2019-국가직-정보보호론-라형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

1. 쿠키(Cookie)에 대한 설명으로 옳지 않은 것은?
① 쿠키는 웹사이트를 편리하게 이용하기 위한 목적으로 만들어졌으며, 많은 웹사이트가 쿠키를 이용하여 사용자의 정보를 수집하고 있다.
② 쿠키는 실행파일로서 스스로 디렉터리를 읽거나 파일을 지우는 기능을 수행한다.
③ 쿠키에 포함되는 내용은 웹 응용프로그램 개발자가 정할 수 있다.
④ 쿠키 저장 시 타인이 임의로 쿠키를 읽어 들일 수 없도록 도메인과 경로 지정에 유의해야 한다.
정답 체크 :
(2) 쿠키는 실행 파일이 아니라 텍스트 파일이므로 디렉터리를 읽거나 파일을 지울 수 없다.
오답 체크 :
(1) 고객이 특정 홈페이지를 접속할 때 생성되는 정보를 담은 임시 파일로 크기는 4KB 이하로 작다. 쿠키는 애초 인터넷 사용자들의 홈페이지 접속을 돕기 위해 만들어졌다. 특정 사이트를 처음 방문하면 아이디와 비밀번호를 기록한 쿠키가 만들어지고 다음에 접속했을 때 별도 절차 없이 사이트에 빠르게 연결할 수 있다.
(3) 개발자가 자바스크립트 등을 이용하여 쿠키 내용을 변경할 수 있다.
(4) 다른 사람(공격자 등)가 사용자의 쿠키를 얻을 수 없도록 도메인과 경로 지정에 유의해야 한다.

2. 악성프로그램에 대한 설명으로 옳지 않은 것은?
① Bot - 인간의 행동을 흉내 내는 프로그램으로 DDoS 공격을 수행한다.
② Spyware - 사용자 동의 없이 설치되어 정보를 수집하고 전송하는 악성 소프트웨어로서 금융정보, 신상정보, 암호 등을 비롯한 각종 정보를 수집한다.
③ Netbus - 소프트웨어를 실행하거나 설치 후 자동적으로 광고를 표시하는 프로그램이다.
④ Keylogging - 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채 기록하는 행위이다.
정답 체크 :
(3) Netbus : 해당 설명은 애드웨어이고, Netbus는 네트워크를 통해 Microsoft Windows 컴퓨터 시스템을 원격으로 제어하기 위한 소프트웨어 프로그램이다. 1998년에 만들어졌으며 백도어로 사용될 가능성에 대해 매우 논란의 대상이되었다(실제 백도어로 사용됨). 1998년 3월에 출시되었다.
오답 체크 :
(1) Bot : 분산 서비스 거부 공격(DDoS)에 사용되는 악성코드를 봇(Bot)이라고 한다.
(2) Spyware : 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어로, 신용 카드와 같은 금융 정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집한다.
(4) Keylogging : 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 행위를 말한다. 하드웨어, 소프트웨어를 활용한 방법에서부터 전자적, 음향기술을 활용한 기법까지 다

양한 키로깅 방법이 존재한다.

3. 정보보호 서비스에 대한 설명으로 옳지 않은 것은?
① Availability - 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 한다.
② Integrity - 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호한다.
③ Confidentiality - 온오프라인 환경에서 인가되지 않은 상대방에게 저장 및 전송되는 중요정보의 노출을 방지한다.
④ Authentication - 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용한다.
정답 체크 :
(1) Availability(가용성) : 해당 설명은 부인방지(Nonrepudiation)이고, 가용성은 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.
오답 체크 :
(2) Integrity(무결성) : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(3) Confidentiality(기밀성) : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.
(4) Authentication(인증) : 상대방의 신원을 확인시켜 준다. 사용자 인증(시스템 접근 통제)과 데이터 출처 인증(MAC)이 있다.

4. 다음에서 설명하는 스캔방법은?

공격자가 모든 플래그가 세트되지 않은 TCP 패킷을 보내고, 대상 호스트는 해당 포트가 닫혀 있을 경우 RST 패킷을 보내고, 열려 있을 경우 응답을 하지 않는다.

