2018년 경찰간부후보생 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
④	①	②	④	③	①	④	①	③	④
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
③	①	③	③	②	③	①	②	③	②
21	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
④	④	①	③	③	④	③	①	②	④
31	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**
④	③	③	②	③	②	①	①	④	③

1. 다음 지문에서 설명하는 기술과 바르게 짝지은 것은?

> (가) 디지털콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.
> (나) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털콘텐츠에 삽입하는 기술이다.
> (다) 공격자가 공격전에 공격대상에 대한 다양한 정보를 수집하는 기술이다.

① (가) 워터마킹 (나) 핑거프린팅 (다) 워터링 홀
② (가) 핑거프린팅 (나) 워터링 홀 (다) 풋프린팅
③ (가) 풋프린팅 (나) 워터마킹 (다) 핑거프린팅
④ (가) 핑거프린팅 (나) 워터마킹 (다) 풋프린팅

답 ④

(가) 핑거프린팅(fingerprinting)
(나) 디지털 워터마킹(digital watermarking)
(다) 풋프린팅(footprinting)

<오답 체크> ① **워터링 홀**(Watering Hole)
열대지방의 맹수들이 물 웅덩이(waterhole) 주변에 잠복해 기다리다가 물을 마시러 오는 동물을 사냥하는 것에 비유한 공격으로, 특정 목표 대상 그룹(표적)을 선택하여 그들이 자주 사용하는 웹사이트의 알려지지 않은 취약점을 이용해 악성코드를 심어두고 해당 사이트를 방문하는 사용자들을 악성코드에 감염시키는 방식이다. 해당 웹사이트를 자주 이용하며 신뢰하는 사용자들의 심리를 이용한 공격이다.

2. 암호학적 해시함수(Cryptographic Hash Function)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 어떤 입력 x 에 대해 h(x) 를 계산하기 어려워야 한다.
② 주어진 값 y 에 대해 h(x)=y 의 x 값을 찾는 계산이 어려워야 한다.
③ 생일역설(Birthday Paradox)은 충돌 저항성 공격(Collision Resistance Attack)과 관련한 수학적 분석 결과이다.
④ 입력 길이에 상관없이 고정된 길이를 출력한다.

답 ①

① x는 원문 메시지를 h(x)는 해시값을 의미한다.
주어진 원문 메시지에 대해 해시값을 구하는 건 쉬워야 한다.

<오답 체크> ② y는 h(x)이기 때문에 해시값을 의미한다.
주어진 해시값(y)에 대한 원문 메시지(x)를 구하는 건 매우 어려워야 한다. (일방향성(onewayness) 또는 역상 저항성(preimage resistance))

③ 생일역설은 출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없어야 한다는 충돌 저항성(collision resistance) 또는 강한 충돌 내성(strong collision resistance)에 대한 분석 결과이다.
④ 대부분의 해시 함수는 입력 메시지의 길이에 상관없이 출력되는 해시값의 길이는 동일하다.

3. MD5(Message Digest 5)는 널리 쓰는 해시함수이며, 최종적으로 ( )비트의 해시코드를 출력한다. ( ) 안에 들어갈 적합한 숫자는 무엇인가?

① 64 ② 128
③ 256 ④ 512

답 ②

MD5는 임의의 길이의 메시지를 입력받아, 128비트짜리 고정 길이의 값을 출력한다. 입력 메시지는 512 비트 블록들로 쪼개진다.

SHA-0, SHA-1: 160비트
SHA-224: 224비트
SHA-256: 256 비트
SHA-384: 384비트
SHA-512: 512 비트
MD4, MD5: 128비트
RIPEMD-128: 128비트
RIPEMD-160: 160 비트
HAVAL: 128~256 비트의 가변 길이를 출력

4. 공개키 암호 시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고 이를 복호화하는 과정에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

1. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
2. Bob은 (가)를 Alice에게 전송한다.
3. Alice는 (나)를 사용하여 메시지를 암호화한다.
4. Alice는 생성된 암호문을 Bob에게 전송한다.
5. Bob은 (다)를 사용하여 암호문을 복호화한다.

① (가) Bob의 공개키 (나) Alice의 공개키 (다) Alice의 개인키
② (가) Bob의 개인키 (나) Bob의 공개키 (다) Bob의 개인키
③ (가) Bob의 개인키 (나) Alice의 공개키 (다) Alice의 개인키
④ (가) Bob의 공개키 (나) Bob의 공개키 (다) Bob의 개인키

답 ④

Alice가 Bob에게 암호문을 전달하고 Bob만이 이 암호문을 복호화할 수 있어야 하기 때문에, 전달하고자 하는 메시지는 Bob의 공개키로 암호화를 하고 Bob의 개인키로 복호화를 해야 한다.

(가) Alice가 암호문을 Bob의 공개키로 암호화할 것이기 때문에 먼저 Bob으로부터 공개키를 받아야 한다. 개인키는 절대 공유해선 안 되므로, ②, ③번은 절대 안 된다.

