정보보호론

문 1. AES(Advanced Encryption Standard)에 대한 설명으로 옳지 않은 것은?

① 미국 NIST(National Institute of Standards and Technology)의 공모에서 Rijndael이 AES로 채택되었다.
② 128비트 크기의 블록 대칭키 암호 알고리즘이다.
③ Feistel 구조를 사용한다.
④ 128, 192, 256비트 길이의 키를 사용할 수 있다.

문 2. 다음 설명에 해당하는 악성 소프트웨어를 옳게 짝지은 것은?

> ㄱ. 시스템 및 응용 소프트웨어의 취약점을 악용하거나 전자우편 또는 공유 폴더를 이용하며, 네트워크를 통해서 컴퓨터에서 컴퓨터로 빠르게 전파된다.
> ㄴ. 사용자 컴퓨터 내에서 자신 또는 자신의 변형을 다른 실행 프로그램에 복제하여 그 프로그램을 감염시킨다.
> ㄷ. 겉으로 보기에는 유용해 보이지만 정상적인 프로그램 속에 숨어있는 악성 소프트웨어로, 사용자가 프로그램을 실행할 때 동작한다.

	ㄱ	ㄴ	ㄷ
①	웜	바이러스	트로이목마
②	바이러스	웜	봇
③	바이러스	웜	트로이목마
④	웜	바이러스	봇

문 3. 메일 수신 서버 또는 웹 메일 서버로부터 전자우편 메시지를 자신의 컴퓨터 단말 장치로 전송받는 데 사용되는 프로토콜이 아닌 것은?

① IMAP(Internet Mail Access Protocol)
② RTP(Realtime Transport Protocol)
③ POP(Post Office Protocol)
④ HTTP(HyperText Transfer Protocol)

문 4. 컴퓨터 보안의 형식 모델에 대한 설명으로 옳은 것은?

① Clark-Wilson 모델은 강력한 기밀성 모델을 제안하며, 데이터 및 데이터를 조작하는 트랜잭션에 높은 수준의 기밀성을 제공한다.
② Bell-LaPadular 모델은 이해 충돌이 발생할 수 있는 상업용 응용프로그램을 위해 개발되었으며, 강제적 접근 개념을 배제하고 임의적 접근 개념을 이용한 것이다.
③ Biba 모델은 데이터 무결성을 위한 것으로, 사용자 자신과 같거나 자신보다 낮은 무결성 수준의 데이터에만 쓸 수 있고, 자신과 같거나 자신보다 높은 무결성 수준의 데이터만 읽을 수 있도록 한 것이다.
④ Bell-LaPadular 모델은 다중 수준 보안에서 높은 수준의 주체가 낮은 수준의 주체에게 정보를 전달하는 것을 다루기 위한 것이다.

문 5. 「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)에서 개인정보처리자가 주민등록번호를 처리할 수 있도록 허용하는 경우는?

① 정보주체에게 별도로 동의를 받은 경우
② 시민단체에서 주민등록번호 처리를 요구한 경우
③ 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
④ 개인정보처리자가 주민등록번호 처리가 불가피하다고 판단한 경우

문 6. TCP 표준을 준수하는 서버의 열린 포트와 닫힌 포트를 판별하기 위한 TCP FIN, TCP NULL, TCP Xmas 포트 스캔 공격 시, 대상 포트가 닫힌 경우 세 가지 공격에 대하여 동일하게 서버가 응답하는 것은?

① SYN/ACK
② RST/ACK
③ RST
④ 응답 없음

문 7. SET(Secure Electronic Transaction)에 대한 설명으로 옳지 않은 것은?

① 신용조회 네트워크와 인터넷 사이에 설치된 지불 게이트웨이가 지불 명령을 처리한다.
② 신용카드 정보를 판매자가 알 수 있도록 단일 서명 방식을 사용한다.
③ 대칭키 암호화 방식과 공개키 암호화 방식이 모두 사용된다.
④ 신용카드를 이용한 인터넷상의 전자결제를 안전하게 할 수 있게 하는 기술이다.

문 8. UNIX 시스템의 특수 접근 권한에 대한 설명으로 옳은 것은?

① getuid는 접근 권한을 출력하거나 변경한다.
② setgid는 파일 소유자의 권한을 지속적으로 사용자에게 부여한다.
③ setuid가 설정된 파일은 파일 사용자의 권한으로 실행된다.
④ sticky bit가 설정된 디렉터리에 있는 파일은 소유자 외 다른 일반 사용자에 의해 삭제되지 않는다.

문 9. 다음에 열거된 순서대로 진행되는 공격은?

> ○ 취약점이 존재하는 웹 서버의 애플리케이션에 악성코드를 삽입
> ○ 해당 웹 서비스 사용자가 공격자가 작성하여 저장한 악성코드에 접근
> ○ 웹 서버는 사용자가 접근한 악성코드가 포함된 게시판의 글을 사용자에게 전달
> ○ 사용자 브라우저에서 악성 스크립트가 실행
> ○ 실행 결과가 공격자에게 전달되고 공격자는 공격을 종료

① 저장(stored) Cross-Site Scripting
② 반사(reflected) Cross-Site Scripting
③ 명령어 삽입(command injection)
④ SQL 삽입(injection)

문 10. 정보보호 관련 법률에서 규정한 인증 제도에 대한 설명으로 옳지 않은 것은?
① 정보보호 관리체계 인증은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 과학기술정보통신부장관이 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 정해진 기준에 적합한지에 관하여 인증할 수 있도록 한 것이다.
② 개인정보보호 관리체계 인증은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 방송통신위원회가 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 정해진 기준에 적합한지에 관하여 인증을 할 수 있도록 한 것이다.
③ 정보보호제품 평가·인증은 「정보통신기반 보호법」상 행정안전부장관이 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호 시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있도록 한 것이다.
④ 개인정보보호 인증은 「개인정보 보호법」상 행정안전부장관이 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 같은 법에 부합하는지 등에 관하여 인증할 수 있도록 한 것이다.