① TCP Half Open 스캔
② NULL 스캔
③ FIN 패킷을 이용한 스캔
④ 시간차를 이용한 스캔
정답 체크 :
(2) NULL 스캔 : 공격자가 모든 플래그가 세트되지 않은 TCP 패킷을 보낸다.
오답 체크 :
(1) TCP half open 스캔 : 처음 SYN 패킷을 보낸다. 열려 있는 경우에는 서버로부터 SYN+RST 패킷을 받은 후 공격자는 무응답한다. 닫혀 있는 경우에는 서버로부터 SYN+ACK 패킷을 받은 후 공격자가 RST 패킷을 보내 연결을 끊는다.
(3) FIN 패킷을 이용한 스캔 : 공격자가 FIN 플래그를 세트한 TCP 패킷을 보낸다.
(4) 시간차를 이용한 스캔 : 서버의 스캔 공격 탐지에 대한 대응 방법이다. 아주 짧은 시간 동안 많은 패킷을 보내는 방법과, 아주 긴시간 동안 패킷을 보내는 방법이다. 아주 짧은 시간 동안 많은 패킷을 보내는 방법은 방화벽과 IDS의 처리 용량의 한계를 넘기고, 아주 긴 시간 동안 걸쳐서 패킷을 보내는 방법은 방화벽과 IDS가 패킷 패턴에 대한 정보를 얻기 힘들게 만

든다.
Tip! : 이외에도 TCP Xmas 스캔은 공격자가 모든 플래그를 세트한 TCP 패킷을 보낸다.

5. SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 옳지 않은 것은?
① ChangeCipherSpec - Handshake 프로토콜에 의해 협상된 암호 규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.
② Handshake - 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.
③ Alert - 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.
④ Record - 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택 적으로 압축된다.
정답 체크 :
(1) Alert : 해당 설명은 VPN에서 사용하는 IKE 프로토콜에 대한 설명이고, Alert는 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.
오답 체크 :
(1) ChangeCipherSpec : 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.
(2) Handshake : 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다. 인증서를 이용한 인증을 수행한다.
(4) Record : 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.
Tip! : 해당 내용을 그림으로 나타내면 다음과 같다.

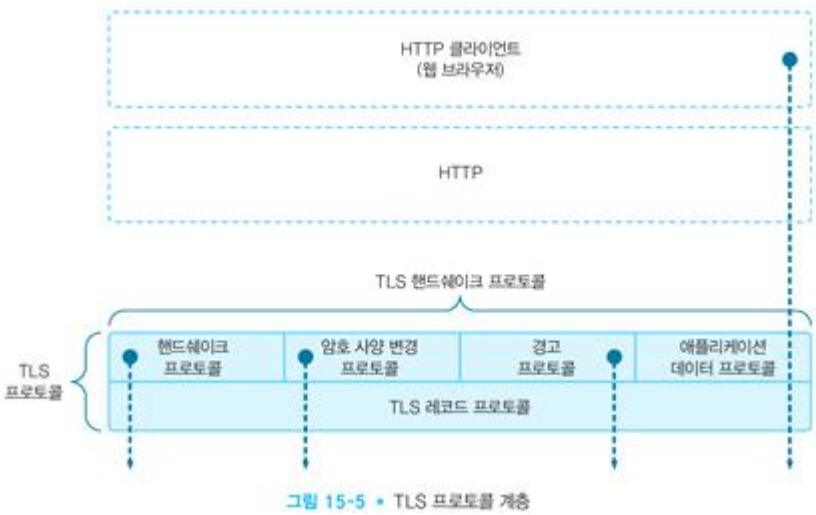


그림 15-5 • TLS 프로토콜 계층

6. 블록체인에 대한 설명으로 옳지 않은 것은?
① 하나의 블록은 트랜잭션의 집합과 헤더(header)로 이루어져 있다.

② 앞 블록의 내용을 변경하면 뒤에 이어지는 블록은 변경할 필요가 없다.
③ 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다.
④ 금융 분야에만 국한되지 않고 분산원장으로 각 분야에 응용할 수 있다.
정답 체크 :
(2) 이어지는 블록은 앞 블록의 내용을 포함하고 있으므로 앞 블록의 내용을 변경하면 뒤에 이어지는 블록을 변경해야 한다.
오답 체크 :
(1) 하나의 블록은 그림에서 보는 바와 같이 집합과 헤더로 이루어져 있다.
(3) 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다. 그러므로 (3)번으로 (2)번이 답임을 유추할 수 있다.
(4) 분산원장 (공유원장, 또는 분산원장기술) : 복제, 공유 또는 동기화된 디지털 데이터에 대한 합의 기술이다. 이때 데이타들은 지리적으로 여러 사이트나, 여러 국가 또는 여러 기관에 분산되어 있게 된다. 즉 중앙집중적인 관리자나 중앙집중의 데이터 저장소가 존재하지 않고 기능이 동작하게 된다.
Tip! : 해당 내용을 그림으로 나타내면 다음과 같다.