(나) Bob이 복호화할 것이기 때문에, Bob의 공개키로 암호화를 한다.

(다) Bob은 자신의 개인키를 이용해 복호화를 한다.

5. 임의적 접근통제(DAC : Discretionary Access Control)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 객체(데이터)의 소유주에 의하여 접근권한 변경이 가능하다.
② 일반적으로 ACL(Access Control List)을 통해서 이루어진다.
③ 민감도 레이블(Sensitivity Label)에 따라 접근을 허용할지 결정한다.
④ ID기반 접근통제이다.

답 ③

③ 주체(사용자)의 객체(정보)에 대한 접근이 주체의 비밀 취급 인가 레이블(clearance label)과 각 객체에 부여된 민감도 레이블 (sensitivity label)에 따라 접근을 허용할지를 결정하는 방식은 **강제적 접근 제어**(**MAC**, Mandatory Access Control)이다.

<오답 체크>

① 임의적 접근 제어(**DAC**, Discretionary Access Control)는 정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.
② 임의적 접근통제는 각 사용자와 객체의 접근 규칙을 정의해놓은 ACL이나 ACM을 통해 접근을 통제한다.
- 접근가능 목록(**CL**, Capability List): 한 주체의 객체들에 대한 접근 권한 명시
- 접근통제 목록(**ACL**, Access Control List): 한 객체에 대한 주체들의 접근 권한 명시
- 접근통제 매트릭스(**ACM**, Access Control Matrix): ACL과 CL의 결합
  주체들과 객체들의 접근 권한 행렬(매트릭스)

④ DAC는 사용자 기반, ID 기반 접근 통제이다.

6. 대칭키와 공개키 암호화 방식에 관한 다음 설명 중 옳은 것은 모두 몇 개인가?

가. 일반적으로 안전한 키 길이는 대칭키 방식의 키가 공개키 방식의 키보다 길다.
나. 대칭키 방식의 암호화키와 복호화키는 동일하며, 모두 비밀이다.
다. 공개키 방식의 암호화키와 복호화키는 모두 공개이다.
라. 일반적으로 암호화 속도는 대칭키 방식이 공개키 방식보다 빠르다.
마. 대칭키 방식의 알고리즘에는 AES, SEED, ECC 등이 있다.

① 2개 ② 3개 ③ 4개 ④ 5개

답 ①

나. 대칭키 방식은 용어 그대로 암호화키와 복호화키가 동일하며, 유출되지 않아야 한다.
라. 암호화 속도는 대칭키 방식이 더 빠르다.
<오답 체크> 가. 동일한 보안 수준에서 공개키 방식의 키의 길이가 더 길어야 한다.
다. 공개키 방식에서 암호화키는 공개키, 복호화키는 개인키이다. 복호화키인 개인키는 절대 유출되어서는 안 된다.
마. AES, SEED는 대칭키 방식 알고리즘이나, ECC는 타원곡선상의 이산대수 계산의 어려움을 이용한 공개키 방식 알고리즘이다.

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

7. 다음 지문에서 설명하는 접근통제모델은 무엇인가?

> 접근통제모델 중 효율적인 업무처리(Well-formed transactions)와 직무분리(Separation of duties) 두 가지 원칙을 통해 좀 더 정교하게 무결성을 보장하는 모델이다.

① 벨-라파듈라(Bell-LaPadula)
② 비바(Biba)
③ 테이크 그랜트(Take Grant)
④ 클락-윌슨(Clark-Wilson)

답 ④

④ **클락-윌슨**(Clark-Wilson) 모델
무결성 중심의 상업적 모델
- 효율적인 업무처리(Well-formed transaction)
- 직무 분리(Separation of duties)
- 접근 주체가 권한을 가지고 직접 접근하는 게 아니라 프로그램을 통해서 접근

<오답 체크> ① **벨 라파듈라**(BLP, Bell-LaPadula) 모델
기밀성을 중시한 모델
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성 – NRU(No Read Up)
Star(*) 속성 – NWD(No Write Down)

② **비바**(Biba) 모델
무결성을 중시한 모델
높은 등급의 데이터에 쓸 수 없고, 낮은 등급의 데이터를 읽을 수 없다.
단순 무결성 속성 – NRD(No Read Up)
무결성 star(*) 속성 – NWD(No Write Up)

③ **테이크-그랜트**(Take Grant) 모델
Create(생성), Revoke(취소), Take(획득), Grant(승인) 4개의 연산으로 접근 권한을 설정하는 모델

8. 생체인증기술의 정확도는 부정거부율(FRR : False Rejection Rate)과 부정허용율(FAR : False Acceptance Rate)로 측정할 수 있다. 생체인증기술의 정확도에 관한 다음 설명 중 옳은 것끼리 짝지은 것은 무엇인가?

> 가. 사용자 편의성을 요구하는 경우 FAR이 높아지고 FRR은 낮아진다.
> 나. 사용자 편의성을 요구하는 경우 FRR이 높아지고 FAR은 낮아진다.
> 다. 보안성을 강화할 경우 FRR은 높아지고 FAR은 낮아진다.
> 라. 보안성을 강화할 경우 FAR은 높아지고 FRR은 낮아진다.

