2017 년 국가직 7 급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
③	④	④	①	①	②	①	④	③	②
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
②	①	④	②	②	②	③	④	③	①

문 1. 다음 대칭키 암호화에서 K 값은?

○ 8 비트 정보 P 와 K 의 배타적 논리합(XOR) 연산의 결과를 Q 라 함
○ P = 11010011
○ Q = 10000110

① 11010011
② 10000110
③ 01010101
④ 01010100

답 ③

XOR 연산은 두 입력 비트의 값이 같으면 0 을, 다르면 1 을 출력한다.

③ Q 의 값이 10000110 이기 때문에, P 와 K 의 1, 6, 7 번 비트는 다르고, 2, 3, 4, 5, 6, 8 번 비트는 같은 값을 가진다.
그러므로 K 는 01010101 이 된다.

(추가)

배타적 논리합(XOR)은 교환법칙이 성립하고

$P \oplus K = K \oplus P$

XOR 은 같은 값과의 연산을 두 번 반복하면 원래의 값이 나온다.

$(P \oplus K) \oplus K = P$

따라서 보기의 식을 계산하면,

$P \oplus K = Q$

$\Rightarrow P (P \oplus K) = P \oplus Q$

$\Rightarrow K = P \oplus Q$

그러므로 K 를 구하기 위해 P 와 Q 를 XOR 해도 된다.

문 2. DRM(Digital Right Management)에 대한 설명으로 옳지 않은 것은?

① 문서의 열람, 편집, 프린트 등에 대한 접근 권한을 설정한다.
② 문서 사용에 인가를 부여받은 사용자에게 접근을 허용한다.
③ DRM 모듈로 운영되는 시스템의 하드디스크는 도난당하더라도 정보 유출의 위험이 적다.
④ 사용하기 불편하므로 인증서를 전혀 사용하지 않는다.

답 ④

디지털 저작권 관리(Digital rights management, DRM)는 각종 미디어의 출판자 또는 저작권자가 배포한 디지털 자료나 하드웨어의 사용을 제어하고 불법적인 유통을 방지하도록 사용되는 기술들을 의미한다.

④ DRM(디지털 저작권 관리) 기술은 공개키 기반의 표준인 X.5.09 인증서를 사용한다.

<오답 체크> ①② DRM 기술은 허용된 사용자에게만 콘텐츠 사용을 허용하고, 불법적인 사용을 방지한다.

③ DRM 기술은 사용자를 확인하기 위해 SID(보안 식별자)나 CMID(클라이언트 식별자)나 랜카드의 MAC 어드레스 등을 활용하기 때문에, 데이터가 저장된 하드디스크만으로는 콘텐츠를 이용할 수 없어 보안이 유지된다.

문 3. 블록암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① IDEA - 상이한 대수 그룹으로부터의 세 가지 연산을 혼합하는 방식
② Blowfish - 키의 크기가 가변적이므로 안전성과 성능의 요구에 따라 유연하게 사용
③ SEED - 1999 년 KISA 와 국내 암호전문가들이 개발한 128 비트 블록암호
④ ARIA - 국가보안기술연구소 주관으로 64 비트 블록암호로 128 비트 암호화키만 지원

답 ④

④ ARIA
128 비트 블록
키 길이 128/192/256 비트
Involutional SPN 구조 12/14/16 라운드
KS 국가 표준, 효율성에 맞게 최적화, 다양한 환경에 적합

<오답 체크> ① IDEA 암호화 알고리즘은 블록 암호 알고리즘 중 가장 안전하다고 알려져 있다.
64 비트 블록 크기 / 128 비트 키 / 8 라운드
상이한 대수 그룹으로부터의 세 가지 연산(XOR, add mod 216, multiply mod 216+1)을 혼합하는 방식

② Blowfish
64 비트 블록 크기 / 32~448 비트의 가변 키 길이 /
16 라운드의 페이스텔 구조

③ SEED **(국산)**
1999 년 한국정보보호진흥원(KISA)이 개발
128 비트 블록 크기 / 128 또는 256 비트 키 /
16 라운드의 페이스텔 구조
- 1999 년 KISA 와 국내 암호전문가들이 개발한 128 비트 블록암호

문 4. 암호화에 대한 설명으로 옳지 않은 것은?