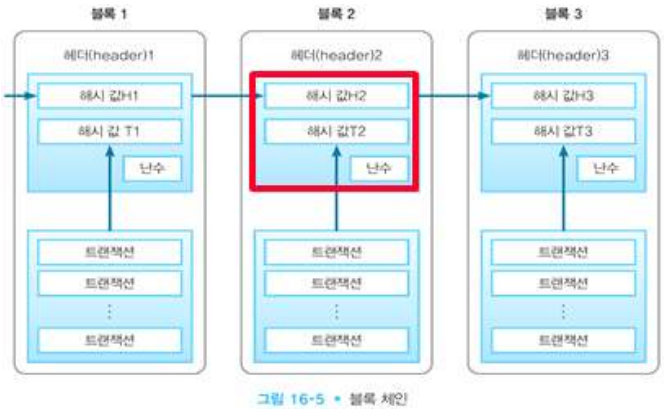


그림 16-5 • 블록 체인

7. 다음의 결과에 대한 명령어로 옳은 것은?

```
Thu Feb 7 20:33:56 20191 198.188.2.2 861486 /tmp/12-67-ftp1.bmp b_o r freeexam ftp 0 * c 861486 0
```

① cat /var/adm/messages
② cat /var/log/xferlog
③ cat /var/adm/loginlog
④ cat /etc/security/audit_event
정답 체크 :
(2) /var/log/xferlog : FTP 전송시 발생하는 로그는 나타낸다. 주어진 로그는 FTP 전송 시에 발생하는 로그이다.
오답 체크 :
(1) /var/adm/messages : 시스템에 전반적인 로그 기록을 나타낸다.
(3) /var/adm/loginlog : 실패한 로그인에 대한 로그를 나타낸다.
(4) /etc/security/audit_event : 일반 감사 로그를 나타낸다.

8. 다음 설명에 해당하는 DoS 공격을 옳게 짝지은 것은?

ㄱ. 공격자가 공격대상의 IP 주소로 위장하여 중계 네트워크에 다량의 ICMP Echo Request 패킷을 전송하며, 중계 네트워크에 있는 모든 호스트는 많은 양의 ICMP Echo Reply 패킷을 공격 대상으로 전송하여 목표시스템을 다운 시키는 공격 ㄴ. 공격자가 송신자 IP 주소를 존재하지 않거나 다른 시스템의 IP 주소로 위장하여 목적 시스템으로 SYN 패킷을 연속해서 보내는 공격 ㄷ. 송신자 IP 주소와 수신자 IP 주소, 송신자 포트와 수신자 포트가 동일하게 조작된 SYN 패킷을 공격 대상에 전송하는 공격

	ㄱ	ㄴ	ㄷ
①	Smurf Attack	Land Attack	SYN Flooding Attack
②	Smurf Attack	SYN Flooding Attack	Land Attack
③	SYN Flooding Attack	Smurf Attack	Land Attack
④	Land Attack	Smurf Attack	SYN Flooding Attack

정답 체크 :

(2)

(ㄱ) Smurf attack : ICMP 패킷과 네트워크에 존재하는 임의의 시스템들을 이용하여 패킷을 확장시켜서 서비스 거부 공격을 수행하는 방법이다. Ping flooding이라고도 한다.

(ㄴ) SYN Flooding attack : 존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서버의 서비스를 제공받지 못하게 하는 공격이다.

(ㄷ) Land attack : 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소값을 똑같이 만들어서 공격 대상에게 보내는 공격이다.

9. 무선 LAN 보안에 대한 설명으로 옳지 않은 것은?

① WPA-PSK는 WEP보다 훨씬 더 강화된 암호화 세션을 제공한다.

② WEP는 64비트 WEP 키가 수분 내 노출되어 보안이 매우 취약하다.

③ WPA는 EAP 인증 프로토콜(802.1x)과 WPA-PSK를 사용한다.

④ WPA2는 RC4 알고리즘을 암호화에 사용하고, 고정 암호키를 사용한다.

정답 체크 :

(4) WPA2는 AES 알고리즘을 암호화에 사용하고, 동적 암호키를 사용한다.