① 가, 다 ② 가, 라
③ 나, 다 ④ 나, 라

답 ①

◈ **생제 인증 기술**(바이오메트릭스, Biometrics)
하나 이상의 고유한 신체적, 행동적 형질에 기반하여 사람을 인식하는 방식을 두루 가리킨다. 생체 인증 기술에 쓰이는 신체적 특성으로는 지문, 홍채, 얼굴, 정맥 등이 있으며 행동적 특성으로는 목소리, 서명 등이 있다.

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

가. 사용자가 이용하기 편리하기 위해서는 쉽게 인증이 잘 되도록 오인식률(FAR)을 다소 높게 설정한다. 그리고 정당한 사용자가 거부되는 확률이 낮도록 오거부율(FRR)은 낮게 설정한다.

다. 강한 보안성이 필요할 때는 인증이 엄격하게 적용되어야 한다. 따라서 허가되지 않은 사용자가 들어오는 걸 방지하는 것에 초점을 맞춰 오인식률(FAR)을 낮추는 게 가장 중요하다.

9. 다음 중 취약점 점검 도구가 아닌 것은 무엇인가?

① SARA ② NIKTO
③ TCP WRAPPER ④ NESSUS

답 ③

③ TCP WRAPPER(TCP 래퍼)는 호스트 기반 네트워킹 ACL(접근 제어 목록) 시스템으로서, 리눅스 또는 BSD 같은 운영체제의 인터넷 프로토콜 서버에서 네트워크 접근을 필터링하는 도구

<오답 체크> ① SARA(Security Auditor's Research Assistant)는 SATAN에 기반을 둔 네트워크 보안 분석 도구

② NIKTO는 웹 서버 취약점에 대한 기본적인 점검을 하는 도구

④ NESSUS는 네트워크 취약성 분석 도구

10. 윈도우 파일 시스템 NTFS(New Technology File System)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① NTFS는 기본 NTFS 보안의 공유 보안과 동일하게 Everyone 그룹에 대해서는 모든 권한이 '허용'이다.
② 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다.
③ 파일과 폴더에 대한 보안강화 및 접근제어가 가능하다.
④ 저용량 볼륨에 최적화되어 있다.

답 ④

④ NTFS(New Technology File System) 방식은 대용량 하드, 압축, 보호, 백업, 로그 등의 기능을 지원하며, 파일과 폴더별로 개별 관리가 가능하다.

<오답 체크> ① NTFS 볼륨의 기본 NTFS 보안은 공유 보안과 같이 Everyone 그룹에 대해서 모든 권한이 '허용'이다. 그러므로 기본값으로만 설정되어 있는 경우는 로컬 로그온하는 사용자마다 서로 다른 NTFS보안이 적용되지 않는다.

② 그러나 NTFS 볼륨이나 파티션의 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다. 이렇게 서로 다른 보안을 적용 시키는 것을 **로컬 파일 시스템 보안**이라고 한다.

③ 공유 보안에서는 파일 단위까지 보안을 적용 시킬 수 없었지만 NTFS 보안에서는 가능하다. 더욱이 파일에 설정한 NTFS 보안이 폴더에 설정한 NTFS 보안보다 우선순위가 높기 때문에 더욱 강력한 보안을 설정 할 수 있다.

11. 다음 중 윈도우 레지스트리 키가 아닌 것은 무엇인가?

① HKEY_CLASSES_ROOT
② HKEY_CURRENT_USER
③ HKEY_MACHINE_SAM
④ HKEY_USERS

답 ③

③ SAM 파일은 윈도우 사용자 계정 정보와 관리자 비밀번호 등을 가지고 있는 파일이다. SAM 파일에 대한 레지스트리 정보는 'HKEY_LOCAL_MACHINE₩SAM'에 들어있다.

HKEY_LOCAL_MACHINE은 시스템에 있는 하드웨어, 소프트웨어 정보를 갖고 있다.

<오답 체크> ① HKEY_CLASSES_ROOT는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 어플리케이션에 대한 맵핑 정보 등을 갖고 있다.
② HKEY_CURRENT_USER는 현재 로그온되어 있는 사용자에 대한 구성 정보(사용자 프로필)를 갖고 있다.
④ HKEY_USERS는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.

12. 리눅스 시스템 로그(log) 파일 중 계정들의 로그인 및 로그아웃에 대한 정보를 가진 파일은 무엇인가?

① wtmp ② dmesg
③ xferlog ④ btmp

답 ①

① wtmp 로그는 로그인/로그아웃에 대한 정보를 기록한다.

<오답 체크> ② dmesg 로그는 시스템 부팅 시의 로그를 기록한다.
③ xferlog 로그는 FTP 파일 전송 내역을 기록한다.
④ btmp 로그에는 로그인 실패 기록에 대한 정보가 포함되어 있다.