① AES 는 블록 크기가 192 비트이며, 키는 192 비트와 256 비트 두 가지를 사용한다.
② Rabin 은 RSA 와 같은 원리로 암호화하고, 2 차 합동에 근거하고 있다.
③ DES 는 대칭키 방식으로서 16 개 라운드로 구성되어 있다.
④ One-Time Pad 는 암호화를 수행할 때마다 랜덤하게 선택된 키 스트림을 사용한다.

답 ①

① AES(Advanced Encryption Standard)
SPN 구조 / 대칭키 알고리즘
블록 128 비트(16 바이트)
키 길이 128 비트 – 10 라운드
키 길이 192 비트 – 12 라운드
키 길이 256 비트 – 14 라운드

<오답 체크> ② RSA 는 지수 합동에 근거하고, Rabin 은 2 차 합동에 근거한다.

③ DES(Data Encryption Standard)
페이스텔(Fiestel) 구조 / 대칭키 알고리즘
블록 64 비트
키 길이 56 비트 + 패리티 8 비트 = 64 비트
16 라운드

④ One-Time Pad(일회용 패드) 스트림 암호의 하나로, 평문과 같은 길이의 랜덤한 비트열을 XOR 하여 암호화하는 방식이다. 랜덤한 비트열은 한 번만 사용하며, 암호화를 수행할 때마다 매번 다른 키 스트림을 생성해 사용한다.

문 5. 가상화 시스템을 보호하는 방법으로 옳지 않은 것은?

① 게스트 운영체제 사용자들에게 하이퍼바이저에 접근하는 관리권한을 부여해야 한다.
② 원격 감독 기능을 사용할 때에는 적절한 인증과 암호화 메커니즘을 사용해야 한다.
③ 게스트 운영체제와 응용프로그램을 보호하는 것 외에도 가상화 환경과 하이퍼바이저도 보호해야 한다.
④ 하이퍼바이저가 게스트의 활동을 투명하게 감시해야 한다.

답 ①

가상화란 물리적 요소와 위치를 추상화하는 것으로, 서버, 애플리케이션 등의 IT 리소스를 물리적 디바이스에서 분리해 논리적 리소스로 제공하는 것이다. 가상화를 통해 하나의 컴퓨터에서 동시에 1 개 이상의 운영체체를 가동시킬 수 있고, 이를 통해 컴퓨터 자원의 효율성을 향상시키고, 보안을 강화할 수 있다.

하이퍼바이저(hypervisor)는 가상화를 구현하기 위한 논리적 플랫폼(platforM)을 의미한다. 가상화 머신 모니터(virtual machine monitor, VMM)이라고도 한다.

① 하이퍼바이저의 역할은 높은 수준의 관리 및 모니터링 도구에 대한 인터페이스를 제공하고, OS 간 서로를 방해하지 못하도록 VM 에 대한 자원 및 메모리 할당 등을 처리하는 것이다. 따라서 관리자만이 하이퍼바이저에 접근할 수 있어야 한다.

문 6. 정보시스템을 보호하기 위한 미국의 정보보호관리체계로 적합한 것은?

① PIPL
② FISMA
③ JIPDEC
④ NICST

답 ②

(생전 처음 볼 법한 용어들이 나왔다...)

② FISMA (Federal Information Security Modernization Act, 미국 연방 정보보안 관리법)는 정보시스템에 대한 기관의 정보보호 활동에 관한 법이다.

<오답 체크> ① PIPL(Personal Information Protection Level, 개인정보 보호 인증)은 개인정보 처리기관의 개인정보보호 조치와 활동에 대한 인증으로, 국내 인증제도이다.
한국정보화진흥원(KISA)이 인증기관 역할을 한다.

③ JIPDEC(Japan Information Processing Development Center, 일본 정보처리 개발협회) 일본의 표준화 주무 관청인 공업기술원의 위촉에 따라서 정보 처리 관련 일본 공업 규격(JIS) 원안을 작성하고 표준화 조사 연구를 수행하는 단체이다.
일본의 ISMS(정보보호 관리체계) 인정기관이며, 개인정보보호 마크 제도(JIPDEC PrivacyMark)의 인증기관이다.

④ NICST 는 대만의 국가정보통신 안전회의 조직으로, 대만의 ISMS 인증 및 취득을 관리한다.

