<정보보호론>

1. 정보보호에 대한 설명으로 옳지 않은 것은? ① 정보자산을 여러 가지 위협으로부터 보호하는 것이다. ② 정보보호의 범위에는 사이버안전이 포함될 수 없다. ③ 정보의 가용성과 보안 측면에서 정보보호는 정보의 활용과 정보의 통제 사이에서 균형 감각을 갖는 행위이다. ④ 정보보호의 대상이 되는 자산에는 소프트웨어, 하드웨어, 데이터, 인적자원이 포함될 수 있다. 답 ②	지방직대비 동형모의고사 4회 1번 1. 위험분석 요소에 관한 내용으로 옳지 않은 것은? ① 자산이 지닌 취약요소를 취약성으로 정의한다. ② 위협요소들은 계속 변하고 있으며, 부분적으로만 알려져 있다. ③ 보호대책은 모든 취약성과 잔재위험을 완벽하게 제거한다. ④ 위험은 대응책이 존재하지 않은 취약성으로 인해 발생하는 기대손실이다. 답 ③

2. 포트 스캔에 대한 설명으로 옳지 않은 것은? ① 분석 대상 시스템에 어떤 서비스가 제공되고 있는지 확인하기 위한 정보수집 방법이다. ② 포트 번호는 0~65,535까지이며, 이 중 0~1,023은 잘 알려진 포트(well-known port)라고 한다. ③ Nmap은 오픈소스 기반 포트 스캔 도구이다. ④ TCP 포트 스캔 시 닫혀 있는 포트로부터 ICMP port Unreachable 패킷이 수신된다. 답 ④	지방직대비 정보보호론 라이브 수업 11번 11. TCP half open 스캔을 수행한다. 대상 포트가 닫혀있을 때의 응답은 무엇인가? ① 응답이 없다. ② RST ③ RST+ACK ④ ICMP Destination Unreachable 메시지 답 ③

3. (가), (나)에 해당하는 정보보호 서비스를 바르게 연결한 것은?

메일 내용에 암호를 적용함으로써 (가) 을 제공할 수 있고, 메일에 전자서명을 적용함으로써 (나) 을/를 제공할 수 있다.

	(가)	(나)
①	기밀성	가용성
②	기밀성	부인방지
③	가용성	기밀성
④	가용성	인증

답 ②

정보보호론 진도별 모의고사 암호시스템 94번

94. 공개키 암호 방식을 사용할 경우 다음 <보기>의 상황에서 사용해야 할 키(key)로 옳은 것은?

<보기>
ㄱ. 철수가 영희에게 보내는 메시지를 제3자가 볼 수 없도록 암호화하여 전송하려 한다.
ㄴ. 철수가 영희에게 철수가 만든 문서이면서 문서가 변경되지 않았음을 확신시켜주는 정보를 함께 보내고자 한다.

	ㄱ	ㄴ
①	철수의 개인키	영희의 공개키
②	철수의 공개키	영희의 개인키
③	영희의 공개키	철수의 개인키
④	영희의 개인키	철수의 공개키

답 ③

4. (가)에 들어갈 용어는?

○ (가) 은/는 1989년에 처음 등장한 것으로 알려져 있고 이후 2006년경에 GPCode라는 (가) 이/가 등장하였다. ○ 최근의 (가) 은/는 공격자의 개인키를 모르면 사실상 풀 수 없는 암호 알고리즘을 사용한다.

① 웜
② 바이러스
③ 랜섬웨어
④ DDoS

답 ③

정보보호론 진도별 모의고사 악성소프트웨어 30번

30. 다음 <보기>의 설명에 해당하는 악성 소프트웨어 또는 공격의 연결이 옳은 것은?

<보기>
ㄱ. 친분이 있는 송신자로 위장해 ID 및 패스워드 정보를 요구한다.
ㄴ. 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구한다.
ㄷ. 불안감을 일으킬 목적으로 SNS나 이메일 등을 통해 거짓 메시지를 전파한다.

	ㄱ	ㄴ	ㄷ
①	스피어피싱	랜섬웨어	혹스
②	스피어피싱	혹스	랜섬웨어
③	혹스	랜섬웨어	스피어피싱
④	혹스	스피어피싱	랜섬웨어

답 ①

5. (가), (나)에 해당하는 악성코드를 바르게 연결한 것은?

