계적 방법, 특징 추출 등의 기술을 사용한다.
② 미리 학습된 사용자 패턴과 다른 경우에 침입으로 판단할 수 있다.
③ 오용(Misuse)탐지 방식보다 False Positive가 상대적으로 낮다.
④ Zero Day Attack에 대응이 가능한 방법이다.

10. 다음 빈칸 (㉠), (㉡)에 들어갈 용어로 가장 적절한 것은?

> 80x86 시스템의 메모리 구성 요소 중 (㉠)은/는 초기화되지 않은 정적/전역 변수를 저장하며, 프로그램을 실행할 때 0이나 NULL 포인터로 초기화되는 영역이다. 그리고 (㉡)는 실행되는 머신 코드가 있는 영역으로 EIP가 다음에 실행하는 명령을 가리킨다.

㉠	㉡
① 스택	텍스트 세그먼트
② 힙	데이터 세그먼트
③ BSS 세그먼트	텍스트 세그먼트
④ 텍스트 세그먼트	데이터 세그먼트

11. 다음에서 설명하는 SNS 보안 위협으로 가장 적절한 것은?

> 이것은 사용자를 속이는 사회공학적 공격기법이다. 공격자는 와이파이 무선 네트워크에서 Rogue AP를 이용해 사용자 정보를 가로채고, 그 정보로 SNS에 가입 후 공격 대상의 지인이나 특정 유명인으로 가장하여 악의적인 목적을 가지고 활동한다.

① 피싱 ② 사이버 폭력
③ 악성 소프트웨어 ④ 이블 트윈 어택

12. 다음에서 설명하는 버퍼 오버플로 공격 대응 기법으로 가장 적절한 것은?

> ○ 함수를 호출할 때는 ret를 Global RET Stack이라는 특수 스택에 저장한다.
> ○ 함수를 종료할 때는 Global RET Stack에 저장된 ret 값과 스택의 ret 값을 비교하여 일치하지 않으면 프로그램을 종료시킨다.

① 스택 가드 ② 스택 실드
③ ASLR ④ Non-Executable Stack

13. 수신한 패킷의 IPv4 헤더의 HLEN 필드에 이진수 1111_2가 저장되어 있다면 이 패킷의 헤더의 길이는 몇 byte가 가장 적절한가?

① 20byte ② 40byte ③ 50byte ④ 60byte

14. 리눅스 파일시스템에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?

① ext 파일시스템은 Extended File System의 약자로 MFS의 기능을 확장했다.
② ext3 파일시스템은 저널링 기능을 도입하여 데이터의 복구 기능을 강화했다.
③ swap은 스왑 영역을 관리하기 위한 스왑 파일시스템이다.
④ proc는 메모리에 임시 파일을 저장하기 위한 파일시스템이며, 시스템이 재시작할 때마다 기존 내용이 없어진다.

15. OTP(One Time Password) 발생기의 인증방식-인증값의 연결이 가장 적절하지 <u>않은</u> 것은?

① S/KEY 방식 - 해시값
② 이벤트 동기화 방식 - 이벤트
③ 시간 동기화 방식 - 시간
④ 도전-응답(Challenge-response) 방식 - 난수

16. 다음에서 설명하는 접근 통제 구현 방법으로 가장 적절한 것은?

> 기술적 통제라고도 불리며, 보호해야 할 정보에 접근하는 것을 제한하기 위해 사용하는 하드웨어와 소프트웨어 도구를 말한다. 특정 애플리케이션에 접근할 수 있는 사용자의 IP 주소 외에 다른 주소는 접근을 차단하는 방법이 이에 해당한다.

① 관리적 접근 통제
② 논리적 접근 통제
③ 물리적 접근 통제
④ 상대적 접근 통제

17. 안티 리버싱 기법으로 가장 적절하지 <u>않은</u> 것은?

① 언패킹
② 안티 디버깅
③ 타이밍 체크
④ 쓰레기 코드 넣기와 코드 치환

18. 다음 설명에 해당하는 공격으로 가장 적절한 것은?

○ 제어 채널과 데이터 채널을 다르게 사용하고, 데이터 채널을 생성할 때 목적지를 확인하지 않는 FTP의 취약점을 이용하여 공격한다. ○ FTP의 능동 모드에서 클라이언트의 IP 주소, 포트 번호가 아닌 임의의 IP주소를 지정할 수 있는 기능을 이용한 공격이다.

① Bounce Attack
② Brute-Force Attack
③ Anonymous FTP Attack
④ Passive Attack

19. 윈도우에서 실행되는 각 서비스에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?

① csrss.exe : 윈도우 콘솔을 관장하고, 스레드를 생성·삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스이다.
② smss.exe : 사용자 세션을 시작하는 기능을 담당하는 프로세스로, winlogon, win32를 구동시킨다.
③ svchost.exe : DLL이 실행하는 프로세스의 기본 프로세스로, 한 시스템에서 svchost 프로세스를 여러 개 볼 수 있다.
④ winmgmt.exe : 윈도우 작업 관리자 자신의 프로세스이다.

20. 인터넷 계층별 보안 서비스를 제공하는 프로토콜의 연결이 가장 적절하지 <u>않은</u> 것은?