문 7. 솔라리스 10 에서 FTP 파일전송 시 발생되는 /var/log/xferlog 기록 내용에 대한 설명으로 옳지 않은 것은?

```
                                  ㉠
Thu Feb 2 16:41:30 2017 1 192.168.10.1 2870

        ㉡      ㉢              ㉣
/tmp/12-ftp.bmp b _ o r wish ftp 0 * c 2870 0
```

① ㉠ - 응답 포트 번호
② ㉡ - 전송된 파일의 이름
③ ㉢ - 바이너리 파일 전송
④ ㉣ - 인증 서버를 사용하지 않음

답 ①

① ㉠ 2870 은 파일의 크기를 나타낸다.

<오답 체크>

Thu Feb 2 16:41:30 2017
파일을 전송한 시간

1
전송 소요 시간

192.168.10.1
전송한 호스트 네임

2870
파일의 크기

/tmp/12-ftp.bmp
파일의 이름

b
전송 방식 (a: ASCII 모드, b: binary 모드)

_
특별한 행동 신호(_는 아무런 행동 없다는 의미)

o
파일 상태 (o: 파일 수신, d: 파일 삭제, i: 파일 송신)

r
사용자 접속 방식 (r: 인증된 사용자, a: 익명 사용자)

wish
접속한 사용자 이름

ftp
이용한 서비스 방식

0
인증 방식 (0: 인증 없음, 1: RFC 931 인증)

*
인증된 사용자 이름(*는 인증 이용 불가 의미)

c
전송 완료 여부(c: 전송 완료, i: 불완전한 전송)

2870

0

문 8. 생체인식에 대한 특징으로 옳지 않은 것은?

① 생체인식은 사람의 생체적 특징과 행동적 특징을 통한 보편성, 유일성, 영속성, 획득성을 요구한다.
② FRR 은 인증 권한이 있는 사람이 인증을 시도했을 때 인증에 실패하는 비율을 말한다.
③ CER 은 잘못된 거부율과 잘못된 허용 비율 곡선의 교차점을 말한다.
④ 엄격한 보안이 요구되는 경우는 FAR 을 높이고, FRR 을 낮춤 으로써 보안성을 향상시킬 수 있다.

답 ④

④ 엄격한 보안을 위해서는 생체인식 시스템의 민감도를 높여야 하며, 따라서 FRR(오거부율)이 다소 높더라도, FAR(오인식률)을 낮추는 것이 중요하다.

<오답 체크> ① 생체인식이 지녀야 할 특성
1) 보편성: 누구나 가지고 있어야 한다.
2) 유일성: 개인마다 달라야 한다.
3) 영속성: 언제나 일정하고 변하지 않아야 한다.
4) 획득성: 쉽게 얻을 수 있어야 한다.
5) 친화성: 개인 거부감이 없어야 한다.
6) 보안성: 위조가 어려워야 한다.

② FRR(False Rejection Rate, 오거부율): 정당한 권한이 있는 사용자가 인증에 실패할 확률
FAR(False Acceptance Rate, 오인식률): 권한이 없는 사용자가 인증에 성공할 확률

③ CER(Crossover Error Rate): FRR 과 FAR 의 교차점

문 9. 정보보호관리체계(ISMS)의 정보보호 관리과정에 대한 설명으로 옳지 않은 것은?

① 정보보호정책은 조직이 수행하는 모든 정보보호활동의 근거를 포함할 수 있도록 수립하고, 조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함할 수 있도록 범위를 설정한다.
② 최고경영자는 조직의 규모, 업무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 최고책임자, 실무조직 등 정보보호조직을 구성하고 정보보호 관리체계 운영 활동을 수행하는 데 필요한 자원을 확보하여야 한다.
③ 위험관리 방법 및 계획에 따라 정보보호 일부 영역에 대한 위험 식별 및 평가를 2 년에 1 회 수행하고 그 결과에 따라 조직에서 수용 가능한 위험수준도 설정하여 관리하여야 한다.
④ 정보보호대책 이행 계획에 따라 보호대책을 구현하고 경영진은 이행 결과의 정확성 및 효과성 여부를 확인하여 구현된 정보 보호대책을 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.