오답 체크 :

(1) WPA는 동적 암호키를 사용하여 고정 암호키를 사용하는 WEP보다 훨씬 더 강화된 암호화 세션을 제공한다.

(2) 64비트 WEP 키에 대해 전사 공격(brute-force attack)을 수행하면 수분 내 노출되어 보안이 매우 취약하다.

(3) WPA는 별도의 인증서버를 이용하는 EAP 프로토콜(802.1x)와 사전 공유된 비밀키를 사용하는 WPA-PSK를 사용한다.

Tip! : 해당 내용을 테이블로 정리하면 다음과 같다.

〈표 6-9〉 무선랜 보안 표준 비교

구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access 2)
개요	1997년 제정(2003년 삭제)	WEP 방식 보완 (Wi-Fi Alliance)	IEEE 802.11i(2004년) 준수
인증	사전 공유된 비밀키 사용 (64비트, 128비트)	• 별도의 인증서버를 이용하는 EAP 인증 프로토콜(802.1x) • WPA-PSK(사전 공유된 비밀키)	• 별도의 인증서버를 이용하는 EAP 인증 프로토콜(802.1x) • WPA-PSK(사전 공유된 비밀키)
암호화	• 고정 암호키 사용(인증키와 동일) • RC4 알고리즘사용	• 암호키 동적 변경(TKIP) • RC4 알고리즘 사용	• 암호키 동적 변경(CCMP) • AES 등 강력한 블록 암호 알고리즘 사용
보안성	• 64비트 WEP 키는 수분 내 노출 • 취약하여 널리 쓰이지 않음	• WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	• 가장 강력한 보안 가능 제공

10. 사용자 A가 사용자 B에게 해시함수를 이용하여 인증, 전자서명, 기밀성, 무결성이 모두 보장되는 통신을 할 때 구성해야 하는 함수로 옳은 것은?

K : 사용자 A와 B가 공유하고 있는 비밀키
KS_a : 사용자 A의 개인키
KP_a : 사용자 A의 공개키
H : 해시함수
E : 암호화
M : 메시지
|| : 두 메시지의 연결

① $E_K[M \,||\, H(M)]$
② $M \,||\, E_K[H(M)]$
③ $M \,||\, E_{KSa}[H(M)]$
④ $E_K[M \,||\, E_{KSa}[H(M)]]$

정답 체크 :
(4) 인증, 전자서명(부인방지), 무결성, 기밀성 제공 : 메시지와 서명된 메시지의 해시값을 암호화한다.
오답 체크 :
(1) 무결성, 기밀성 제공 : 메시지와 메시지의 해시값을 암호화한다.
(2) 무결성 제공 : 해시값을 암호화한다(불필요하다).
(3) 인증, 전자서명(부인방지), 무결성 제공 : 메시지의 해시값에 서명한다.

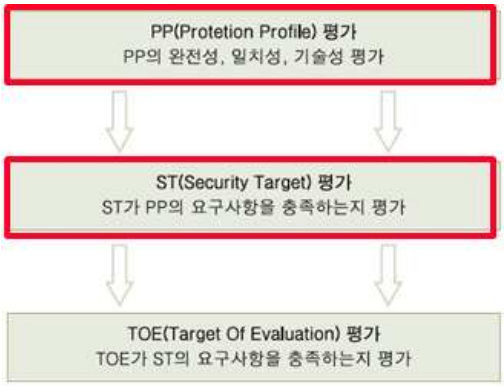
11. 다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은?
① SEED 알고리즘
② RSA 알고리즘
③ DES 알고리즘
④ AES 알고리즘
정답 체크 :
(2) : 비대칭키(공개키)에는 RSA, Rabin, Elgamal, ECC 등이 있다.
오답 체크 :

(1), (3), (4) : 대칭키에는 DES, 3-DES, AES, Blowfish, IDEA, RC6, SEED, ARIA 등이 있다.