13. 리눅스 명령어에 관한 다음 설명 중 바르게 짝지은 것은 무엇인가?

(가) 파일과 디렉터리의 퍼미션(Permission) 변경
(나) 파일과 디렉터리의 소유권(Ownership) 변경
(다) 사용자 패스워드 변경
(라) 계정 생성

	(가)	(나)	(다)	(라)
①	umask	chown	passwd	netuser
②	chmod	chgroup	passwd	useradd
③	chmod	chown	passwd	useradd
④	umask	chown	chpwd	useradd

답 ③

(가) chmod 명령어는 파일과 폴더의 권한을 변경하는 명령어이다.
(나) chown 명령어는 파일 또는 폴더의 소유권을 바꾸는 명령어이다.
(다) passwd 명령어는 계정의 비밀번호를 지정·변경할 때 사용하는 명령어이다.
비밀번호를 변경하는 다른 명령어로는 chpasswd 명령어가 있다. (chpwd(X))
(라) useradd 명령어는 새로운 사용자 계정을 추가하는 명령어이다.
usermod 명령어는 계정 설정을 변경할 때 사용하는 명령어이다.
userdel 명령어는 계정을 지우는 명령어이다.
<오답 체크> ① umask 명령어는 새 폴더, 새 파일의 퍼미션(권한)을 설정하는 명령어이다.
'net user'**(띄어 써야 한다)** 명령어는 윈도우에서 사용자 계정 정보를 출력하고 변경하는 명령어이다.
리눅스에 netuser 명령어는 없다.
② 파일이나 폴더의 그룹을 변경하는 명령어는 chgrp 명령어이다. (chgroup(X))

14. 사용자가 자신의 홈디렉터리 내에서 새롭게 생성되는 서브 파일의 디폴트 퍼미션을 파일 소유자에게는 읽기(r)와 쓰기(w), group과 other에게는 읽기(r)만 가능하도록 부여하고 싶다. 로그인 쉘에 정의해야 되는 umask의 설정 값으로 옳은 것은 무엇인가?

① umask 133 ② umask 644
③ umask 022 ④ umask 330

답 ③

리눅스에서 폴더를 처음 생성하면 기본적으로 777의 권한이 설정되어 있고, 파일을 처음 생성하면 666의 권한이 설정되어 있다. umask 명령어를 통해 현재 설정된 권한을 제거할 수 있다.
문제에서 파일이기 때문에 현재 설정된 권한은 666다.
소유자에게 rw-, 그룹에 r--, other에 r-- 권한을 부여한다는 것은 644 권한을 의미하기 때문에,
umask 022를 설정하면 된다.

변경 전 권한 110 110 110 = 666
umask -) 000 010 010 = 022

변경 후 권한 110 100 100 = 644

15. 정보보호 보안평가 표준 등에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① TCSEC은 보안등급을 A,B,C,D로 구분하며 네트워크를 고려하지 않은 시스템 보안평가 표준이다.
② ITSEC은 오렌지북으로 불리는 컴퓨터시스템 평가기준으로 미 국방부에서 최초로 수용되었다.
③ CC(Common Criteria)는 단일화된 공통 평가기준을 제정하여 적용함으로써 시간의 절약, 평가비용의 절감 등의 효과가 있다.
④ ISMS는 BS7799를 기반으로 국내 환경에 적합하게 작성하였다.

답 ②

② 오렌지북이라 불리는 미국의 정보보호 시스템 평가 제도는 **TCSEC**(Trusted Computer System Evaluation Criteria)이다.
ITSEC(Information Technology Security Evaluation Criteria)은 유럽의 정보보호 시스템 평가 제도이다.

<오답 체크> ① TCSEC은 네트워크는 고려하지 않고 운영 시스템에만 중점을 둔 단순한 평가 제도이다.
평가 등급으로는 A1, B3, B2, B1, C2, C1, D 등급이 있다.

③ **CC**(Common Criteria, 국제공통평가기준)은 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준

④ **ISMS**(Information Security Management System)는 2004년에 BS7799를 기반으로 국내 실정에 맞춘 정보보호관리체계로 KISA(구 한국정보보호진흥원)에서 국내 표준을 만들었다.
현재 이 제도는 방송통신위원회 소관으로 "정보통신망이용촉진 및 정보보호 등에 관한 법률"에 명시되어 있고 인증기관은 한국인터넷진흥원(KISA)이다. BS7799의 국제 표준화가 이뤄진 ISO27001와 비교하여, KISA ISMS에서 요구하는 인증기준 및 심사절차가 좀더 엄격하다고 할 수 있다.

16. 서비스거부 공격(DoS: Denial of Service)의 유형 중 Smurf 공격에 관한 다음 설명 중 가장 옳은 것은 무엇인가?

① 출발지 IP주소를 존재하지 않는 IP주소로 변조한 후 다량의 SYN 패킷을 전송한다.
② 출발지와 목적지의 IP주소를 동일하게 공격대상의 IP주소로 위조하여 전송한다.
③ 출발지 IP주소를 공격대상 IP주소로 위조하여 ICMP 패킷을 브로드캐스트 주소로 전송한다.
④ ICMP PING 패킷을 비정상적으로 크게 만들어 전송한다.