답 ③

③ 2 년에 1 회(X) -> 매년(○)
위험관리 방법 및 계획 수립
ㅇ 위험관리 방법 및 절차에 따라 매년 위험관리계획을 수립하고 이행하여야 하며 계획에는 다음과 같은 내용을 포함하여야 한다.
- 위험관리 대상 : 정보보호 관리체계 인증범위 내 핵심자산 및 서비스를 누락 없이 포함
- 위험관리 수행인력 : 위험관리 방법, 조직의 업무 및 시스템에 대한 전문성을 갖춘 인력과 관련 부서 실무책임자가 참여 (위험관리 전문가, 정보보호관리자, IT 실무 책임자, 현업부서 실무 책임자 등)
- 위험관리 기간 등

문 10. ISO/IEC JTC 1 의 SC 27 에서 담당하는 범위가 아닌 것은?

① Management of information and ICT security
② Cards and personal identification
③ Security evaluation criteria and methodology
④ Security requirements capture methodology

답 ②

(그냥 영문 위키 긁어서 섞은 문제)
② Cards and personal identification 은 SC 17 의 담당 범위다.

ISO/IEC JTC1 (Joint Technical Committee)은 ISO 와 IEC 가 정보기술 분야의 표준을 공동 제정하기 위해 설립한 표준화 기관이다.
SC 6 - RFID 미들웨어 등
SC 17 - 비접촉형 식별용 IC 카드 표준
SC 22 - 프로그래밍 언어 호환성/이식성
SC 25 - 정보기기의 상호 접속을 위한 표준 정의
SC 27 - 정보보호 기술
SC 29 - 음성, 영상, 멀티미디어 하이퍼미디어 정보의 부호화
SC 31 - 바코드 및 RFID 표준화 추진
SC 37 - 응용과 시스템 사이의 상호운용성과 데이터 교환을 지원하기 위한, 인간에 관련된 일반적인 생체인식 기술의 표준화`

※ SC 27 의 담당 범위
- Security requirements capture methodology
- Management of information and ICT security; in particular information security management systems, security processes, security controls and services
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components
- Security aspects of identity management, biometrics and privacy
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems
- Security evaluation criteria and methodology

문 11. 해킹 수단과 그 공격 방법에 대한 설명으로 옳지 않은 것은?

① Ransomware - 파일을 암호화한 후 복호화를 조건으로 금전을 요구함
② Rootkit - 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴
③ SQL Injection - 데이터베이스에 질의어를 변조하여 공격함
④ Cross-site Scripting - 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함

답 ②

② 버퍼 오버플로우에 대한 설명이다.
루트킷(Rootkit)은 해커들이 컴퓨터나 또는 네트웍에 침입한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득하는데 사용하는 도구의 모음이다.
<오답 체크> ① **랜섬웨어**(Ransomware)
인질의 몸값을 뜻하는 ransom 과 제품을 뜻하는 ware 의 합성어컴퓨터에 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.
③ **SQL 삽입**(SQL 인젝션, SQL injection)은 클라이언트의 입력값(SQL 질의어)을 조작하여 서버의 데이터베이스를 공격하는 것이다.
④ **크로스 사이트 스크립팅**(XSS, Cross-site Scripting)
웹 사이트에 악성 스크립트를 삽입한 뒤, 다른 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.

문 12. 암호모듈을 KS X ISO/IEC 19790 에 따라 검증하고 암호모듈의 안전성을 보증하는 국내 제도는?

① KCMVP
② TCSEC
③ ITSEC
④ METI

답 ①

① KCMVP(Korea Cryptographic Module Validation Program, 한국 암호화모듈 검증 제도)
<오답 체크> ② TCSEC(Trusted Computer System Evaluation Criteria) 미국의 정보보호 시스템 평가 제도
③ ITSEC(Information Technology Security Evaluation Criteria) 유럽의 정보보호 시스템 평가 제도
④ METI(Ministry of Economy, Trade and Industry, 일본 경제산업성)
2016 년 사물인터넷(IoT)에 대한 보안 지침을 제정했다.

문 13. 사용자가 무선랜 보안을 위하여 취할 수 있는 방법이 아닌 것은?

① MAC 주소 필터링의 적용
② SSID(Service Set Identifier) 브로드캐스팅의 금지
③ 무선 장비 관련 패스워드의 주기적인 변경
④ WPA, WPA2, WEP 중에서 가장 안전한 보안 방법인 WEP 를 이용한 무선랜의 통신 보호

답 ④

④ WEP 는 초창기의 무선랜 보안 프로토콜이며, 현재는 많은 취약점이 드러나 잘 사용하지 않는 방식이다.

