2019년 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 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.

답 ②

▷ **쿠키**(cookie): 인터넷 사용자가 웹사이트를 방문할 경우, 사용자 편의를 제공하기 위해 사용자의 계정정보와 환경설정 값 등을 기록하는 정보 파일. 서버가 아니라 클라이언트의 컴퓨터에 저장된다.

<오답 체크> ② 쿠키는 실행파일이 아니며, 데이터를 정보를 기록하기 위한 텍스트 파일이다. 따라서 스스로 디렉터리나 파일에 접근할 수 없다. 물론 쿠키 파일 안에 기록된 내용에 한해서는 읽고 쓰는 것이 가능하며, 접속중인 해당 도메인과 일치하는 웹사이트에서만 가능하다.

문 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.

답 ③

③ **Adware**(애드웨어)에 대한 설명이다.
애드웨어 중 불법적인 애드웨어는 사용자의 동의 없이 컴퓨터에 설치되어 광고 화면을 무분별하게 띄워 불편을 초래하는 악성코드이다.
Netbus(넷버스)는 트로이 목마의 일종으로, 상대방의 컴퓨터를 몰래 조작할 수 있는 크래킹 도구이다. 사용법이 간단하여 초심자들도 쉽게 조작할 수 있으며, 과거 온라인게임 도중 상대방의 PC 전원을 끄거나 네트워크를 차단하는 등 골탕 먹일 목적으로 자주 사용되었다.

문 3. 정보보호 서비스에 대한 설명으로 옳지 않은 것은?

① Authentication - 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용한다.
② Confidentiality - 온오프라인 환경에서 인가되지 않은 상대방에게 저장 및 전송되는 중요정보의 노출을 방지한다.
③ Integrity - 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호한다.
④ Availability - 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 한다.

답 ④

④ 부인 방지(Nonrepudiation)에 대한 설명이다.
가용성(Availability)은 정당한 권한이 있는 사용자는 원하는 시간에 서비스를 정상적으로 이용할 수 있어야 한다는 것을 말한다.

문 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

답 ②

② **Stealth Scan**(스텔스 스캔)은 세션 연결을 완전히 성립하지 않은 상태로 공격 대상 시스템의 포트 활성화 여부를 스캔하는 것으로, 세션 연결이 성립되지 않은 상태이기 때문에 공격 대상 시스템에 로그가 남지 않는다. 따라서 공격 대상의 시스템 관리자는 어떤 IP를 가진 공격자가 자신의 시스템을 스캔했는지 확인할 수 없다. 스텔스 스캔은 포트가 열려있을 때는 아무 응답이 오지 않고, 포트가 닫혀있을 때는 RST 패킷이 전송되어 온다.
스텔스 스캔 중 NULL 스캔은 TCP flag를 모두 비활성화 하여 대상 포트로 패킷을 전송한다.

<오답 체크> ① TCP half은 일반 OPEN 스캔과 비슷하나, 마지막에 서버의 활성화 여부만 확인한 뒤 바로 RST 패킷을 보내 즉시 세션을 끊는 스캔 방법이다.
공격자는 공격 대상 시스템에 SYN 패킷을 보내는데, 포트가 열려있을 경우 SYN/ACK 응답이 오며 공격자는 응답을 받자마자 RST 패킷을 보내 즉시 연결을 끊는다.
포트가 닫혀있을 경우에는 공격 대상 시스템으로부터 RST/ACK 응답이 온다.

③ TCP FIN 스캔도 스텔스 스캔 중 하나로, NULL 스캔과 달리 TCP flag의 FIN을 활성화 하여 대상 포트로 패킷을 전송하는 방식이다.
또 다른 스텔스 스캔인 Xmas Tree 스캔은 TCP flag의 FIN, URG, PUSH을 활성화 하여 대상 포트로 패킷을 전송한다.

④ 시간차를 이용한 스캔으로는 짧은 시간 동안 많은 패킷을 보내어, 방화벽과 IDS의 처리 용량의 최대치를 넘기는 방법과 긴 시간 동안에 걸쳐서 패킷을 전송하여 방화벽과 IDS가 공격자가 전송하는 패킷에 대한 패턴 및 정보 분석을 어렵게 만드는 것이다.

문 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 선택적으로 압축된다.

