※ 답안지에 한 번 표기한 답을 수정테이프 등으로 정정하거나 칼 등으로 긁어 변형할 경우 그 문항은 무효로 처리함.

1. 정보보호의 목표에 관한 설명 중 옳지 않은 것은?
① 기밀성(Confidentiality)을 보장하기 위한 기술로는 암호화, 접근제어 등이 있다.
② 가용성(Availability)은 사용자가 필요할 때 데이터에 접근할 수 있는 능력을 말한다.
③ 가용성(Availability)을 유지하기 위해 데이터 백업, 위협 요소 제거 등의 기술을 사용할 수 있다.
④ 무결성(Integrity)은 특정한 작업 또는 행위에 대해 책임소재를 확인하는 것이 가능함을 말한다.

2. 암호 해독 공격의 유형에 관한 설명으로 옳지 않은 것은?
① 암호문 단독 공격(Ciphertext Only Attack)은 암호문만을 가지고 평문이나 키를 찾아내는 방법으로, 암호문의 통계적 특성 등을 추정하여 해독하는 방법이다.
② 알려진 평문 공격(Known Plaintext Attack)은 평문에 대응되는 암호문을 약간 알고 있는 상태에서, 나머지 암호문에 대한 공격을 하는 방법이다.
③ 선택 평문 공격(Chosen Plaintext Attack)은 암호 해독자가 암호기에 접근할 수 있어, 적당한 평문을 선택하여 그 평문에 해당하는 암호문을 얻어 키나 평문을 해독하는 방법이다.
④ 선택 암호문 공격(Chosen Ciphertext Attack)은 해독자가 암호기와 복호기에 모두 접근할 수 있어, 선택한 암호문에 대한 평문과 선택한 평문에 대한 암호문을 얻어 키나 평문을 해독하는 방법이다.

3. 블록 암호 모드에 관한 설명 중 옳지 않은 것은?
① ECB(Electronic Code Book) 모드는 평문을 동일한 크기의 평문블록으로 나누고, 키로 암호화하여 암호블록을 생성한다.
② CTR(CounTeR) 모드는 평문블록의 암호화를 병렬적으로 처리 가능하다.
③ CBC(Cipher Block Chaining) 모드는 인증을 수행하는 대칭키 암호 시스템의 하나인 Kerberos 버전 5에서도 사용된다.
④ CFB(Cipher Feed Back) 모드에서 이전 블록 값의 최상위 비트에서 발생한 에러는 이후 블록 값에 영향을 미치지 않는다.

4. 다음 중 AES의 특징이 아닌 것은?
① Feistel 구조의 암호화 알고리즘이다.
② 128비트 블록 단위의 암호화를 수행한다.
③ 사용 가능한 암호키의 길이는 총 3종류로 128비트, 192비트, 256비트가 있다.
④ 암호키 길이가 128비트인 경우 라운드의 횟수는 10회이다.

5. 비대칭키 암호화 알고리즘으로만 묶인 것은?
① RSA, ElGamal ② FEAL, AES
③ SEED, DES ④ ARIA, IDEA

6. MAC(Message Authentication Code)에 대한 설명 중 옳지 않은 것은?
① MAC에 대한 재전송 공격(Reply Attack)은 순서 번호(Sequence Number) 사용, 타임스탬프(Timestamp), 비표(Nonce) 등을 사용하여 막을 수 있다.
② HMAC(Hashed MAC)은 일방향 해시 함수를 이용하여 메시지 인증 코드를 구성하는 방법이다.
③ MAC은 제3자에 대한 증명, 부인방지를 해결할 수 없다.
④ HMAC(Hashed MAC)에 사용되는 일방향 해시함수는 교체가 어려워 다른 해시함수를 사용할 수 없다.

7. 전자 서명에 관한 설명 중 옳은 것은?
① 전자 서명의 요구조건으로는 재사용 가능과 서명자 인증이 있다.
② 전자 서명에서 메시지를 송신자의 개인키로 암호화하는 것이 서명 작성에 해당되고, 그 암호문을 송신자의 공개키로 복호화하는 것이 서명 검증에 해당한다.
③ 전자 서명을 통해 메시지의 기밀성이 보장되는 통신을 할 수 있다.
④ 전자 서명으로 부인은 방지할 수 있지만, 내용 변경 행위를 검출 할 수는 없다.

