

# 정보보호론

- 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.

- 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.

- 문 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.

- 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

- 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.

- 문 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.

- 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 freexam 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

- 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	SYN Flooding Attack
② Smurf Attack	SYN Flooding Attack	Land Attack	Land Attack
③ SYN Flooding Attack	Smurf Attack	Land Attack	Land Attack
④ Land Attack	Smurf Attack	SYN Flooding Attack	SYN Flooding Attack

- 문 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.

- 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<sub>a</sub>: 사용자 A의 개인키, KP<sub>a</sub>: 사용자 A의 공개키  
 H: 해시함수, E: 암호화  
 M: 메시지, ||: 두 메시지의 연결

- ① E<sub>K</sub>[M || H(M)]
- ② M || E<sub>K</sub>[H(M)]
- ③ M || E<sub>KS<sub>a</sub></sub>[H(M)]
- ④ E<sub>K</sub>[M || E<sub>KS<sub>a</sub></sub>[H(M)]]

- 문 11. 다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은?  
 ① SEED 알고리즘                      ② RSA 알고리즘  
 ③ DES 알고리즘                        ④ AES 알고리즘
- 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 크래킹 하는 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 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, 보호목표명세서는 보호프로파일을 수용할 수 있다.  
 ④ 보호프로파일은 구현에 독립적이고, 보호목표명세서는 구현에 종속적이다.
- 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

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 개인정보 파일”이란 개인정보를 전자적으로 처리할 수 있는 개인정보 파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운영 또는 변경하려는 개인정보파일로서 ( ㉠ ) 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운영하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운영하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운영 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

- 문 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
- 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.
- 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.
- 문 19. 업무연속성(BCP)에 대한 설명으로 옳지 않은 것은?  
 ① 재난복구서비스인 워밍 사이트(Warm Site)는 구축 및 유지비용이 콜드 사이트(Cold Site)에 비해서 높다.  
 ② 콜드 사이트(Cold Site)는 주전산센터의 장비와 동일한 장비를 구비한 백업 사이트이다.  
 ③ 재해복구시스템의 백업센터 중 미러 사이트(Mirror Site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구한다.  
 ④ 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.
- 문 20. 「개인정보 보호법 시행령」의 내용으로 옳지 않은 것은?  
 ① 공공기관의 영상정보처리기는 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 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.