답 ③

③ IPSec에서의 IKE 프로토콜에 대한 설명이다.
IKE(Internet Key Exchange, 인터넷 키 교환)는 IPSec에서 RSA와 디피 헬만 등의 공개키 기술을 기반으로, 암호화에 사용할 세션키를 관리하고 SA(Security Association, 보안 연계)를 협의하기 위한 프로토콜이다.
SSL의 **Alert** 프로토콜은 이름 그대로 경고 프로토콜로, 에러 메시지를 전송하는 프로토콜이다.

문 6. 블록체인에 대한 설명으로 옳지 않은 것은?

① 금융 분야에만 국한되지 않고 분산원장으로 각 분야에 응용할 수 있다.
② 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다.
③ 앞 블록의 내용을 변경하면 뒤에 이어지는 블록은 변경할 필요가 없다.
④ 하나의 블록은 트랜잭션의 집합과 헤더(header)로 이루어져 있다.

답 ③

③ 블록체인의 각 블록에는 해당 거래 데이터뿐만 아니라 앞 블록의 해시 정보를 담고 있다. 그러므로 이전 블록의 내용을 변경하면 그 해시가 변경되어 뒤에 이어지는 블록과 불일치하게 된다. 따라서 거래 내역을 수정하거나 조작하면 뒤에 이어지는 모든 블록을 수정하여야 하며, 이러한 특성으로 인해 블록체인을 조작하는 것은 굉장히 어렵다.

문 7. 다음의 결과에 대한 명령어로 옳은 것은?

```
Thu Feb 7 20:33:56 2019 1 198.188.2.2 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

답 ②

② 대충 앞부분을 보면 요일, 날짜, 시간으로 추정되는 부분(Thu Feb 7 0:33:56 2019)이 보이며, 그 뒷 부분은 IP주소로 추정되는 부분(198.188.2.2)이 보인다.
그리고 결정적인 부분은 중간의 (/tmp/12-67-ftp1.bmp) 부분과 뒷 부분의 (ftp)라는 값인데, 이것을 통해 FTP 프로토콜을 이용해 bmp 파일을 취급한 기록이라는 것을 추정할 수 있다.