8. 다음 지문은 윈도우 운영체제의 주요 하이브 레지스트리에 관한 설명이다. 옳은 것은 모두 몇 개인가?

가. HKEY_CURRENT_CONFIG는 시작 프로세스에서 필수적인 소프트웨어 관련 정보를 포함한다.
나. HKEY_LOCAL_MACHINE은 컴퓨터 하드웨어 및 운영체제 정보를 포함한 시스템 설정 정보를 갖고 있다.
다. HKEY_CLASSES_ROOT는 파일 확장자에 대한 정보를 갖고 있다.
라. HKEY_USERS는 시스템에 등록된 모든 사용자들에 대한 정보를 갖고 있다.

① 1개 ② 2개 ③ 3개 ④ 4개

9. 쿠키(Cookie)에 관한 설명 중 옳지 않은 것은?
① 쿠키는 사용자가 인터넷 웹 사이트에 방문할 때 생기는 8KB 이상의 파일을 말한다.
② 쿠키는 유효기간, 패스, 도메인 등의 내용을 포함하고 있다.
③ 사용자가 웹 사이트에 방문하면 웹 사이트는 사용자의 컴퓨터에 쿠키를 만든다.
④ 쿠키는 단순히 정보를 담고 있는 텍스트 파일이기 때문에 바이러스를 전파할 수는 없다.

10. 다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은?

chmod 733 test.txt

① -rwxrwxrwx ② -rwxr--r--
③ -rwx-wx-wx ④ -rwxr-xr-x

11. 시스템에 상주하는 프로세스 정보를 알려주는 명령어는?

① df ② file ③ find ④ ps

12. 다음 괄호 안에 알맞은 것은?

> 리눅스 시스템에서 관리자(root) 권한이 필요 없는 프로그램에 소유자가 관리자(root)로 되어 있으면서 ( )가 설정된 경우에는 시스템의 보안에 허점을 초래할 수 있다. 실제로 이것이 설정된 파일은 백도어 및 버퍼 오버플로우 등 여러 공격에 이용된다.

① SetGID ② SetUID
③ Sticky Bit ④ umask

13. 악성코드 중 자기복제 기능은 없지만, 다른 프로그램으로 위장하여 공격하는 악성코드는?

① 바이러스(Virus) ② 웜(Worm)
③ 님다(Nimda) ④ 트로이 목마(Trojan Horse)

14. OSI 7 계층 중 계층과 데이터 전송단위가 바르게 짝지어진 것은?

① Application - Packet ② Transport - Segment
③ Network - Frame ④ Data Link - Data

15. 다음 무선랜 보안에 관한 설명 중 옳은 것은 모두 몇 개인가?

> 가. TKIP는 64비트의 확장된 길이의 초기벡터(IV)를 사용한다.
> 나. WEP 인증은 양방향 인증을 제공하여 보안에 강하다.
> 다. WPA는 RADIUS, Kerberos 등과 같은 다른 인증서버와 호환 가능하다.
> 라. WPA2는 2세대 WPA로써, RSA에 기반을 둔 CCMP 암호화 방식을 사용한다.
> 마. EAP 인증 방식은 WPA에서는 사용할 수 없고, WPA2 이후부터 사용 가능하다.

① 1개 ② 2개 ③ 3개 ④ 4개

16. 다음 중 DoS 공격의 대응 방안으로 옳은 것은 모두 몇 개인가?

> 가. UDP Flooding 공격 : 불필요한 서비스를 비활성화 한다.
> 나. SYN Flooding 공격 : 공격 인정 시간 내에 SYN 개수가 공격 인정 횟수 이상인 IP 주소를 소스로 해서 들어오는 트래픽을 차단한다.
> 다. Ping of death 공격 : 반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 무시하도록 설정한다.
> 라. LAND 공격 : 다른 네트워크로부터 자신의 네트워크로 들어오는 IP 브로드캐스트 패킷을 차단한다.

① 1개 ② 2개 ③ 3개 ④ 4개

17. 스니핑(Sniffing) 공격을 수행하는 스니퍼를 탐지하는 기법에 관한 설명 중 옳은 것은 모두 몇 개인가?