12. 정보보안 관련 용어에 대한 설명으로 옳지 않은 것은?
① 부인방지(Non-repudiation) - 사용자가 행한 행위 또는 작업을 부인하지 못하는 것이다.
② 최소 권한(Least Privilege) - 계정이 수행해야 하는 작업에 필요한 최소한의 권한만 부여한다.
③ 키 위탁(Key Escrow) - 암호화 키가 분실된 경우를 대비하여 키를 보관하는 형태를 의미한다.
④ 차분 공격(Differential Attack) - 대용량 해쉬 테이블을 이용하여 충분히 작은 크기로 줄여 크랙킹하는 방법이다.
정답 체크 :
(4) 차분 공격 : 해당 설명은 레인보우 테이블이고, 차분 공격은 평문의 일부를 변경할 때 암호문이 어떻게 변화하는지 관찰하여 조사하는 암호 해독법이다.
오답 체크 :
(1) 부인방지 : 송신부인방지(어떤 메시지가 송신되었을 때 수신자는 그 메시지가 실제로 송신자라고 주장하는 주체에 의해 송신되었음을 확인한다). 수신부인방지(어떤 메시지가 수신되었을 때 송신자는 그 메시지가 실제로 수신자라고 주장하는 주체에 의해 수신되었음을 확인한다).
(2) 최소권한 : 수행해야 하는 작업에 딱 필요한 권한만큼만 사용자 혹은 프로세스에게 부여하는 것을 의미한다.
(3) 키 위탁 : 특수 상황(키가 분실된 경우 등)에서 해당 키에 사용하기 위해 암호화에 사용된 키를 보관하는 것을 의미한다.

13. 공통평가기준은 IT 제품이나 특정 사이트의 정보시스템의 보안성을 평가하는 기준이다. '보안기능요구사항'과 '보증요구사항'을 나타내는 보호프로파일(PP), 보호목표명세서(ST)에 대한 설명으로 옳지 않은 것은?
① 보호프로파일은 오퍼레이션이 완료되지 않을 수 있으나, 보호목표명세서는 모든 오퍼레이션이 완료되어야 한다.
② 보호프로파일은 여러 시스템·제품을 한 개 유형의 보호프로파일로 수용할 수 있으나, 보호목표명세서는 한 개의 시스템·제품을 한 개의 보호목표명세서로 수용해야 한다.
③ 보호프로파일은 보호목표명세서를 수용할 수 있고, 보호목표 명세서는 보호프로파일을 수용할 수 있다.
④ 보호프로파일은 구현에 독립적이고, 보호목표명세서는 구현에 종속적이다.
정답 체크 :
(3) 보호목표명세서가 보호프로파일의 요구사항을 충족하는지 평가하기 때문에 보호목표명세서는 보호프로파일을 수용할 수 있지만, 보호프로파일은 보호목표명세서를 수용할 수 없다.
오답 체크 :
(1) 보호프로파일은 사용자 또는 개발자의 요구사항들이므로 오퍼레이션이 완료되지 않을 수 있지만, 보호목표명세서는 제품 평가를 위한 상세 기능이므로 모든 오퍼레이션이 완료되어야 한다.

(2) 보호프로파일은 사용자 또는 개발자의 요구사항들이므로 여러 시스템•제품을 한 개 유형의 보호프로파일로 수용할 수 있으나, 보호목표명세서는 제품 평가를 위한 상세 기능이므로 한 개의 시스템•제품을 한 개의 보호목표명세서로 수용해야 한다.
(4) 보호프로파일은 사용자 또는 개발자의 요구사항들을 정의, 기술적인 구현 가능성을 고려하지 않는다(구현에 독립적). 그리고 보호목표명세서는 개발자가 작성하며 제품 평가를 위한 상세 기능을 정의, 기술적 구현 가능성 고려한다(구현에 종속적).
Tip! : 해당 내용을 그림으로 나타내면 다음과 같다.



14. 방화벽 구축 시 내부 네트워크의 구조를 외부에 노출하지 않는 방법으로 적절한 것은?
① Network Address Translation
② System Active Request
③ Timestamp Request
④ Fragmentation Offset
정답 체크 :
(1) NAT : 방화벽 구축 시 내부 네트워크와 외부 네트워크를 분리시킨 후 내부 네트워크에 존재하는 사용자(private network)와 공개용 서버(public network)를 위해 가상 Network IP 주소를 부여한다.
오답 체크 :
(2) System Active Request : 출제자가 어떤 의도로 사용 했는지 모르지만 굳이 해석하자면 (일반적으로 사용하지 않는 단어) "시스템이 현재 처리중인 요청"을 의미한다.
(3) Timestamp request : ICMP 질의 메시지, 두 시스템 사이에서 IP 데이터그램이 왕복하는데 필요한 시간(RTT)을 알아내거나,두 시스템의 시각을 동기화하는데 사용한다.
(4) Fragmentation offset : 큰 IP 패킷들이 적은 MTU(Maximum Transmission Unit)를 갖는 링크를 통하여 전송되려면 여러개의 작은 패킷으로 쪼개어/조각화(Fragmentation)되어 전송되어야 한다. Fragmentation offset은 8 바이트 단위(2 워드)로 최초 분열 조각으로부터 어떤 곳에 붙여야하는 위치를 나타낸다. 각 조각들이 순서 바뀌어 도착할 수도 있기 때문에 이 필드가 중요하다.