```
Thu Feb 7 20:33:56 2019          - 파일을 전송한 시각
1                                - 전송 소요 시간
198.188.2.2                      - 전송한 호스트 네임
861486                           - 파일의 크기
/tmp/12-67-ftp1.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)
freeexam                         - 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)
```

② **xferlog** 로그는 FTP를 통해 송수신되는 데이터에 대한 정보를 기록하는 로그파일이다.
<오답 체크> ① **messages**: 콘솔 상의 화면에 출력되는 메시지를 기록하는 로그
③ **loginlog**: 로그인할 때 5번 이상 실패하는 경우를 기록하는 로그
④ **audit_event**: 유저가 설정한 특정한 감사(audit) 이벤트들에 대한 내용을 기록하는 로그

문 8. 다음 설명에 해당하는 DoS 공격을 옳게 짝 지은 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 다운시키는 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

답 ②

ㄱ. **Smurf**(ICMP flooding) 공격
출발지 IP주소를 공격대상의 IP주소로 위장하여 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상으로 많은 양의 ICMP Echo 응답 패킷이 몰리게 만들어 시스템 자원이 고갈되도록 만드는 공격이다.

ㄴ. **SYN flooding**(SYN 플러딩)
TCP 3-way handshaking을 이용한 DoS공격
공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

ㄷ. **Land 공격**(Land Attack)
패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격자의 IP 주소 값으로 만들어 전송하는 공격이다. 출발지 주소와 목적지 주소가 같기 때문에 이 패킷의 응답 은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가는데, SYN Flooding처럼 동시 사용자 수를 점유해버리며 CPU 자원을 고갈시킨다.

문 9. 무선 LAN 보안에 대한 설명으로 옳지 않은 것은?

① WPA2는 RC4 알고리즘을 암호화에 사용하고, 고정 암호키를 사용한다.
② WPA는 EAP 인증 프로토콜(802.1x)과 WPA-PSK를 사용한다.
③ WEP는 64비트 WEP 키가 수분 내 노출되어 보안이 매우 취약하다.
④ WPA-PSK는 WEP보다 훨씬 더 강화된 암호화 세션을 제공한다.

답 ①

① RC4 알고리즘에 고정된 암호키를 사용하는 것은 WEP 방식이다. WPA2는 AES 알고리즘의 CCMP 방식을 사용한다.

○ **WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용
○ **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
○ **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증

문 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 $E_K[M \,||\, E_{KSa}[H(M)]]$

답 ④

송신자 인증, 기밀성을 보장하기 위해서는 비밀키 필요
전자서명을 보장하기 위해서는 A의 개인키 필요
무결성을 보장하기 위해서는 해시함수 필요
④ 해시값을 생성(H(M))하였고, 그 해시값을 A의 개인키로 암호화하여 전자서명을 하였다.($E_{KSa}[H(M)]$)
그리고 그 서명을 원본 메시지에 첨부(연결)한 뒤 전체를 비밀키로 암호화하여 기밀성을 부여하였다.

<오답 체크> ① 해시와 비밀키는 사용하였지만, 개인키를 사용하지 않았다. 따라서 누가 보낸 메시지인지 확인할 수 없다.
② 해시값만 비밀키로 암호화하고, 원본 메시지는 암호화하지 않고 그냥 결합하였다. 따라서 기밀성이 보장되지 않는다. 또한 전자서명도 되어 있지 않다.
③ 해시값에 전자서명은 하였으나, 원본 메시지를 암호화하지 않아 기밀성이 보장되지 않는다.

문 11. 다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은?

① SEED 알고리즘 ② RSA 알고리즘
③ DES 알고리즘 ④ AES 알고리즘

답 ②

✠ **대칭키** 암호 알고리즘
DES, 3-DES, IDEA, AES, RC5, Skipjack, Blowfish
(국산) SEED, HIGHT, ARIA, LEA, LSH

✠ **비대칭키** 암호(공개키 암호) 알고리즘
RSA : 소인수분해
Rabin : 소인수분해
ElGamal : 이산대수
ECC : 타원곡선 상의 이산대수
Schnorr : 이산대수, ElGamal에 기반, 짧은 키 길이
DSA : 이산대수, Schnorr의 응용
DSS : 이산대수, 전자서명 전용
ECDSA : 내부적으로 타원곡선
Knapsack : 부분집합의 합을 구하는 문제
(NP-complete 문제)
KCDSA : 국산, 국내표준
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

문 12. 정보보안 관련 용어에 대한 설명으로 옳지 않은 것은?

① 부인방지(Non-repudiation) - 사용자가 행한 행위 또는 작업을 부인하지 못하는 것이다.
② 최소권한(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 크랙킹 하는 방법이다.

답 ④

④ 차분공격은 두 개의 평문 블록들의 비트 차이에 대응되는 암호문 블록들의 비트 차이를 분석하여 사용된 키를 추측하는 방법이다.