문 11. 보안의 3대 요소 중 가용성에 대한 직접적인 위협 행위는?
① 데이터 변조(modification)
② 패킷 범람(packet flooding)
③ 신분 위장(masquerading)
④ 트래픽 분석(traffic analysis)

문 12. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은?
① 두 사용자가 메시지 암호화에 사용할 공개키를 안전하게 교환하기 위한 것이다.
② 중간자(MITM) 공격에 안전하다.
③ 키를 교환하는 두 사용자 간의 상호 인증 기능을 제공한다.
④ 이산대수 문제를 푸는 것이 어렵다는 점을 활용한 것이다.

문 13. 인증기관에서 사용자에게 발급한 인증서의 생성 방법에 대한 설명으로 옳은 것은?
① 사용자의 공개키를 포함한 인증 정보를 인증기관의 공개키로 암호화한다.
② 사용자의 개인키를 포함한 인증 정보를 인증기관의 개인키로 암호화한다.
③ 사용자의 공개키를 포함한 인증 정보를 인증기관이 자신의 개인키로 서명한다.
④ 사용자의 공개키를 포함한 인증 정보를 인증기관의 독자적인 해시 함수로 해시한다.

문 14. 전송할 메시지에서 메시지 무결성 검증을 위한 고정 크기의 출력물을 만드는 방법으로 적합한 것만을 고른 것은?
① 메시지 인증 코드 생성기, 해시 함수
② 의사 난수 생성기, 해시 함수
③ 메시지 인증 코드 생성기, 코덱
④ 난수 생성기, 코덱

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 의거하여 정부가 정보통신망의 고도화(정보통신망의 구축·개선 및 관리에 관한 사항을 제외한다)와 안전한 이용 촉진 및 방송통신과 관련한 국제협력·국외진출 지원을 효율적으로 추진하기 위하여 설립한 기관은?
① 방송통신위원회
② 한국인터넷진흥원
③ 한국정보화진흥원
④ 정보통신산업진흥원

문 16. 쿠키에 대한 설명으로 옳지 않은 것은?
① 웹 사이트 접속 시 HTTP의 무상태성(statelessness)을 보완하기 위해 사용되는 정보이다.
② 사용자가 웹 사이트에 접속할 때 사용자 컴퓨터에서 생성되어 해당 웹 서버에 임시 파일로 전송·저장된다.
③ 보존 기간에 따라 임시(또는 세션) 쿠키와 영구(persistent) 쿠키로 분류할 수 있다.
④ 사용자가 인식하지 못하는 사이에 사용자의 다양한 정보가 쿠키에 담겨 웹 서버로 전송될 수 있기 때문에 개인정보에 대한 피해가 발생할 수 있다.

문 17. 동일 LAN 상에서 서버와 클라이언트의 IP 주소에 대한 2계층 MAC 주소를 공격자의 MAC 주소로 속임으로써, 공격자가 서버와 클라이언트 간의 통신을 엿듣거나 통신 내용 또는 흐름을 왜곡시킬 수 있다. 이러한 상황에서 발생한 공격과 거리가 먼 것은?
① MITM(Man-In-The-Middle)
② 스니핑(sniffing)
③ ARP 스푸핑(spoofing)
④ IP 스푸핑(spoofing)

문 18. ISO 27001:2013의 통제 항목에 해당하지 않는 것은?
① 정보보호 정책(information security policy)
② 자산 관리(asset management)
③ 모니터링과 검토(monitoring and review)
④ 정보보호 사고 관리(information security incident management)

문 19. RSA 암호 시스템에서 어떤 사용자의 공개키를 {e,n}이라 할 때, 평문 블록 M과 암호문 블록 C는 수식, $C = M^e \bmod n$을 만족한다. n을 두 소수 11과 13의 곱이라 할 때, e로 선택할 수 있는 것만을 모두 고른 것은?

ㄱ. 9	ㄴ. 17	ㄷ. 19	ㄹ. 127

① ㄴ, ㄷ
② ㄱ, ㄴ, ㄷ
③ ㄴ, ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ

문 20. 클라이언트와 서버 간의 파일 전송을 위한 FTP(File Transfer Protocol)에 대한 설명으로 옳지 않은 것은?
① TCP 포트 21은 제어 연결을 위해, TCP 포트 20은 데이터 연결을 위해 사용된다.
② 공개 파일 접근을 허용하는 사이트에서는 익명(anonymous) 로그인을 사용할 수 있으나, 익명 사용자에게는 보안상 제한적인 명령어만 사용하도록 한다.
③ 로그인 시 사용자 아이디와 패스워드를 사용하더라도 로그인 정보 도청이 가능하다.
④ FTP 대신에 TELNET를 사용함으로써 인증과 무결성의 보안 문제를 해결할 수 있다.