정보보호론

문 1. 송신자가 수신자에게 전달하는 세션키를 공개키 암호 방식을 이용하여 암호화할 때 사용되는 키는?

① 송신자의 개인키
② 송신자의 공개키
③ 수신자의 개인키
④ 수신자의 공개키

문 2. 다음의 정보보호와 관련된 원칙을 제시한 사람은?

> 이 원칙은 공격자가 암호 알고리즘을 완전히 알고 있더라도 키가 없이는 복호화해 평문을 얻을 수 없어야 함을 의미하는 것으로, 암호 알고리즘의 안전성이 암호 알고리즘 설계 자체의 비밀성에 의존해서는 안 되고 키의 비밀성에 의존해야 함을 강조한다. 따라서 암호 알고리즘은 널리 공개해서 많은 암호학자의 검증을 거치는 과정을 통해 안전성을 인정받아야 한다.

① Rabin
② Hellman
③ Kerckhoffs
④ Koblitz

문 3. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

> PGP 기법은 세션키로 메시지를 암호화하기 위해 [(가)] 알고리즘과 사용자 인증을 위한 전자서명에 이용하기 위해 [(나)] 알고리즘을 사용할 수 있다.

	(가)	(나)
①	IDEA	RSA
②	IDEA	DES
③	RSA	IDEA
④	RSA	AES

문 4. 쓰레기 처리장 또는 휴지통을 뒤져서 정보를 얻어내는 사회공학적 공격 기법은?

① Eavesdropping
② Shoulder Surfing
③ Dumpster Diving
④ Forensic Analysis

문 5. 접근제어(Access Control)에 대한 설명으로 옳지 않은 것은?

① 임의적 접근제어(Discretionary Access Control)는 정보 소유자가 정보의 보안 수준을 결정하고 그에 대한 접근제어까지 설정한다.
② BLP(Bell-LaPadula) 모델과 Biba 모델은 강제적 접근제어(Mandatory Access Control) 모델에 해당한다.
③ 역할 기반 접근제어(Role-Based Access Control)는 사람이 아닌 역할 또는 직책에 권한을 부여한다.
④ BLP 모델에서는 낮은 수준의 보안 권한을 가진 사람이 자신의 권한보다 높은 보안 수준의 문서에 쓸 수 없다.

문 6. 윈도우 운영체제에서 컴퓨터의 MAC 주소를 출력하는 명령어는?

① ping
② ipconfig/all
③ ifconfig
④ nslookup

문 7. 다음 /etc/passwd 파일 내용의 일부에서 사용자의 그룹 ID는?

```
user05:x:1001:501:group05:/home/user05:/bin/bash
```

① x
② 1001
③ 501
④ group05

문 8. 다음은 블록 암호의 운영모드 중 하나를 표현하고 있다. 해당 운영모드에 대해 추론할 수 있는 설명으로 옳은 것은? (단, $i, j \geq 0$, $i \neq j$이다)

P_i: 평문 블록	$C_i = P_i \oplus O_i$
C_i: 암호문 블록	$P_i = C_i \oplus O_i$
E_k: 암호화 함수(키 k 이용)	$O_i = E_k(I_i)$
IV: 초기벡터(Initial Vector)	$I_i = O_{i-1}$(단, $I_0 = IV$)

① C_i에 비트 오류가 발생하더라도 복호화된 P_j에 영향을 미치지 않는다.
② P_i와 P_j가 동일할 경우 C_i와 C_j가 같아지는 문제점이 존재한다.
③ 고속의 암·복호화를 위해 별도의 전처리 없이 병렬처리가 가능하다.
④ 복호화에 사용되는 IV값은 암호화에 사용된 IV값과 다를 수 있다.

문 9. 개인정보 보호법령상 민감정보와 고유식별정보를 바르게 연결한 것은?