답 ③

③ **Smurf**(ICMP flooding) 공격
공격대상 호스트의 IP주소로 위장된 소스 IP주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상이 많은 양의 ICMP Echo 응답 패킷을 받아 시스템의 자원을 고갈된다.

<오답 체크> ① **SYN flooding**(SYN 플러딩) 공격
TCP 3-way hancshaking을 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.

② **Land 공격**(Land Attack)
패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격대상의 IP 주소 값으로 위조하여 전송하는 공격이다.
출발지 주소와 목적지 주소가 같기 때문에 이 패킷은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가는데, SYN Flooding처럼 동시 사용자 수를 점유해버리며 CPU 자원을 고갈시킨다.

④ **Ping of Death**
icmp 패킷을 정상보다 매우 크게 만들어 공격하는 DoS 공격이다.
크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

17. 리눅스에서 파일 접근권한 중 setuid나 setgid가 설정되어 있으면 보안상 위험해 질 수 있다. setuid나 setgid가 설정되어 있는 파일을 찾는 명령이 아닌 것은 무엇인가?

① find / -perm -1000 -print
② find / -perm -2000 -print
③ find / -perm -4000 -print
④ find / -perm -6000 -print

답 ①

① 파일에 setuid(Set UserID)나 setgid(Set GroupID)가 설정되어 있으면, 사용자는 해당 파일을 실행하는 동안 그 파일의 소유자(또는 그룹)의 권한을 가지게 된다.
프로그램의 소유자가 관리자라면, 사용자는 소유자인 관리자 권한을 얻게 되고, 공격자는 이렇게 획득한 관리자 권한을 통해 여러 악의적인 동작을 수행할 수 있다.
setuid는 특수 권한 4, setgid는 특수 권한 2로 표시한다.

find 명령어는 특정 파일을 찾는 명령어인데 다음과 같은 옵션을 가진다.
-perm : 특정 권한과 일치하는 파일을 찾는다.
-name : 특정 이름과 일치하는 파일을 찾는다.
-user : 특정 유저와 일치하는 파일을 찾는다.
-group : 특정 그룹과 일치하는 파일을 찾는다.
-size : 특정 사이즈와 일치하는 파일을 찾는다.

'/'는 리눅스의 최상위 디렉터리를 의미하는데 즉, 해당 시스템 전체를 검색한다는 의미이다.
권한은 특수 권한+소유자, 그룹, other 권한의 네 자리수로 표시하는데, 숫자 앞의 '–' 표시는 '적어도'라는 의미다.
setuid는 특수 권한이 4이므로 4000~4777의 설정값을 가지고, setgid는 특수 권한이 2이므로 2000~2777의 설정값을 가지고, setuid와 setgid가 모두 설정된 경우 특수 권한은 '4 + 2 = 6'이므로 6000~6777의 설정값을 가진다.
예를 들어, '-4000'으로 검색을 하면 특수 권한이 4로 시작하는, setuid가 설정된 파일을 찾을 수 있다.

① find / -perm –1000 -print 명령은 특수 권한이 1로 설정된 파일을 찾는데, **특수 권한 1은 스티키 비트(Sticky Bit)**를 의미한다.
스티키 비트(Sticky Bit)가 설정된 폴더에는 누구나 접근 가능하고 파일을 생성할 수 있지만,(파일은 생성한 사람이 소유자가 된다) 파일을 삭제하거나 변경하는 건 소유자나 관리자만 가능하다. 즉, 다른 사람은 자신의 소유가 아닌 파일은 삭제할 수 없으므로, 공유 디렉터리로 쓰고자 할 때 설정한다.

18. 다음 지문에서 설명하는 프로토콜은 무엇인가?

> 가. TCP/IP 네트워크의 시스템이 동일 네트워크나 다른 시스템의 MAC 주소를 알고자 하는 경우에 사용한다.
> 나. IP 주소를 물리적인 하드웨어 주소인 MAC 주소로 변환하여 주는 프로토콜이다.

① TCP/IP ② ARP
③ RARP ④ SMTP

답 ②

② **ARP**(Address Resolution Protocol, 주소 결정 프로토콜)
IP 주소에 대응하는 MAC 주소를 응답해주는 프로토콜

<오답 체크>

① **TCP/IP**(Transmission Control Protocol/Internet Protocol) 프로토콜
인터넷의 기본적인 통신 프로토콜로서이다.
TCP는 메시지나 파일들을 좀더 작은 패킷으로 나누어 인터넷을 통해 전송하는 일과 수신된 패킷들을 원래의 메시지로 재조립하는 일을 담당하며, 하위계층인 IP는 각 패킷의 주소 부분을 처리함으로써, 패킷들이 목적지에 정확하게 도달할 수 있게 한다.