(가) DDoS 공격 시 지정된 공격을 수행하도록 하는 악성코드
(나) 사용자의 동의 없이 설치되어 사용자 또는 컴퓨터의 정보를 수집하여 전송하는 악성코드

	(가)	(나)
①	봇	스파이웨어
②	봇	애드웨어
③	루트킷	스파이웨어
④	루트킷	애드웨어

답 ①

정보보호론 진도별 모의고사 - 악성소프트웨어 28번

28. 사용자의 동의 없이 설치되어 컴퓨터의 운영체제 정보, 설치된 프로그램 정보 등 컴퓨터의 정보를 수집하고 이를 외부에 전송하는 악성코드는 무엇인가?

① 스파이웨어 ② 트랩도어
③ 애드웨어 ④ 봇넷

답 ①

6. VPN에서 사용하는 프로토콜이 아닌 것은?

① IGMP
② IPSec
③ L2TP
④ PPTP

답 ①

지방직대비 동형모의고사 16회 20번

20. 다음 중 VPN 관련 프로토콜에 대한 설명으로 옳지 않은 것은?

① L2F(Layer 2 Forwarding)는 CISCO사에서 개발한 터널링 프로토콜로 데이터 링크 계층에서 캡슐화를 지원한다.
② IPSec은 IP망에서 안전한 전송을 위해 표준화된 3계층 터널링 프로토콜이다.
③ L2TP는 L2F 기반으로 PPTP와의 호환성을 고려하여 만들어진 터널링 프로토콜이다.
④ PPTP는 데이터링크 계층의 PPP 프로토콜에 보안기능을 추가하여 만든 것이고, 네트워크 계층에 적용되는 프로토콜이다.

답 ④

7. (가)에 들어갈 용어는?

윈도우 운영체제에서 SAM이 사용자의 로그인 입력 정보(사용자 계정과 패스워드)와 SAM 데이터베이스 정보의 일치 여부를 확인하여 SRM에게 알리면 인증된 사용자에게 고유한 (가) 가 부여된다. 또 SRM은 (가) 를 기반으로 파일이나 디렉토리에 접근을 허용할지 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① GID
② SID
③ SetUID
④ SSID

답 ②

지방직대비 동형모의고사 11회 17번
윈도우 운영체제 보안 컴포넌트에 대한 설명으로 옳지 않은 것은?
① SAM은 로컬 사용자에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스이다.
② LSA는 사용자 모드에서 수행되며, 로컬 보안 정책을 집행하는 책임이 있다.
③ SRM은 커널 모드에서 수행되며, 사용자나 프로세스가 어떤 객체를 열려고 시도하면, 접근 권한을 확인한다.
④ LSA는 사용자에게 보안식별자(SID)를 부여한다.

답 ④

8. 위험 처리 방법에 대한 설명으로 옳은 것은?
① 위험 수용: 위험에 처한 자산의 구조나 사용을 변경한다.
② 위험 감소: 위험을 발생시키는 행위나 시스템을 수행하지 않는다.
③ 위험 전가: 위험에 대응하여 보험을 들거나 다른 기관과 계약을 맺는다.
④ 위험 회피: 현재의 위험을 받아들이고 잠재적 손실 비용을 감수한다.

답 ③

지방직대비 동형모의고사 8회 13번
13. 식별된 위험을 처리하는 방안에 대한 설명으로 옳은 것은?
① 위험 전가 - 사업 목적상 정상적인 수준보다 더 큰 수준의 위험을 받아들이기로 선택하는 것
② 위험 수용 - 위험을 발생시키는 행위나 시스템을 수행하지 않는 것
③ 위험 회피 - 위험에 대한 책임을 제3자와 공유하는 것
④ 위험 감소 - 기술적 통제나 관리적 통제를 수행하여 취약점이 이용될 가능성을 줄이는 것

답 ④

9. 공개키 암호 알고리즘이 아닌 것은? ① RSA ② 타원곡선암호 ③ 배낭암호 ④ A5/1 답 ④	지방직 대비 동형모의고사 1회 2번 2. 공개키 암호 알고리즘에 해당하지 않는 것은? ① RSA ② ElGamal ③ Rijndael ④ DSA 답 ③