① 유전자검사 등의 결과로 얻어진 유전정보 – 운전면허의 면허번호
② 정당의 가입정보 – 유전자검사 등의 결과로 얻어진 유전정보
③ 여권번호 – 외국인등록번호
④ 범죄경력자료 – 군번

문 10. 개인정보보호위원회 고시에 따른 개인정보 영향평가 영역과 평가분야를 짝 지은 것으로 옳지 않은 것은?

① 대상기관 개인정보보호 관리체계 – 개인정보 침해대응
② 대상시스템의 개인정보보호 관리체계 – 접근권한 관리
③ 개인정보처리 단계별 보호조치 – 이용 및 제공
④ 대상시스템의 기술적 보호조치 – 개인정보의 암호화

문 11. 사용자가 웹브라우저에서 정확한 웹페이지 주소를 입력하여도 가짜 웹페이지로 접속되는 피싱 공격은?

① 보이스 피싱(Voice Phishing)
② 메신저 피싱(Messenger Phishing)
③ 스미싱(Smishing)
④ 파밍(Pharming)

문 12. DSS(Digital Signature Standard)에 대한 설명으로 옳지 않은 것은?

① 부인방지를 보장한다.
② 공개키 암호 방식을 사용한다.
③ 메시지의 길이에 비례하는 길이의 전자서명을 생성한다.
④ 사용되는 해시 함수는 일방향성과 충돌 저항성을 만족해야 한다.

문 13. KISA의 IoT 공통 보안 7대 원칙을 기반으로 IoT 보안을 수행할 때 옳지 않은 것은?

① 안전한 초기 보안 설정 방안을 제공하여 기본으로 설정된 파라미터 설정 후 재설정 금지
② 안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라미터 설정
③ IoT 제품과 서비스의 취약점 패치 및 업데이트 지속 이행
④ 안전한 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련

문 14. 다음에서 설명하는 시스템 공격 기법은?

> ○ 두 개 이상의 프로세스가 동시에 한정된 CPU 자원을 활용할 경우 서로 경쟁하는 상황이 발생
> ○ 두 개의 프로세스는 일반 프로그램과 공격 프로그램에 의해 생성되며, 일반 프로그램은 파일 소유자가 root이며 임시파일을 생성하는 SetUID가 설정된 프로그램
> ○ 공격자는 SetUID가 설정된 일반 프로그램이 생성하는 임시파일에 심볼릭 링크를 연결하여 일반 프로그램이 생성하는 임시파일을 공격 프로그램이 원하는 목표파일로 연결하는 공격

① Race Condition Attack
② Reverse Engineering Attack
③ Format String Attack
④ Heap Buffer Overflow Attack

문 15. 무선랜 보안 기술에 대한 설명으로 옳지 않은 것은?

① TKIP는 WPA의 취약점을 해결하기 위해 도입되었다.
② CCMP는 CBC-MAC와 CTR 모드를 이용한다.
③ IEEE 802.11i는 TKIP와 CCMP 방식을 지원한다.
④ WPA2는 AES 암호 알고리즘을 이용한다.

문 16. 스택 버퍼 오버플로우 공격에 대한 방어 기법으로 옳지 않은 것은?

① Stack Guard
② ASLR(Address Space Layout Randomization)
③ Stack Shield
④ Stack Frame

문 17. IDS(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은?

① 비정상행위(Anomaly) 침입탐지는 오용(Misuse) 침입탐지 대비 낮은 오탐률을 보이지만 알려지지 않은 새로운 공격에 취약하다.
② 호스트 기반 IDS는 트로이목마, 백도어, 내부자에 의한 공격을 탐지할 수 있다.
③ '외부망  라우터  내부망'으로 구성된 네트워크에서 네트워크 기반 IDS를 Ⓐ 위치에 설치할 경우, Ⓑ 위치에 설치할 경우보다 이론적으로 더 많은 네트워크 공격을 탐지할 수 있지만 처리할 데이터가 더 많다는 단점이 있다.
④ IDS 설계 시 침입자의 행동을 엄격하게 정의할수록 공격탐지의 부정오류(False Negative)가 증가한다.