15. 개인정보 보호법 시행령 상 개인정보 영향평가의 대상에 대한 규정의 일부이다. ㉠ , ㉡ 에 들어 갈 내용으로 옳은 것은?

제35조(개인정보 영향평가의 대상) 개인정보 보호법 제33조 제1항에서 “대통령령으로 정하

는 기준에 해당하는 개인정보 파일”이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. 1. 구축·운용 또는 변경하려는 개인정보파일로서 (㉠) 이상의 정보 주체에 관한 민감 정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50 만명 이상의 정보 주체에 관한 개인정보가 포함되는 개인정보파일 3. 구축·운 용 또는 변경하려는 개인정보파일로서 (㉡) 이상의 정보 주체에 관한 개인정보파일

	㉠	㉡
①	5만 명	100만 명
②	10만 명	100만 명
③	5만 명	150만 명
④	10만 명	150만 명

정답 체크 :

(1)

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축ㆍ운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축ㆍ운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축ㆍ운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축ㆍ운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일

16. 버퍼 오버플로우(Buffer Overflow) 공격에 대한 대응으로 해당하지 않는 것은?

① 스택 스매싱(Stack Smashing)
② 스택 가드(Stack Guard)
③ Non-Executable 스택
④ 안전한 함수 사용

정답 체크 :

(1) 스택 스매싱 : 스택 스매싱은 공격자가 의도적으로 버퍼를 오버플로우하여 컴퓨터 메모리의 금지된 영역을 접근하려는 공격이다. 스택 오버플로우는 스택 스매싱 중의 하나라로 생각하면 된다.

오답 체크 :

(2) 스택 가드 : 컴파일러가 프로그램의 함수 호출 시에 복귀 주소 앞에 canary(밀고자, Random, NULL, Terminator(CR, LF)) 값을 주입하고, 종료 시에 canary 값 변조 여부 확인한다.

(3) Non-Executable 스택 : 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우

가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드(eggshell)가 실행된다. Non-Executable 스택을 이용하면 스택에서 프로그램(eggshell)을 실행할 수 없게 하여 버퍼 오버플로우 문제를 해결할 수 있다.
(4) 예를 들어, strcpy(입력 문자열의 길이를 검사하지 않음) 대신에 strncpy(입력 문자열의 길이를 검사함)를 사용한다.

17. 블록체인(Blockchain) 기술과 암호화폐(Cryptocurrency) 시스템에 대한 설명으로 옳지 않은 것은?
① 블록체인에서는 각 트랜잭션에 한 개씩 전자서명이 부여된다.
② 암호학적 해시를 이용한 어려운 문제의 해를 계산하여 블록체인에 새로운 블록을 추가할 수 있고 일정량의 암호화폐로 보상받을 수도 있다.
③ 블록체인의 과거 블록 내용을 조작하는 것은 쉽다.
④ 블록체인은 작업 증명(Proof-of-work)과 같은 기법을 이용하여 합의에 이른다.
정답 체크 :
(3) 블록 체인을 조금이라도 바꿔 쓰면 그 이후의 모든 블록 헤더를 변경해야만 하기 때문에 과거 블록 내용을 조작하는 것은 어렵다. 해당 문제에 대해 전혀 모른다고 하더라도 과거 블록 내용을 조작하는 것은 말이 되지 않는다.
오답 체크 :
(1) 예를 들어, 「어드레스 A로부터 어드레스 B로의 1BTC(비트코인) 송금」이라는 트랜잭션을 만든다. 이때 개인키를 사용해서 디지털서명을 작성한다. 원래 전자서명이라는 단어보다는 디지털서명이라는 단어를 사용해야 한다.
(2) 비트코인에서 블록 체인에 블록을 추가하는 것을 금광으로부터 채굴하는 것에 비유하는데, 채굴을 위해서는 엄청난 양의 해시를 계산하여야 한다.
(4) 비트코인(블록체인)의 위조를 방지하기 위하여 채굴자는 자신의 정당한 분량의 작업을 한 것을 증명하여야 하는 데 이를 PoW(Proof-of-Work)라 한다.