① 응용 계층 - MPLS
② 응용 계층 - HTTPS
③ 네트워크 계층 - IPSec
④ 데이터링크 계층 - PPTP

21. 다음에서 침입차단 시스템 구현 유형과 명칭의 연결이 가장 적절한 것은?

가. 접근통제, 로그 관리 등의 기능을 지원할 수 있으나 처리 속도가 상대적으로 느리다. 나. OSI 전 계층에서 패킷의 콘텐츠를 해석하여 침입차단을 수행한다. 다. 3계층과 4계층에서 동작하며 IP 프로토콜과 포트를 차단 및 허용할 수 있다.

	가	나	다
①	애플리케이션 게이트웨이	패킷 필터링	상태기반 패킷 검사
②	애플리케이션 게이트웨이	상태기반 패킷 검사	패킷 필터링
③	회선 게이트웨이	데이터그램 필터링	상태기반 패킷 검사
④	회선 게이트웨이	상태기반 패킷 검사	데이터그램 필터링

22. IPv4 헤더 필드 중에서 라우터를 통과하면서 값이 변경되는 필드로 가장 적절한 것은?

① Protocol ② TTL
③ Source Address ④ Version

23. 다음 중 망 분리에 관한 설명에 해당하는 레벨의 연결이 가장 적절한 것은?

가. 망 분리를 통해 업무 프로세스를 재정립하여 인터넷망에 있어야 하는 시스템과 업무망에 있어야 하는 시스템을 분리한다. 나. 인터넷 사용 PC와 업무용 PC를 분리하여 운영한다. 다. 인터넷 접속망과 업무용 망이 분리되어 있다.

	가	나	다
①	단말 레벨	업무 레벨	네트워크 레벨
②	네트워크 레벨	단말 레벨	업무 레벨
③	업무 레벨	단말 레벨	네트워크 레벨
④	업무 레벨	네트워크 레벨	단말 레벨

24. 다음에서 설명하는 용어로 가장 적절한 것은?

○ 신뢰 컴퓨팅을 위한 하드웨어/소프트웨어 방법에서 핵심이 되는 하드웨어 모듈이다. ○ 이것은 하드웨어 칩으로 구현하는 것이 일반적이나 소프트웨어로 구현하기도 하며, 암호화 키의 생성과 저장, 패스워드의 저장, 디지털 인증서 관련 신뢰 연산 등이 제공된다.

① TCB ② TPM
③ 보안 커널 ④ 참조 모니터

25. 다음에서 설명하는 무결성 점검 도구로 가장 적절한 것은?

○ 유닉스/리눅스 환경에서 파일시스템 무결성을 점검하는 대표적인 도구로 오픈 소스 버전과 상용 버전이 있다. ○ MD5, SHA 등의 다양한 해시 함수를 지원하고, 파일 및 디렉터리의 해시값을 생성하여 데이터베이스를 만들어 이를 통해 공격자들에 의한 파일들의 변조 여부를 판별한다.

① Nmap ② Nessus
③ Tripwire ④ SATAN

26. OSPF 라우팅 프로토콜에 사용되는 알고리즘으로 가장 적절한 것은?

① Dijkstra 알고리즘
② Greedy 알고리즘
③ Distance Vector 알고리즘
④ Euclidean 알고리즘

27. IPSec에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 보안 서비스가 제공되는 방식에는 전송 모드와 터널 모드가 존재한다.
② AH는 암호화를, ESP는 인증과 무결성 기능을 제공한다.
③ 암호화 기술을 이용하여 IP 패킷 단위로 데이터 변조 방지 및 은닉 기능을 제공한다.
④ 터널 모드는 IP 헤더를 포함한 기존 전체 패킷 앞에 새로운 IPSec 헤더 정보가 추가된다.

28. WEP 인증에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① RC4 대칭형 암호화 알고리즘을 사용하며 24bit의 IV를 결합하여 공유 비밀키를 생성한다.
② IEEE 802.11b의 표준인 스트림 암호화 기법을 사용한다.
③ 정적 키를 사용하기 때문에 무작위 공격에 취약하다.
④ AP는 인증 요청을 받으면 임의로 생성한 인증용 문자열을 암호화키로 암호화하여 클라이언트에 전송한다.

29. 다음에서 설명하는 블루투스 공격으로 가장 적절한 것은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다. 공격자는 블루투스 장치끼리 인증 없이 간편하게 정보를 교환하도록 개발된 OPP(Obex Push Profile) 기능을 이용하여 블루투스 장치에 있는 주소록이나 달력 등의 내용을 요청하여 열람하거나 취약한 장치의 파일에 접근할 수 있다.

① 블루스나핑　② 블루프린팅
③ 블루버깅　④ 블루재킹

30. 다음에서 설명하는 보안 기술로 가장 적절한 것은?

기업과 기관의 보안 정책을 반영하고, 다양한 네트워크 보안 제품의 인터페이스를 표준화하여 중앙 통합 관리, 침입 종합 대응, 통합 모니터링 등을 효율적으로 구현한 지능형 보안 관리 시스템이다.