문 18. 리눅스 사용자 user02의 현재 패스워드 유효기간을 60일로 지정하는 명령어는?

① passwd -l 60 user02
② passwd -w 60 user02
③ chage -M 60 user02
④ chage -W 60 user02

문 19. 데이터베이스 암호화 방식에 대한 설명으로 옳지 않은 것은?

① Plug-In 방식은 구축 시 일부 응용프로그램 수정이 필요할 수 있으며 DB 성능에 대한 검토가 필요하다.
② Hybrid 방식은 일반적으로 Plug-In 방식과 TDE(Transparent Data Encryption) 방식이 조합된 것이다.
③ API 방식은 응용프로그램 서버에 설치하는 방식으로써 응용프로그램의 수정이 필요하다.
④ TDE 방식은 DBMS 내부 또는 옵션으로 제공되는 암호화 기능을 이용한다.

문 20. 섹터의 크기가 512바이트이고, 4개의 섹터로 구성된 하나의 클러스터에 600바이트 크기의 데이터 파일이 저장되어 있을 때, RAM 슬랙의 크기[바이트]와 파일 슬랙의 크기[바이트]를 바르게 연결한 것은?

	RAM 슬랙의 크기	파일 슬랙의 크기
①	424	1024
②	424	1448
③	1024	424
④	1024	1448

문 21. ISMS-P(정보보호 및 개인정보보호 관리체계 인증)의 보호대책 요구사항에 해당되지 않는 분야는?

① 정책, 조직, 자산 관리
② 외부자 보안
③ 개인정보 제공 시 보호 조치
④ 접근통제

문 22. 「개인정보 보호법」상 개인정보처리자가 개인정보의 수집 및 이용 동의를 받을 때 정보주체에게 알릴 의무가 있는 사항이 아닌 것은?

① 개인정보를 제공받는 자
② 동의 거부 시 불이익이 있을 경우 그 불이익 내용
③ 수집하려는 개인정보의 항목
④ 개인정보의 보유 및 이용 기간

문 23. ISO 27001에 대한 설명으로 옳지 않은 것은?

① 영국의 BSI(British Standards Institute)에서 제정한 BS 7799를 기반으로 구성되어 있는 보안 프레임워크이다.
② ISO 27001:2013은 7개의 관리과정으로 구성되어 있으며, 정보보호 통제 요구사항은 10개 영역, 114개 통제 항목으로 구성되어 있다.
③ ISO 27001:2013의 관리과정을 PDCA 모델에 적용할 때, 조치(Act)에 해당하는 항목은 개선(Improvement)이다.
④ ISO 27001에서 제시한 프레임워크에 따라 조직의 위험을 관리하고 이를 개선해나가는 체계를 갖추더라도 보안 침해는 발생할 수 있다.

문 24. CC(Common Criteria)에서 사용하는 EAL(Evaluation Assurance Level)과 설계, 시험 및 검토 수준을 짝 지은 것으로 옳은 것은?

① EAL 1 – 구조적 시험
(structurally tested)
② EAL 3 – 방법론적 설계, 시험과 검토
(methodically designed, tested, and reviewed)
③ EAL 5 – 준정형적 설계와 시험
(semiformally designed and tested)
④ EAL 6 – 정형적으로 검증된 설계와 시험
(formally verified design and tested)

문 25. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자는 서비스 제공을 위해 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 이용자의 동의를 받도록 하고 있다. 이에 대한 사항으로 옳은 것은?

① 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우, 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실을 알리고 동의를 받아야 한다.
② 접근권한이 필요한 정보는 알리고 동의를 받아야 하지만 접근권한이 필요한 이유는 알릴 필요가 없다.
③ 접근권한의 범위 및 동의의 방법은 대통령령으로 정한다.
④ 이용자 정보 보호를 위하여 필요한 조치 및 그 밖에 필요한 사항은 과학기술정보통신부령으로 정한다.