> 가. 유인(Decoy)을 이용한 탐지 : 관리자가 가짜 ID와 패스워드를 네트워크에 계속 뿌리고, 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지하는 방법
> 나. ARP를 이용한 탐지 : 정상적인 ARP Request를 보냈을 때 위조된 ARP Response를 되돌려 보내는 것을 모니터링하여 탐지하는 방법
> 다. ping을 이용한 탐지 : 네트워크에 존재하지 않는 MAC 주소로 위장하여 ping을 보냈을 때, ICMP Echo Reply를 되돌려 보내는지를 모니터링하여 탐지하는 방법
> 라. ARP Watch를 이용한 탐지 : MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여, 이를 변하게 하는 패킷이 탐지되면 알려주는 툴인 ARP Watch를 이용하여 탐지하는 방법

① 1개 ② 2개 ③ 3개 ④ 4개

18. 다음 설명에 해당하는 공격은?

> 개인 단체, 정치 단체, 국가, 산업체 등 목표 조직을 타깃으로 하여 다양한 보안 위협을 만들어 침해에 성공해 정보를 유출하거나 장기간의 접속 권한을 획득하기 위해 또는 장기간의 접근을 위해 지속적으로 수행되는 공격이다.

① APT(Advanced Persistent Threat)
② DDoS(Distributed Denial of Service)
③ Ransomware
④ Zero-Day Attack

19. 다음 중 DDoS 공격에 관한 설명으로 옳은 것은 모두 몇 개인가?

> 가. DDoS 공격에 사용된 좀비 PC는 악성코드의 흔적을 지우기 위해 스스로 하드디스크를 손상시킬 수도 있다.
> 나. DDoS 공격의 구성 요소로는 공격자, 마스터, 핸들러 프로그램, 에이전트 등이 있다.
> 다. 트리누(Trinoo), TFN 등이 대표적인 공격 유형이다.
> 라. DDoS 공격에서 악성코드에 감염된 좀비 PC끼리 형성된 네트워크를 봇넷(Botnet)이라고 한다.
> 마. 라우터의 Egress 필터링 기능을 이용하여 대응할 수 있다.

① 2개 ② 3개 ③ 4개 ④ 5개

20. 다음 중 세션 하이재킹(Session Hijacking)에 관한 설명으로 옳은 것은 모두 몇 개인가?

> 가. 정당한 절차로 인증을 받은 사용자의 세션을 가로채는 공격이다.
> 나. 패킷의 유실과 재전송이 증가해 서버와의 응답시간이 길어진다.
> 다. 공격자는 클라이언트와 서버 사이의 기존 세션을 동기화 시킨다.
> 라. 암호화, 지속적인 인증 등을 통해 대응할 수 있다.

① 1개 ② 2개 ③ 3개 ④ 4개

21. 다음 설명에 해당하는 기술은?

> 과거 IP 관리 시스템에서 발전한 솔루션을 말한다. 이 기술은 클라이언트가 네트워크에 접근하는 것을 통제할 뿐만 아니라, IP가 무질서하게 사용되는 것을 막아, 가용 IP를 쉽게 확인할 수 있게 해주고 IP 충돌로 인한 문제를 막아준다.

① NAT(Network Address Translation)
② NAC(Network Access Control)
③ VLAN(Virtual Local Area Network)
④ VPN(Virtual Private Network)

22. IPS(Intrusion Prevention System)와 IDS(Intrusion Detection System)에 관한 설명 중 옳지 <u>않은</u> 것은?

① IPS는 침입 공격에 대하여 방지하는 것을 목표로 하는 시스템이다.
② IPS는 호스트의 IP 주소, 포트번호, 사용자 인증에 기반을 두고 외부 침입을 차단한다.
③ IDS는 침입 공격에 대하여 탐지하는 것을 목표로 하는 시스템이다.
④ IDS는 해커의 공격이나 정보유출이 탐지되면 해당 기능을 차단하도록 되어 있다.

23. IPSec의 프로토콜 구조로 옳지 <u>않은</u> 것은?

① Encapsulating Security Payload
② Security Association
③ Internet Group Management Protocol
④ Authentication Header

24. 다음 중 네트워크 스캔(Network Scan)에 관한 설명으로 옳은 것은 모두 몇 개인가?

> 가. TCP FIN 스캔은 TCP 헤더 내에 FIN 플래그(flag)를 설정하여 전송하는 방식으로 Half-open 스캔 방식에 속한다.
> 나. TCP Full Open 스캔은 포트가 열려 있는 경우, 대상시스템으로부터 SYN+ACK 패킷을 수신하면 RST 패킷을 보내 연결 과정을 중단한다.
> 다. XMAS 스캔은 스텔스(Stealth) 스캔에 속한다.
> 라. XMAS 스캔은 패킷의 모든 플래그를 NULL로 설정하여 전송한다.
> 마. NULL 스캔의 대상이 포트가 닫혀 있을 경우 RST 패킷이 돌아온다.