③ **RARP**(Reverse Address Resolution Protocol) 프로토콜은 ARP의 반대로, MAC 주소를 IP 주소를 변환해주는 프로토콜이다.

④ **SMTP**(Simple Mail Transfer Protocol, 간이 전자 우편 전송 프로토콜)
전자메일 송신 프로토콜

POP3(Post Office Protocol)
전자메일 수신 프로토콜, 읽으면 자동 삭제 자동 다운

IMAP(Internet Message Access Protocol, 인터넷 메시지 접속 프로토콜)
전자메일 수신 프로토콜, 읽어도 삭제되지 않음, 다운 여부 본인이 결정

19. 방화벽(firewall)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 패킷 필터링(Packet Filtering) 방화벽은 특정 IP, 프로토콜, 포트의 차단 및 허용을 할 수 있다.
② 패킷 필터링(Packet Filtering) 방화벽은 바이러스에 감염된 파일 전송시 분석이 불가능하다.
③ 어플리케이션 게이트웨이(Application Gateway) 방화벽은 응용 계층에서 동작하기 때문에 다른 방식의 방화벽에 비해 처리 속도가 가장 빠르다.
④ 어플리케이션 게이트웨이(Application Gateway) 방화벽은 각 서비스별로 프록시 데몬이 존재한다.

답 ③

③ 응용 계층 게이트웨이(Application Level Gateway)는 OSI 7계층 응용 계층에서 작동하는 방화벽으로, 프록시(proxy) 기능을 적용하여 내부와 외부 간의 응용 계층의 모든 트래픽에 대해 인증 기능을 제공한다.
응용 계층 게이트웨이는 각 서비스별로 전용 게이트웨이가 존재하며 접속 제어를 수행하기 때문에, 단순하게 패킷의 주소와 포트번호만으로 접속 제어를 수행하는 패킷 필터링에 비해 처리 속도가 느리다.

<오답 체크> ② 패킷 필터링 방화벽(Packet filtering Firewall)은 OSI 7계층 중 네트워크 계층과 전송 계층 사이에서 작동하며, 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등의 규칙을 설정하여 접속제어를 수행한다.
IP 주소와 포트 번호의 규칙을 통해서만 접속 제어만 수행하기 때문에, 패킷 내의 데이터 위·변조 공격에 대해서는 방어할 수 없다.

20. 침입탐지방법에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

> 오용탐지(Misuse)는 침입패턴 정보를 데이터베이스화하고, 사용자 혹은 침입자가 네트워크 및 호스트를 사용하는 활동 기록과 비교하여 동일하면 침입으로 식별하는 것이다. 이 방법은 False Positive가 (가)는 장점이 있지만 반대로 False Negative가 (나)는 단점이 있다.

① (가) 높다 (나) 낮다
② (가) 낮다 (나) 높다
③ (가) 높다 (나) 높다
④ (가) 낮다 (나) 낮다

답 ②

▶ False Positive(거짓 양성)은 실제 상태는 X인데 ○라고 진단하는 오류로서, 실제로는 침입이 아닌데 침입이라고 오진을 하는 것이다.(통계학적으로는 제1종 오류라고 한다.)
▶ False Negative(거짓 음성)은 실제 상태는 ○인데 X라고 진단하는 오류로서, 실제로는 침입인데 침입이 아니라고 오진을 하는 것이다.(통계학적으로는 제2종 오류라고 한다.)

② 오용탐지(Misuse Detection)는 미리 알려진 공격 패턴을 DB로 구성한 뒤, 비교하여 같을 경우에만 침입으로 탐지하는 방식이기 때문에, 실제 침입이 아니라면 DB에 없기 때문에 침입으로 판단할 확률이 매우 적다. 따라서 False Potisivie가 낮다.
하지만 이미 알려진 공격 패턴만 탐지할 수 있기 때문에 새로운 유형의 침입에 대해서는 탐지하지 못하고 정상 활동으로 판단하게 된다. 따라서 False Negative가 높다.

비정상행위 탐지(Anomaly Detection)는 정상 패턴의 범위를 정의해두고, 이러한 범위를 벗어나는 모든 행위를 침입으로 판단하기 때문에, 정상 활동인데도 침입으로 판단하는 False Positive가 높다.
반대로 이미 정상이라고 확인된 패턴을 벗어난 건 모두 침입으로 판단하기 때문에, 침입 활동인데 침입이 아니라고 판단하는 False Negative는 낮다.

21. 보안 취약점 점검 도구에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① netstat은 대부분의 운영체제에 기본으로 탑재된 도구이며 네트워크 상태를 확인하기 위해 사용한다.
② tcpdump는 네트워크 패킷 출력 도구로 특정 구간의 장비 사이에서 네트워크 통신이 되는지 확인하기 위해 사용한다.
③ nmap은 포트 스캔뿐만 아니라 대상 시스템의 운영체제나 네트워크 장치 정보 등을 수집할 수 있는 보안 스캐너이다.
④ WireShark는 네트워크 패킷 생성 및 재전송 도구로 네트워크 침해사고 분석 중 확보한 패킷 파일을 시뮬레이션하기 위해 사용한다.