① IDS　② ESM
③ NAC　④ IPS

31. 유닉스/리눅스 시스템 로그 설정(/etc/syslog.conf)에서 사용하는 메시지 우선순위 중 낮은 것부터 높은 것 순으로 가장 적절한 것은?

가. Notice 나. Alert 다. Error 라. Critical

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

32. 다음 중 인터넷 전송계층 프로토콜인 TCP에서 사용되는 용어로 가장 적절하지 <u>않은</u> 것은?

① Process-to-Process Service
② Port number
③ Segment
④ Datagram

33. 다음에서 설명하는 접근 통제 유형으로 가장 적절한 것은?

이것은 사용자 권한에 종속되지 않고, 민감하거나 중요한 자원에 대한 접근과 관련된 것이다. 예를 들면 일반 사용자가 관리자 권한을 전부 획득하지 못했더라도 관리자만 접근할 수 있는 메뉴에 접근하는 경우를 말한다.

① 수직적 접근 통제　② 수평적 접근 통제
③ 비즈니스 로직 접근 통제　④ 강제적 접근 통제

34. 다음에서 설명하는 소스코드 취약점으로 가장 적절한 것은?

개발 단계에서 사용자의 권한에 대한 검증을 적절하게 수행하지 않았을 때 주로 발생하는 취약점이다. 이것이 취약할 경우, 공격자는 매개변수 조작이나 강제 브라우저 접근 등을 통해 다른 사용자나 상위 관리자의 정보를 볼 수도 있다.

① 위험한 형식의 파일 업로드 취약점
② 디렉터리 경로 조작 취약점
③ 코드 내 중요 정보 노출 취약점
④ 세션 처리 및 접근 통제 취약점

35. 다음 빈칸 (㉠), (㉡)에 들어갈 용어로 가장 적절한 것은?

패스워드는 해시와 암호화 알고리즘으로 변경하여 저장하지만, 해시값이나 암호문은 동일한 결과만으로도 패스워드를 노출하는 단점이 있다. 따라서, (㉠)는 이런 상황을 막기 위해 패스워드 해시와 암호화에 사용하는 첨가물의 일종으로 운영체제별로 다양한 알고리즘이 존재한다. 패스워드 크래킹 방법 중 패스워드에 사용할 수 있는 문자열 범위를 정하고, 그 범위 안에서 생성 가능한 모든 패스워드를 생성하여 입력해 보는 방법이 (㉡)이다.

㉠	㉡
① Salt	사전 대입 공격
② Salt	무차별 대입 공격
③ S/Key	무차별 대입 공격
④ S/Key	사전 대입 공격

36. 다음 중 SIEM에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 보안솔루션 위주의 로그를 수집하고 통합한다.
② 사용자, IP, Port, Application 등의 단위로 분석이 가능하고, APT 공격 및 알려지지 않은 패턴에 대한 분석이 가능하다.
③ MapReduce, indexing 등을 사용하며 고성능의 데이터 분석이 가능하다.
④ 수집하는 정보는 보안시스템, 보안소프트웨어, 네트워크 장비에 대한 로그, 이벤트, 웹로그 등을 대상으로 한다.

37. 다음에 출력된 내용의 밑줄 친 ㉠에 대한 설명으로 가장 적절한 것은?

```
[root@localhost ~]#crontab -l
 - 생략 -
1 1 1 * * /home/cron.sh
          ㉠
```

① 매주 일요일 새벽 1시 1분에 cron.sh를 실행
② 매주 월요일 새벽 1시 1분에 cron.sh를 실행
③ 매월 1일 새벽 1시 1분에 cron.sh를 실행
④ 매일 새벽 1시 1분에 cron.sh를 실행

38. 다음에서 설명하는 이메일 보안 기술로 가장 적절한 것은?

IETF의 작업 그룹에서 개발한 전자우편 보안 기술이며, RFC 3370, 3850 등에 정의되어 있다. 전자우편에 대한 무결성, 부인불가, 암호화, 인증 등의 기능 제공을 위해 다양한 암호 알고리즘이 사용된다.

① PGP
② PEM
③ S/MIME
④ Mail-Safe

39. 다음에서 설명하는 SNMP의 구성 요소로 가장 적절한 것은?

이것은 관리할 개체의 집합이며, 관리자가 조회하거나 설정할 수 있는 개체들의 데이터베이스이고, 개체별로 트리 형식 구조를 이룬다. 관리될 각 개체를 위해 객체의 수를 결정하고, 이들을 정의된 규칙에 따라 이름을 붙이며, 각 객체에 유형을 연결한다.

① MIB
② SMI
③ OID
④ EGP

40. 다음에서 설명하는 악성코드로 가장 적절한 것은?

○ 전파할 때 과다한 TCP/135, 445 트래픽이 발생한다. ○ windows, windows/system32, winnt, winnt/system32 폴더에 svchost.exe 파일을 설치하고, 공격 성공 후 UDP/5599 등의 특정 포트를 열어 외부와 통신한다. ○ 대표적으로 아고봇, 웰치아, 블래스터 등이 있다.

① 백도어
② 스파이웨어
③ 익스플로잇
④ 시스템 공격형 웜