10. 다음에서 설명하는 보안 솔루션은? ○ 조직 내 중요한 자료가 외부로 유출되는 것을 막는다. ○ 사용자의 다양한 데이터 전송 수단인 USB 메모리 등과 같은 이동식 저장 매체, 이메일과 같은 네트워크 등을 제어한다. ① DRM ② DLP ③ IPS ④ SIEM 답 ②	정보보호론 진도별 모의고사 네트워크정보보호 1번 1. 다음 네트워크 보안 시스템에 대한 설명으로 옳지 않은 것은? ① 침입 차단 시스템(firewall)은 내부 네트워크와 외부 네트워크의 정보흐름을 통제한다. ② 침입 탐지 시스템(IDS)은 침입 시도에 대해 차단 기능을 수행한다. ③ 침입 방지 시스템(IPS)은 실시간 탐지, 분석하여 비정상적인 패킷인 경우 자동으로 차단한다. ④ 정보유출방지 시스템(DLP)은 내부에서 외부로 나가는 정보를 통제한다. 답 ②

11. 다음 문제가 모두 해결된 블록암호 운용 모드는?

○ 평문 블록이 동일하면 암호문 블록이 같아지는 문제
○ 암호문 블록에 오류가 발생하면 다음 블록의 복호화에 오류가 전파되는 문제

① ECB(Electronic CodeBook)
② OFB(Output FeedBack)
③ CFB(Cipher FeedBack)
④ CBC(Cipher Block Chaining)

답 ②

지방직대비 정보보호론 라이브 수업 3번
3. 블록 암호 운용 모드 중 OFB(Output FeedBack Mode)에 대한 설명으로 옳지 않은 것은?
① 암호화와 복호화가 같은 구조를 갖는다.
② 비트 단위의 오류가 있는 암호문을 복호화하면, 평문의 대응하는 비트에만 오류가 생긴다.
③ 패딩(padding)이 필요없다.
④ 초기화 벡터(IV)를 사용하지 않는다.

답 ④

12. 다음에서 설명하는 블루투스 취약점 공격은?

블루투스 장비 간의 취약한 연결 관리를 악용한 공격으로, 공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행한다. 블루투스 기기가 한 번 연결된 이후에는 다시 연결하지 않아도 자동으로 연결되는 인증 취약점을 이용한 공격이다.

① 블루버그(bluebug)
② 블루재킹(bluejacking)
③ 블루프린팅(blueprinting)
④ 블루스나프(bluesnarf)

답 ①

지방직대비 동형모의고사 8회 23번
23. 다음 <보기>의 내용에 해당하는 블루투스 공격은 무엇인가?

<보기>
◦공격대상이 되는 블루투스 장치를 원격에서 연결하여 임의의 동작을 실행시킨다.
◦블루투스 장치가 서로 한 번 연결되면 그 이후에는 별다른 인증 절차 없이도 자동으로 연결되는 취약점을 악용한다.
◦공격대상과 10m 이내에서 가능하고 이러한 공격으로 전화 걸기, 전화 내용 감청도 가능하다.

① 블루프린팅(Blueprinting)
② 블루스나핑(Bluesnarfing)
③ 블루버깅(Bluebugging)
④ 블루재킹(Bluejacking)

답 ③

14. 안티 리버싱 기법에 해당하는 것만을 모두 고르면?

ㄱ. 난독화 ㄴ. 스택 실드 ㄷ. 안티 디버깅 ㄹ. 카나리아

① ㄱ, ㄷ　② ㄱ, ㄹ
③ ㄴ, ㄷ　④ ㄴ, ㄹ

답 ①

정보보호론 진도별 모의고사 웹보안 53번

53. 리버스 엔지니어링에 대한 대응책에 해당하지 않는 것은?

① 패킹(packing)
② 안티 디버깅(anti-debugging)
③ 쓰레기 코드(garbage code) 삽입
④ 퍼징(fuzzing)

답 ④

15. 개인정보 보호법 상 개인정보의 파기에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
② 개인정보처리자가 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
③ 개인정보처리자가 개인정보를 파기하지 아니하고 다른 법령에 따라 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.
④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 총리령으로 정한다.