18. 정보통신기반 보호법 상 주요정보통신기반 시설의 보호체계에 대한 설명으로 옳지 않은 것은?
① 주요정보통신기반 시설 관리기관의 장은 정기적으로 소관 주요정보통신시설의 취약점을 분석·평가하여야 한다.
② 중앙행정기관의 장은 소관 분야의 정보통신기반 시설을 필요한 경우 주요정보통신기반 시설로 지정할 수 있다.
③ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설은 지방자치단체의 장이 주요정보통신기반 시설로 지정한다.
④ 과학기술 정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반 시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반 시설로 지정하도록 권고할 수 있다.
정답 체크 :
(3) "정보통신기반 보호법" 제8조(주요정보통신기반시설의 지정 등) 상 ④지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.

오답 체크 :
(1) "정보통신기반 보호법" 제9조(취약점의 분석ㆍ평가) 상 ①관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석ㆍ평가하여야 한다.
(2) "정보통신기반 보호법" 제8조(주요정보통신기반시설의 지정 등) 상 ①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
(4) "정보통신기반 보호법" 제8조의2(주요정보통신기반시설의 지정 권고) 상 ① 과학기술정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다. 이 경우 지정 권고를 받은 중앙행정기관의 장은 위원회의 심의를 거쳐 지정 여부를 결정하여야 한다.

19. 업무연속성(BCP)에 대한 설명으로 옳지 않은 것은?
① 재난복구 서비스인 웜 사이트(Warm Site)는 구축 및 유지비용이 콜드 사이트(Cold Site)에 비해서 높다.
② 콜드 사이트(Cold Site)는 주 전산센터의 장비와 동일한 장비를 구비한 백업 사이트이다.
③ 재해 복구 시스템의 백업센터 중 미러 사이트(Mirror Site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구 한다.
④ 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.
정답 체크 :
(2) 콜드 사이트는 장소만 존재하고, 나머지 사이트(웜, 핫, 미러)는 주전산센터의 장비(하드웨어)와 동일한 장비를 구비하고 있다.
오답 체크 :
(1) 웜 사이트는 콜드 사이트에 없는 장비(하드웨어)를 가지므로 구축 및 유지비용이 높다.
(3) 미러 사이트는 주 전산센터와 동일한 백업 센터(하드웨어, 소프트웨어, 인원)이므로 가장 짧은 시간 안에 시스템을 복구한다.
(4) BCP는 장애에 대한 예방을 통한 중단 없는 서비스 체계를 나타내고, DRP는 재난 발생 후에 경영 유지 • 복구 방법을 명시한다.
Tip! : 해당 문제는 BCP에 DRP 개념을 포함해서 출제하였다.

20. 개인정보 보호법 시행령의 내용으로 옳지 않은 것은?
① 공공기관의 영상정보처리기기는 재위탁하여 운영 할 수 없다.
② 개인정보처리자가 전자적 파일 형태의 개인정보를 파기하여야 하는 경우 복원이 불가능한 형태로 영구 삭제하여야 한다.
③ 개인정보처리자는 개인정보의 처리에 대해서 전화를 통하여 동의 내용을 정보주체에게 알리고 동의 의사표시를 확인하는 방법으로 동의를 받을 수 있다.
④ 공공기관이 개인정보를 목적 외의 용도로 이용하는 경우에는 '이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭'을 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다.
정답 체크 :

(1) "개인정보 보호법 시행령" 제26조(공공기관의 영상정보처리기기 설치·운영 사무의 위탁) 상 재위탁 제한에 관한 사항을 규정하고 있으므로 영상정보처리기기를 재위탁하여 운영할 수 없다고 볼 수는 없다.

오답 체크 :

(2) "개인정보 보호법 시행령" 제16조(개인정보의 파기방법) 상 전자적 파일 형태인 경우 복원이 불가능한 방법으로 영구 삭제하여야 한다.

(3) "개인정보 보호법 시행령" 제17조(동의를 받는 방법) 상 개인정보처리자는 개인정보의 처리에 대하여 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인할 수 있다.

(4) "개인정보 보호법 시행령" 제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항(다른 법률에 특별한 규정이 있는 경우) 각 호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 행정안전부령으로 정하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다.

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 법 제18조제5항(개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우)에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용