WEP 방식(WiFi Equivalent Pravicy)
암호화를 위해 RC4 사용하며(암호키 계속 사용), 암호화와 인증에 동일한 키를 사용
WPA 방식(WiFi Protected Access)
RC4-TKIP 를 통한 암호화(암호키 주기적인 변경), EAP 를 통한 사용자 인증
48 비트 길이의 초기벡터(IV) 사용
WPA2 방식
AES-CCMP 사용, EAP 를 통한 사용자 인증

문 14. ISO 27001 의 통제 영역별 주요 내용에 대한 설명으로 옳지 않은 것은?

① 자산 관리 영역은 자산을 파악하고, 이를 적절히 분류하고 보호하는 데 활용하는 것이다.
② 사업 연속성 관리 영역은 형법과 민법, 법령, 규정 또는 계약 의무 및 보안 요구 사항에 대한 위반을 피하기 위한 기준을 제시한 것이다.
③ 정보시스템 획득, 개발, 유지 보수 영역은 정보시스템 내에 보안이 수립되어 있음을 보장하기 위한 것이다.
④ 통신 및 운영 관리 영역은 정보처리 설비의 정확하고 안전한 운영을 보장하기 위한 내용을 포함하고 있다.

답 ②

② 법과 규정을 준수하고, 위반을 피하기 위한 기준을 제시한 것은 준거성(Compliance) 영역이다.
사업 연속성 관리(Business Continuity Management) 영역은 사업 활동의 방해 요소를 완화시키며, 주요 실패 및 재해의 영향으로부터 주요 사업 활동을 보호하기 위한 프로세스를 검토하는 영역이다.

문 15. 정수의 소인수분해를 기반으로 한 RSA 암호 알고리즘에서 공개키 (e, n) = (7, 33)을 이용하여 생성된 암호문 C 값이 7 일 때, 이를 다시 복호화한다면 원문 메시지 값은?

① 11
② 13
③ 17
④ 19

답 ②

(사실상 이 문제는 1 분 내에 풀기가 어렵다. 전형적인 시간 깎아먹기 문제다.)
복호화를 하기 위해서는 먼저 개인키를 구해야 한다.
개인키 (d, n)에서 'e × d mod Φ(n) = 1'의 식을 만족하는 d 를 구하기 위해서는 먼저 Φ(n)을 구해야 한다..
n 은 두 소수 p 와 q 의 곱으로 나타낸다.
n 은 33 이므로, p = 3, q = 11 로 소인수분해가 된다.
Φ(n) = (p – 1) × (q – 1) = 2 × 10 = 20
d 는 e × d mod Φ(n) = 1 을 만족해야 하므로, 7d 가 20 의 배수보다 1 커야 한다.
20 × 1 + 1 = 21 (7 의 배수)
21 은 7 × 3 이므로 개인키 (d, n) = (3, 33)이 된다.

복호화 공식은
평문 = $\left(\text{암호문}\right)^{d} \bmod n$ 이므로,
$7^3 \bmod 33$ 을 계산하면 원문이 나온다.
$7^3 \bmod 33$ 를 모듈러 곱셈 법칙을 이용해 구해보겠다.
$7^2 \bmod 33 = 49 \bmod 33 = 16$
$7^3 \bmod 33 = (7^1 \bmod 33)(7^2 \bmod 33) \bmod 33$
$= 7 * 16 \bmod 33 = 112 \bmod 33 = 13$
따라서 원문은 13 이 나온다.

※ RSA 알고리즘 공개키와 개인키 생성 순서
◦ 단계 1: 두 소수 p, q 를 선정한다.
◦ 단계 2: n = p × q 를 계산한다.
◦ 단계 3: Φ(n) = (p – 1) × (q – 1)을 계산한다.
(단, Φ(n)은 오일러의 Totient 함수이다.)
◦ 단계 4: Φ(n)과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
◦ 단계 5: e × d mod Φ(n) = 1 의 관계를 갖는 d 를 계산한다. (단, mod 는 나머지를 구하는 연산자이다.)
◦ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

암호문 = $\left(\text{평문}\right)^{e} \bmod n$
평문 = $\left(\text{암호문}\right)^{d} \bmod n$

문 16. 리눅스 파일의 접근 제어에 대한 설명으로 옳지 않은 것은?