답 ④

정보보호론 진도별 모의고사 정보보호관련법 17번

17.「개인정보보호법」21조 개인정보의 파기에 관한 내용으로 옳지 않은 것은?

① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 결합하여서 저장·관리하여야 한다.
④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

답 ③

16. 다중문자 암호 방식에 해당하는 것만을 모두 고르면?

ㄱ. 비즈네르(Vigenèe) 암호
ㄴ. 시저(Caesar) 암호
ㄷ. 플레이페어(Playfair) 암호
ㄹ. 아핀(Affine) 암호

① ㄱ, ㄷ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄴ, ㄹ

답 ①

정보보호론 기본이론서 p.35

심|화|학|습

1. 플레이페어 암호
   ① 다중문자 대치(polyalphabetic substitution) 암호로 1차 세계대전 중에 영국군이 사용한 암호이다.
   ② 이 암호에 사용된 대칭키는 5×5 행렬로 배열된 25개의 알파벳 문자로 구성된다. (문자 I와 J는 암호화될 때 동일한 것으로 간주된다)
   ③ 행렬에서 문자의 배열을 다르게 함으로서 서로 다른 많은 키를 생성할 수 있다.

17. 개인정보 보호법 상 개인정보처리자가 개인정보의 제3자 제공과 관련하여 정보주체에게 동의를 받을 때 정보주체에게 알려야 하는 사항이 아닌 것은?
① 개인정보를 제공받는 자의 개인정보 이용 목적
② 동의에 따른 이익이 있는 경우에는 그 이익의 내용
③ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

답 ②

지방직대비 동형모의고사 5회 19번

19.「개인정보보호법」상 개인정보처리자가 정보주체의 동의를 받아 제3자에게 개인정보를 제공하는 때에 정보주체에게 알려하는 사항에 해당하지 않는 것은?
① 개인정보를 제공받는 자
② 개인정보를 제공하는 자
③ 개인정보의 이용 목적
④ 개인정보의 보유 및 이용 기간

답 ②

19. 개인정보 가명 처리 세부기술에 대한 설명으로 옳지 않은 것은? ① 총계 처리는 평균값, 최댓값, 최솟값, 최빈값, 중간값 등으로 처리한다. ② 일반 라운딩은 올림, 내림, 반올림 등의 기준을 적용하여 집계 처리하는 방법으로, 일반적으로 세세한 정보보다는 전체 통계 정보가 필요한 경우 많이 사용한다. ③ 로컬 일반화는 전체 정보집합물 중 특정 열 항목(들)에서 특이한 값을 가지거나 분포상의 특이성으로 인해 식별성이 높아지는 경우 해당 부분만 일반화를 적용하여 식별성을 낮추는 방법이다. ④ 순서보존 암호화는 원문에 대한 암호화의 적용만 가능하고 암호문에 대한 복호화 적용이 불가능한 암호화 기법이다. 답 ④	지방직대비 동형모의고사 3회 9번 9. 암호화된 상태에서의 연산이 가능한 암호화 방식은? ① 형태보존 암호화 ② 순서보존 암호화 ③ 동형 암호화 ④ 일방향 암호화 답 ③

20. S/MIME에서 사용하는 암호 알고리즘과 기능을 옳게 짝지은 것은? ① DSS - 전자서명 ② ElGamal - 메시지 인증 ③ AES - 전자서명과 세션키 암호화 ④ RSA - 메시지 암호화 답 ①	지방직대비 동형모의고사 6회 11번 11. S/MIME에 대한 설명으로 옳지 않은 것은? ① IETF의 작업 그룹에서 RSA-DSI의 기술을 기반으로 개발된 전자우편 보안 시스템이다. ② 메시지 기밀성, 무결성, 사용자 인증, 송신사실 부인 방지 서비스를 제공한다. ③ 메시지 기밀성을 제공하기 위해 대칭키 암호 알고리즘을 사용한다. ④ 인증기관을 사용하지 않고 공개키의 인증을 사용자 개개인에게 일임한다. 답 ④