① 1개 ② 2개 ③ 3개 ④ 4개

25. 메일의 헤더 정보, 제목, 메시지 내용의 특정 단어 및 문장 패턴을 검색하여 스팸 메일을 탐지 및 차단하는 기술적 대응 방안은?

① 콘텐츠 필터링 ② 발송량 기준 차단
③ 송신자 필터링 ④ 시간대별 차단

26. 다음 설명에 해당하는 DNS 보안 위협은?

> 보안이 취약한 DNS 서버에 조작된 쿼리를 전송하여 DNS 서버가 저장하고 있는 주소 캐시(Cache) 정보를 위·변조하는 공격이다.
> 이 공격을 통해 사용자는 자신이 의도하지 않은 다른 사이트로 접속되는 문제가 발생한다.

① DNS Cache Poisoning 공격
② Bind DNS 서비스 방해 공격
③ DNS Spoofing
④ DNS Sinkhole

27. 다음 설명에 해당하는 것은?

> 응용 프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 말한다 또한, 컴퓨터 메모리에서 애플리케이션 호스트 시스템에 해를 끼치지 않고 작동하는 것이 허락된 보호받는 제한구역을 가리킨다.

① Sandbox ② Bluebox
③ Middlebox ④ Whitebox

28. 웹 취약점 및 공격에 대한 설명 중 옳지 <u>않은</u> 것은?

① 명령 삽입 취약점 : 클라이언트의 요청을 처리하기 위해 전송받은 인수에 특정 명령을 실행하는 코드를 포함시켜 웹서버에 전송하는 것
② XSS(Cross Site Scripting) 취약점 : 공격자에 의해 작성된 스크립트가 다른 웹사용자에게 전달되어 수행되는 것
③ CSRF(Cross Site Request Forgery) 취약점 : 브라우저를 통해 디렉터리에 있는 파일과 목록을 나열하는 것
④ SQL Injection 공격 : 데이터베이스와 연동되어 있는 애플리케이션의 입력값을 조작하여 DBMS가 의도되지 않은 결과를 반환하도록 하는 공격 기법

29. 다음 사례에 해당하는 WEB 공격 유형은?

> 입사 지원을 위한 채용 사이트에서는 지원자의 성명, 주민등록번호, 주소 등 입사 지원 정보에 대한 확인 방법을 숫자로 된 단순 아이디 값으로 검증하고 있다. 이로 인해 공격자는 지원자 별로 할당된 숫자 아이디 파라미터 값을 순차적으로 증가시켜 타인의 입사지원서를 열람할 수 있는 자동화 프로그램을 제작하여 개인정보를 유출하였다.

① SQL Injection 공격
② 사회공학 기법
③ 파라미터 변조 취약점
④ 파일 다운로드 취약점

30. 전자상거래에서 사용되는 SET 프로토콜에 관한 설명 중 옳지 <u>않은</u> 것은?

① RSA 암호화를 사용하여 속도가 빠르고, 강력한 보안을 제공한다.
② 기존의 신용카드 기반을 그대로 활용할 수 있다.
③ 신용카드 소지자에게 전자지갑 소프트웨어를 요구한다.
④ 신용카드 트랜잭션을 보호하기 위해 기밀성, 인증 및 메시지 무결성 등의 서비스를 제공한다.

31. 다음 설명에 해당하는 전자서명 방식은?

고객의 지불정보가 판매자를 통하여 해당 지급정보 중계기관으로 전송됨에 따라 고객의 지불정보가 판매자에게 노출될 가능성과 판매자에 의한 결제 정보의 위·변조 가능성을 제거한다.

① 부인불가 서명 ② 이중 서명
③ 은닉 서명 ④ 위임 서명

32. 재해복구 시스템은 복구 수준에 따라 4가지 유형으로 구분된다. 다음 중 콜드 사이트(Cold Site) 복구 시스템에 관한 설명으로 적합한 것은?