답 ④

④ 네트워크 패킷 생성 도구로는 nping이 있다.
다양한 프로토콜을 지원하고 각 프로토콜의 헤더를 조정할 수 있고 네트워크 성능 측정에도 이용될 수 있는데, ARP Poisong, DoS 공격 등과 같은 트래픽 생성도 가능하다.
WireShark(와이어샤크)는 WinPcap 패킷 캡쳐 라이브러리를 기반으로 한 자유 및 오픈 소스 패킷 분석 프로그램으로, NIC (Network Interface Card)를 통해 송수신되는 패킷을 분석하는데 유용한 프로그램이다.

<오답 체크> ① netstat는 네트워크의 연결상태, 네트워크 인터페이스 상태를 확인하는 명령어이다.
② tcpdump는 네트워크 상에 흐르는 패킷을 캡처하고 분석하는 프로그램이다.
③ nmap(network mapper)은 스캐닝 프로그램으로 운영 체제, 장치 종류, 운영 시간, 서비스에 쓰이는 소프트웨어 제품, 그 제품의 정확한 버전, 방화벽 기술의 존재와 네트워크 카드의 공급자 등의 컴퓨터 정보를 알아낼 수 있다.

22. 스위치 환경 하에서 나타나는 스니핑(Sniffing) 기법이 아닌 것은 무엇인가?

① Switch Jamming
② ARP Spoofing
③ ICMP Redirect
④ Session Hijacking

답 ④

④ **Session Hijacking**(세션 하이재킹) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채는 공격이다.

<오답 체크> ① **Switch Jamming**(스위치 재밍)은 위조된 MAC 주소를 지속적으로 보내 스위치가 관리하는 매핑 테이블을 넘치게 만드는 스니핑 기법이다.
스위치는 매핑 테이블이 가득 차게 되면, 스위치는 브로드캐스팅(broadcasting) 모드로 전환하게 되어 스니핑이 가능해진다.
② **ARP Spoofing**(ARP 스푸핑)은 공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격으로, 공격 대상자로 보내지는 패킷을 가로채 스니핑을 하는 것이 목적이다.
③ **ICMP Redirect**(ICMP 리다이렉트 = ICMP 스푸핑)
공격자는 공격 대상에게 ICMP 리다이렉트 메시지를 보내, 자신이 공격 대상의 게이트웨이 역할을 하게 만든다. 그러면 공격 대상이 보내는 메시지는 게이트웨이인 공격자를 통하게 되므로 스니핑이 가능해진다.

23. 다음 지문은 무엇에 관한 설명인가?

> 무선랜을 통하여 전송되는 패킷의 각 헤더에 덧붙여지는 32 바이트 길이의 고유 식별자로서, 무선장비가 BSS(Basic Service Set)에 접속할 때 암호처럼 사용한다.

① SSID(Service Set Identifier)
② WEP(Wired Equivalent Privacy)
③ MAC(Message Authentication Code)
④ RFID(Radio Frequency Identification)

답 ①

① **SSID**(Service Set Identifier, 무선 네트워크 이름) 노트북이나 스마트폰 등의 Wi-Fi 무선 장치들을 구분하는 이름이다. 무선 장치들이 BSS(basic service set)에 접속할 때 사용하는 텍스트 데이터이다. 하나의 무선랜을 다른 무선랜으로부터 구별해주는 특징을 갖기 때문에, 특정 무선랜에 접속하려는 모든 AP나 무선 장치들은 반드시 일정한 SSID를 사용해야 한다. 만약 SSID가 변경되면. 그 BSS에 접속할 수 없게 된다.

<오답 체크> ② **WEP**(Wired Equivalent Privacy)
초창기의 무선랜 보안 프로토콜이며, 암호화를 위해 RC4 사용하며, 암호화와 인증에 동일한 키를 사용한다.

③ **MAC**(Message Authentication Code, 메시지 인증 코드)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(송신자에 대한 인증)이 가능하다.

④ **RFID**(Radio Frequency Identification)는 주파수를 이용해 원격 장비를 식별하는 시스템으로 일명 전자태그로 불린다.

24. IPSec 프로토콜에서 AH(Authentication Header) 프로토콜이 제공하는 보안 기능이 아닌 것은 무엇인가?

① 무결성 ② 인증
③ 기밀성 ④ 재전송 공격방지

답 ③

③ 암호화를 통해 기밀성을 제공하는 것은 ESP(Encapsulating Security Protocol, 보안 캡슐 프로토콜)이다.
AH(인증 헤더)는 메시지 무결성과 출처 인증 기능을 하지만, 암호화는 하지 않는다.

<오답 체크> ④ AH(인증 헤더)에는 순서 번호 필드가 포함되어 있어서, 재전송 공격을 방지할 수 있다.