① 모든 종류의 파일은 inode 라는 파일 관리 수단으로 운영체제에 의해서 관리된다.
② passwd 명령으로 패스워드를 설정하면, 패스워드에 대한 암호화나 해시된 값이 /etc/passwd 에 저장된다.
③ superuser 계정은 시스템의 모든 권한이 가능하므로 외부에 노출되지 않도록 주의해야 한다.
④ 어떤 권한을 가지고 있는가에 대한 UID, GID 가 별도로 존재 한다.

답 ②

② 패스워드가 암호화되거나 해시값으로 저장되는 파일은 /etc/shadow 파일이다.
/etc/passwd 에는 사용자의 기본 정보가 평문 형태로 저장된다.

<오답 체크> ① 아이노드(Inode)는 파일시스템에 관한 정보를 담고 있다.

④ UID(User ID): 사용자 구분 식별자
GID(Group ID): 사용자가 속한 그룹의 식별자
UID 와 GID 를 통해 권한이 있는 사용자인지 없는 사용자인지 식별한다.

문 17. 블루투스에 대한 설명으로 옳지 않은 것은?

① 페어링 과정은 한 장치가 그 지역에 있는 다른 장치들을 찾아 BD_ADDR 이나 논리적 이름에 근거해 파트너가 될 장치를 선택하는 것이다.
② 장치 간 종류를 식별하기 위해서 SDP(Service Discovery Protocol)를 보내고 받는다.
③ 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격은 BlueBug 이다.
④ OPP(OBEX Push Profile)는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발되었다.

답 ③

③ 임의의 파일에 접근하는 공격은 블루스나프다.

- 블루 프린팅(Blueprinting)
  블루투스 공격장치의 검색활동을 의미한다.
  각 블루투스 장치는 MAC 주소와 유사하게 6 바이트의 고유주소가 있다. 블루투스 장치는 장치간 종류를 식별하기 위해 SDP(서비스 발견 프로토콜)을 보내고 받는다. 그리고 이 SDP 를 이용해 공격자는 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.
- 블루 스나프(BlueSnarf)
  블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.
  공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP 기능을 사용하여 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근할 수 있다.
- 블루 버그(BlueBug)
  블루버그는 블루투스 장비간 취약한 연결 관리를 악용한 공격이다. 공격장치와 공격대상 장치를 연결하여 공격대상 장치에서 전화 걸기, SMS 보내기 등 임의의 동작을 실행하는 공격이다.

<오답 체크> ① 페어링(pairing)은 무선으로 연결하기 위해 블루투스 장치에 정보를 수동으로 등록하는 데 필요한 절차를 말한다.

② SDP(Service Discovery Protocol, 서비스 발견 프로토콜)는 블루투스 디바이스가 제공하는 서비스를 찾고 응답하기 위한 프로토콜이다.

④ OBEX(Object Exchange)는 원래 적외선 링크를 통해 데이터 객체를 교환하기 위해 개발되었으며, 연락처 정보와 일정 정보 등과 같은 객체들을 쉽게 교환할 수 있게 해주는 프로토콜 세트를 가리킨다.

문 18. 방화벽의 보안 기능에 대한 설명으로 옳은 것은?

① 방화벽은 내부의 불만이 있는 사용자 또는 외부 공격자와 무의식적으로 협력하는 사용자를 완벽히 차단할 수 있다.
② 방화벽을 설치하게 되면 외부로부터의 모든 무선랜 통신을 안전하게 보호할 수 있다.
③ 랩톱, PDA 와 같은 이동형 저장장치가 감염되는 경우에도 방화벽을 설치하여 내부 네트워크를 안전하게 보호할 수 있다.
④ 내부 보안 정책을 만족하는 트래픽만이 방화벽을 통과할 수 있다.

답 ④

④ 패킷의 출발지 및 목적지 IP 주소, 서비스 포트 번호, TCP 접속의 Syn 패킷 등을 이용하여 패킷 필터링 규칙을 설정하여 규칙에 맞는 패킷만 방화벽을 통과할 수 있다.

<오답 체크> ①② 방화벽은 외부 네트워크와 내부 네트워크 사이에서 트래픽을 제어한다. 따라서 방화벽을 통과하지 않는 트래픽에 대해서는 전혀 대응할 수 없다.
무선이나 공중 전화망을 통한 네트워크 접속이 방화벽을 거치지 않도록 허용되어 있거나, 내부자에 의한 악의적인 행위에 대해서는 완전한 무방비 상태가 된다.
또한 허용된 서비스에 대해서 허용된 패킷 안의 데이터를 변조하여 공격하는 기법에 무방비 상태가 된다.
③ 랩톱, PDA 와 같은 이동형 저장장치가 감염되는 경우 같은 방화벽 내부에 문제가 발생한 경우에는 대처할 수 없다.