① 주 센터와 동일한 수준의 정보기술자원을 원격지에 구축하고, 주 센터와 재해복구센터 모두 운영(Active) 상태로 동시에 서비스를 제공하는 방식
② 주 센터와 동일한 수준의 정보기술자원을 대기 상태로 원격지에 구축하여 주 센터 재해 발생 시 재해복구센터의 정보 시스템을 운영(Active) 상태로 서비스를 제공하는 방식
③ 데이터만 백업하여 원격지에 보관하고, 업무 재개를 위한 정보기술자원은 확보하지 않거나 또는 장소 등 최소한의 자원만 확보한 후, 재해 시 백업된 데이터를 활용하여 정보 시스템을 복구하는 방식
④ 핫 사이트와 유사하나, 주 센터와 동일한 정보기술자원을 보유하는 대신에 중요성이 높은 자원만 부분적으로 재해복구센터에 보유하는 방식

33. 다음 괄호 안에 해당하는 국제 표준은?

( )은(는) 과거 BS7799 Part01에서 ISO/IEC17799를 거쳐 현재는 국제 표준이 되었다. 정보보호 관리체계(ISMS)를 수립, 구현 및 유지하기 위해 공통적으로 적용할 수 있는 실무적인 지침 및 일반적인 원칙을 규정하고 있다.

① ISO/IEC 27000 ② ISO/IEC 27002
③ ISO/IEC 27004 ④ ISO/IEC 27006

34. 정보보호 관리체계(ISMS)에 관한 설명 중 옳은 것은?

① ISMS 인증 제도는 「정보통신기반 보호법」에 근거를 두고 2002년부터 시행해오고 있다.
② 인증 심사 기준은 정보보호관리과정과 정보보호대책의 두 가지로 구성되어 있다.
③ 모든 기업이 자율적으로 심사를 신청하는 자율 제도로 운영된다.
④ 국가정보원이 평가하여 인증하며, 인증의 유효기간은 3년이다.

35. 다음 중 OWASP(Open Web Application Security Project)에서 발표한 OWASP TOP 10 - 2017에 해당되는 항목은 모두 몇 개인가?

가. 인젝션	나. 취약한 인증
다. 민감한 데이터 노출	라. XML 외부 개체(XXE)
마. 크로스 사이트 요청 변조(CSRF)	
바. 안전하지 않은 역직렬화	

① 2개 ② 3개 ③ 4개 ④ 5개

36. 「정보통신기반 보호법」에서 명시한 주요정보통신기반시설의 취약점을 분석·평가하는 전담반에 속하지 <u>않는</u> 것은?

① 한국인터넷진흥원
② 한국전자통신연구원
③ 「정보통신기반 보호법」 제16조의 규정에 의한 정보공유·분석센터
④ 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 컨설팅 전문기업

37. 「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)에서 개인정보 보호책임자의 업무에 속하지 <u>않는</u> 것은?

① 개인정보 보호 인증 취득
② 개인정보 보호 교육 계획의 수립 및 시행
③ 개인정보 처리와 관련한 불만의 처리 및 피해 구제
④ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

38. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조(개인정보의 수집·이용 동의 등)에서 정의하는 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 이용자에게 알리고 동의 받아야 할 사항이 <u>아닌</u> 것은?

① 개인정보의 수집·이용 목적
② 수집하는 개인정보의 항목
③ 개인정보처리의 위탁기관명
④ 개인정보의 보유·이용 기간

39. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3(개인정보 유출등의 통지·신고)에서 통지 및 신고 시에 필수로 포함되어야 할 사항은 모두 몇 개인가?

가. 유출등이 된 개인정보 항목 나. 유출등의 공격에 대한 분석 내용 다. 유출등이 발생한 시점 라. 이용자가 취할 수 있는 조치 마. 정보통신서비스 제공자등의 대응 조치

① 1개 ② 2개 ③ 3개 ④ 4개

40. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정의하는 용어에 관한 설명으로 옳은 것은 모두 몇 개인가?

가. “정보통신서비스”란 「전기통신사업법」 제2조 제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다. 나. “침해사고”란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다. 다. “전자적 전송매체”란 정보통신망을 통하여 부호·문자·음성·화상 또는 영상 등을 수신자에게 전자문서 등의 전자적 형태로 전송하는 매체를 말한다. 라. “통신과금서비스이용자”란 정보보호제품을 개발·생산 또는 유통하는 사람이나 정보보호에 관한 컨설팅 등과 관련된 사람을 말한다. 마. “전자문서”란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전기적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 정형화된 것을 말한다.

① 2개 ② 3개 ③ 4개 ④ 5개