공격자가 사용가능한 패스워드의 문자열과 그 해시값을 미리 계산하여 저장해놓은 대용량 해시 테이블을 레인보우 테이블(Rainbow Table)이라고 한다. 서버에 패스워드가 원본 문자열로 저장되지 않고 해시값으로 저장되어 있다는 것을 이용한 공격 방법이다.

문 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 구현에 독립적이고, 보호목표명세서는 구현에 종속적이다.
② 보호프로파일은 보호목표명세서를 수용할 수 있고, 보호목표명세서는 보호프로파일을 수용할 수 있다.
③ 보호프로파일은 여러 시스템·제품을 한 개 유형의 보호프로파일로 수용할 수 있으나, 보호목표명세서는 한 개의 시스템·제품을 한 개의 보호목표명세서로 수용해야 한다.
④ 보호프로파일은 오퍼레이션이 완료되지 않을 수 있으나, 보호목표명세서는 모든 오퍼레이션이 완료되어야 한다.

답 ②

② 보호목표명세서는 보호프로파일을 포함하나, 그 반대는 성립하지 않는다.

○ **보호프로파일(PP**, Protection Profile)
사용자나 개발자의 보안 요구사항을 표현하기 위해 CC를 준용하여 작성된 것으로, 보안기능을 포함한 IT 제품이 갖추어야 할 보안요구사항 집합.
제품군에 대한 보안 요구사항을 정의한 것으로, 특정 제품의 기술적인 구현에 독립적이며, 여러 제품이나 시스템이 동일한 PP를 적용할 수 있다.
○ **보안목표명세서(ST**, Security Target)
개발자가 특정 IT 제품의 보안기능을 표현하기 위해 CC를 준용하여 작성한 것으로, 제품 평가를 위한 기초자료로 사용됨
특정 제품에 대한 보안 명세를 정의한 것이기 때문에 기술적인 구현에 종속적이며, 각 제품이나 시스템은 각각의 ST를 적용한다.
ST는 PP를 포함한다.

문 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

답 ①

① **NAT**(Network Address Translation)
사설 IP 주소를 공인 IP 주소로 변환해주는 기능이다.
NAT 환경에서는 내부 주소가 밖으로 드러나지 않아 보안성을 높이는 효과가 있으며, 내부 사용자 다수가 하나의 공인 IP 주소를 공유할 수 있어 IP 주소를 절약할 수 있다.

<오답 체크> ③ Timestamp Request와 Timestamp Reply는 ICMP의 질의 메시지 중 하나로, 두 시스템 사이에서 IP 데이터그램이 왕복하는데 걸리는 시간(RTT)을 알아내거나, 두 시스템의 시각을 동기화하는데 사용하는 메시지이다.

④ Fragmentation Offset(단편화 오프셋)
단편화 오프셋 값은, 데이터그램을 단편화(분할)할 때, 분할된 부분이 기존 전체의 데이터그램에서 어느 부분의 조각인지 구분하기 위한 태그값(번지 수)이다. 이 태그값은 8바이트 단위로 나누어 표시하는데, 예를 들어 해당 단편화 조각이 전체 데이터그램에서 1,000바이트 위치에 해당하는 조각이라면 오프셋 값은 2000 ÷ 8 = 250이 된다.

문 15. 「개인정보 보호법 시행령」상 개인정보 영향평가의 대상에 대한 규정의 일부이다. ㉠, ㉡에 들어갈 내용으로 옳은 것은?

> 제35조(개인정보 영향평가의 대상) 「개인정보 보호법」 제33조 제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.
> 1. 구축·운용 또는 변경하려는 개인정보파일로서 (㉠) 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
> 2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
> 3. 구축·운용 또는 변경하려는 개인정보파일로서 (㉡) 이상의 정보주체에 관한 개인정보파일

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

답 ①

「개인정보 보호법 시행령」 제35조(개인정보 영향평가의 대상)에서 규정하고 있는 개인정보파일은 다음의 3가지로 나뉜다.

1. **5만명** 이상의 정보주체에 관한 민감정보 또는 고유식별정보
2. 다른 개인정보파일과 연계하려는 경우로서 연계 결과 **50만명** 이상
3. **100만명** 이상의 정보주체 개인정보

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

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

답 ④

④ **Stack Samshing**(스택 스매싱)
스택 버퍼 오버플로우 공격 방법 중 하나로, 버퍼 오버플로우 공격의 타깃이 되는 메모리 부분이 스택에 위치한 버퍼일 경우를 치징하는 용어이다.

<오답 체크> ①

▷ 버퍼 오버플로우 공격에 취약한 함수
strcpy(), strcat(), gets(), getwd(), scanf(), fscanf(), sscanf(), vscanf(), vsscanf(), realpath(), sprintf(), vsprintf(), gethostbyname() 등

▷ 버퍼 오버플로우 공격에 **안전한** 함수
strncpy(), strncat(), fgets(), fscanf(), vfscanf(), snprintf(), vsnprintf() 등

② Non-Executable Stack
가장 기초적인 오버플로우 방어 기법으로, 스택에서 코드가 실행되지 않도록 설정하는 것이다.(**NX-bit** 설정)

③ **Stack Guard**(스택 가드)
메모리의 특정한 위치(ret 앞)에 카나리(canary)라는 특정한 값을 집어넣어, 프로그램 실행시 해당 카나리 값이 변조되었을 경우 스택 영역이 변조되었다고 판단하여 프로그램을 종료하는 방법이다.

문 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 블록 체인에 새로운 블록을 추가할 수 있고 일정량의 암호화폐로 보상받을 수도 있다.
③ 블록체인의 과거 블록 내용을 조작하는 것은 쉽다.
④ 블록체인은 작업증명(Proof-of-work)과 같은 기법을 이용하여 합의에 이른다.

답 ③