문 19. 재해복구 시스템의 복구 수준별 유형에 대한 설명으로 옳지 않은 것은?

① Mirror Site - 주 센터와 동일한 수준의 정보기술 자원(하드웨어, 소프트웨어, 기타 부대 장비 등)을 원격지에 구축하여 모두 액티브 상태에서 실시간으로 동시에 서비스하는 방식
② Hot Site - 주 센터와 동일한 수준의 정보기술 자원을 대기 상태(standby)로 원격지에 구축하여 동기적 혹은 비동기적 미러링을 통해 데이터의 최신을 유지하고 있다가 주 센터 재해 시 액티브로 전환하여 서비스하는 방식
③ Down Site - 웹 애플리케이션 서비스 등 데이터의 업데이트 빈도가 높은 정보시스템을 액티브로 전환하여 서비스하는 방식
④ Cold Site - 기계실, 전원 시설, 통신 설비, 공조 시설, 온도 조절 시스템 등을 갖추어 놓고, 주 센터 재해 시 정보기술 자원을 설치하여 서비스하는 방식

답 ③

③ 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하는 방식은 웜 사이트(Warm Site)이다.

- Mirror Site(미러 사이트)
  원본 시스템과 동일한 데이터를 실시간으로 처리하여 **동시에 운영**되는 백업 사이트이다
- Hot Site(핫 사이트)
  원본 시스템과 동일한 장비와 데이터를 갖춘 백업 사이트지만, 평소엔 운영하지 않고 대기상태(Standby)로 둔다. 원본 시스템과 항상 동일한 데이터를 유지하기 때문에 백업은 실시간
- Warm Site(웜 사이트)
  핫 사이트와 콜드 사이트의 중간 단계로, 원본 시스템의 장비 일부를 백업 사이트에 설치하여 주요 업무에 대한 복구를 지원한다.
  하드웨어가 이미 연결이 되어 있으며, 직접 백업본을 갖출 수 있으나 완전하지 못할 수도 있다.
- Cold Site(콜드 사이트)
  평소에는 시스템을 사용할 수 있는 전기, 통신, 온도조절 시스템만 갖춰놓은 상태로, 재해 발생시 하드웨어와 소프트웨어를 설치하여 가동한다.
  백업 사이트 가운데 가장 값이 저렴하며, 데이터와 정보의 백업된 복사본을 거의 보유하고 있지 않다.

문 20. 정보보안 관리 규격 중 IT 보호 및 통제부문의 모범적인 업무 수행 방법에 적용 가능한 ISACA (Information Systems Audit and Control Association) 에서 개발된 프레임워크는?

① COBIT
② BS 7799
③ BSI
④ HIPAA

답 ①

① COBIT 은 ISACA 에서 개발한 프레임워크로, IT 프로세스와 이들의 관리를 위한 프레임워크이며 기존의 다양한 표준과 실무를 참조하고 포괄하는 지식 베이스라고 할 수 있다. COBIT 은 정의된 표준이라기보다는 실무적인 관리도구이며 지침, 구현 도구, 전 세계에서 수집되는 케이스 스터디 등으로 지원되고 있다.

※ 프레임워크(framework)란 소프트웨어의 구체적인 부분에 해당하는 설계와 구현을 재사용이 가능하게끔 일련의 협업화된 형태로 클래스들을 제공하는 것이다.

<오답 체크> ②③ BS7799 란 영국 정부 기관인 UKAS(United Kingdom Accreditation Service)가 정보보안에 대한 인증이 필요한 조직들의 요청에 의해 마련한 정보보호 관리체계 인증 규격으로, BSI Group(영국왕립표준협회)를 비롯한 7 개의 공식 인증기관의 평가와 심사를 거쳐 규격기준을 만족한 업체들에게 부여하는 인증이다.

④ HIPAA(Health Insurance Portability and Accountability Act)는 1995 년 미국에서 개인의 전자 의료 정보를 안전하게 지키기 위한 특별 보호 조항을 제정한 미국의 보안 규정이다.