③ 블록체인의 각 블록에는 해당 거래 데이터뿐만 아니라 앞 블록의 해시 정보를 담고 있다. 그러므로 이전 블록의 내용을 변경하면 그 해시가 변경되어 뒤에 이어지는 블록과 불일치하게 된다. 따라서 거래 내역을 수정하거나 조작하면 뒤에 이어지는 모든 블록을 수정하여야 하며, 이러한 특성으로 인해 블록체인을 조작하는 것은 굉장히 어렵다.

<오답 체크> ④ 블록체인에 새로운 블록을 하나 추가하려 할 때, 많은 노드 중 어떤 노드에 블록을 추가할 권한을 부여할지를 결정해야 한다. 이 때 블록체인 참여자들은 작업증명이나 지분증명과 같은 알고리즘을 통해 한 노드에 한 노드를 선정하고 나머지 참가자들은 그것을 인정하고 합의에 도달하게 된다.

▷ 작업증명(PoW, Proof of Work)
블록체인 채굴자(miner)가 가진 시스템의 해시 연산 능력에 비례하여 데이터를 기록할 수 있는 권한을 획득하는 방식. 각 참여자들은 자신들이 불록체인에서 사용할 암호학적 해시 값을 얼마나 많이 계산하였는가를 경쟁한다.

▷ 지분증명(PoS, Proof of Stake)
채굴자가 가진 현재의 자산에 비례하여 데이터 기록 권한을 획득하는 방식

문 18. 「정보통신기반 보호법」상 주요정보통신기반시설의 보호체계에 대한 설명으로 옳지 않은 것은?

① 주요정보통신기반시설 관리기관의 장은 정기적으로 소관 주요정보통신시설의 취약점을 분석·평가하여야 한다.
② 중앙행정기관의 장은 소관분야의 정보통신기반시설을 필요한 경우 주요정보통신기반시설로 지정할 수 있다.
③ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설은 지방자치단체의 장이 주요정보통신기반시설로 지정한다.
④ 과학기술정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.

답 ③

③ 지방자치단체의 장이 홀로 주요정보통신기반시설을 지정하는 것이 아니라 행정안전부장관이 지방자치단체의 장과 협의하여 지정한다.

「정보통신기반 보호법」 제8조(주요정보통신기반시설의 지정 등)
④ **지방자치단체의 장이 관리 · 감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의**하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.

<오답 체크>
① 「정보통신기반 보호법」 제9조(취약점의 분석 · 평가) ①항
② 「정보통신기반 보호법」 제8조(주요정보통신기반시설의 지정 등) ①항
④ 「정보통신기반 보호법」 제8조의2(주요정보통신기반시설의 지정 권고) ①항

문 19. 업무연속성(BCP)에 대한 설명으로 옳지 않은 것은?

① 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지· 복구 방법을 명시해야 한다.
② 재해복구시스템의 백업센터 중 미러 사이트(Mirror Site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구한다.
③ 콜드 사이트(Cold Site)는 주전산센터의 장비와 동일한 장비를 구비한 백업 사이트이다.
④ 재난복구서비스인 웜 사이트(Warm Site)는 구축 및 유지비용이 콜드 사이트(Cold Site)에 비해서 높다.

답 ③

③ 주전산센터와 동일한 장비를 구비한 백업 사이트는 핫 사이트이다.(일부 자료에서는 웜 사이트 역시 동일한 장비를 구비한다고 설명이 되어 있다.)

Cold Site(콜드 사이트)는 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.

<오답 체크> ② **Mirror Site**(미러 사이트)

원본 시스템과 동일한 데이터를 실시간으로 처리하여 **동시에 운영**되는 백업 사이트이다. 평상시에도 원본 시스템과 동일한 장비와 데이트를 이용하여 동시에 운영하기 때문에, 원본 시스템에 문제가 발생하여도 미러 사이트가 온전하다면 계속해서 서비스가 가능하다.

④ **Warm Site**(웜 사이트)

핫 사이트와 콜드 사이트의 중간 단계로, 원본 시스템과 동일하거나 그보다 적은 수준의 장비를 구비해놓으며, 전체 데이터가 아닌 중요 데이터만을 백업 사이트에 설치하여 주요 업무에 대한 복구를 지원한다.

하드웨어가 이미 연결이 되어 있으며, 직접 백업본을 갖출 수 있으나 완전하지 못할 수도 있다.

문 20. 「개인정보 보호법 시행령」의 내용으로 옳지 않은 것은?

① 공공기관의 영상정보처리기기는 재위탁하여 운영할 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 의사 표시를 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.

답 ①

① 제26조에 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우 재위탁 제한에 관한 사항을 문서에 포함하여야 한다.
'재위탁 제한'이라는 표현 때문에 헷갈릴 수 있으나, 이는 재위탁을 하는 것은 가능하되 다른 사항들에 비해 제한적으로 가능하다는 것을 의미한다.

① **제26조**(공공기관의 영상정보처리기기 설치·운영 사무의 위탁) ① 법 제25조제8항 단서에 따라 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.
1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

<오답 체크> ② **제16조**(개인정보의 파기방법) ①항
개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.
1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

③ **제17조**(동의를 받는 방법) ①항
개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.
1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

④ **제15조**(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항 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