◈ AH(인증 헤더) 구조
▷ Next Header(다음 계층 프로토콜 헤더)
8 비트
원래의 IP 패킷의 프로토콜 필드 값이 이곳에 복사됨
▷ Payload Length(페이로드 길이)
8 비트, 인증 헤더의 길이
▷ Reserved(예약)
16비트, 미래에 사용될 부분으로 예약된 필드
0으로 채워져 있다.
▷ SPI(Security Parameter Index(보안 매개변수 색인)
32 비트, 보안연관(SA)을 결정하는 역할
▷ Sequence Number(순서 번호)
32 비트
재전송 공격 방지를 위한 순서번호
▷ Authentication Data(인증 데이터)
가변 길이
전송 도중에 변경되는 TTL 필드를 제외한 전체 IP 패킷에 해쉬 함수를 적용한 결과 값(HMAC-SHA-96, HMAC-MD5-96 등)

25. 무선랜에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 일반적으로 유선랜에 비해 품질이 낮다.
② 인증 암호의 취약성이 있다.
③ 무선 네트워크는 외부 전자기기와의 전파간섭이 없다.
④ 물리적 특성으로 인한 도난, 불법설치, 불법도청 등의 취약성이 있다.

답 ③

③ 무선랜 통신과 전파간섭을 떼려야 뗄 수 없는 관계의 문제이다. 특히 최근 스마트폰, 태블릿 PC 등 모바일 기기가 보급화되면서 와이파이에 대한 인식이 넓어졌고, 실제로 같은 지역에 많은 와이파이 AP(Access Point) 설치되면서, 서로 전파간섭 현상이 자주 발생하고 있다.

26. 다음 지문은 무엇에 관한 설명인가?

> 가. Phil Zimmermann이 개발한 대표적인 이메일 보안 프로토콜이다.
> 나. RSA와 Diffie-Hellman 등으로 공개키 생성이 가능하다.
> 다. 암호 알고리즘을 이용하여 기밀성, 인증, 무결성, 부인방지 등의 기능 지원이 가능하다.

① POP3 ② S/MIME
③ PEM ④ PGP

답 ④

④ **PGP**(Pretty Good Privacy)는 전자우편 서비스에 대한 보안 기술로, 인증기관을 사용하지 않고 개개인의 신뢰 관계를 이용하여 인증하는 방식이다.

가. 1991년에 Philip R. Zimmermann에 의해 개발되었으며, 전자우편 보안에 있어 사실상의 표준이 되었다.

나. PGP는 RSA 버전과 Diffie-Hellman 버전 등이 있다.
RSA 버전에서는, 전체 메시지를 암호화하는데 사용되는 짧은 키의 생성을 위해 IDEA 대칭키 알고리즘을 사용하며, 짧은 키를 암호화하기 위해 RSA 공개키 알고리즘를 사용한다.
Diffie-Hellman 버전은 전체 메시지를 암호화하기 위한 짧은 키를 위해 CAST 대칭키 알고리즘을 사용하며, Diffie-Hellman 알고리즘을 사용해 짧은 키를 암호화하기 위한 키를 생성한다.

다. PGP는 대칭키 암호화 단독 방식뿐 아니라, 대칭키와 공개키를 같이 사용하는 하이브리드 암호화 방식 또한 지원하여 기밀성, 인증, 무결성에 부인방지 기능까지 지원한다.

<오답 체크> ① **POP3**(Post Office Protocol)
전자메일 수신 프로토콜로, 메일을 읽으면 자동 다운 및 자동 삭제가 된다.

② **S/MIME**(Secure/Multipurpose Internet Mail Extension)는 MIME를 보호하기 위한 보안 기술로, RSA 이용하고 인증기관 필요로 한다.

③ **PEM**(Privacy Enhanced Mail)은 IETF에서 만든 전자우편 암호화 시스템으로, 자동 암호화로 전송 중 데이터가 유출되더라도 내용을 볼 수 없어, PGP에 비해 보안성이 뛰어나다. 다만, 중앙 집중식 키 인증 방식을 사용하기 때문에 대중적으로 널리 사용되기 어렵다는 단점이 있다.

27. FTP(File Transfer Protocol)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 네트워크에서 컴퓨터 간 파일 송.수신을 위한 프로토콜이다.
② FTP는 두 개의 잘 알려진(well-known) TCP 포트를 사용한다.
③ 포트 20번은 제어 연결을 위해 사용되고, 포트 21번은 데이터 연결을 위해 사용된다.
④ FTP는 기본적으로 Active Mode와 Passive Mode를 지원한다.

답 ③

③ FTP는 연결 시 인증 제어 정보 전송을 위해 21번 포트를 사용하고, 실제 데이터 전송을 위해 20번 포트를 사용한다.
<오답 체크> ② 20번과 21번 TCP 포트를 사용한다.
④ Active 모드는 클라이언트가 수신 가능한 포트 번호를 미리 정해서 서버에 알려주는 것이고, Passive 모드는 서버가 포트를 결정하는 것이다.
Active 모드에서 클라이언트는 제어 신호와 함께 수신 가능한 포트 번호를 서버에 알려주는데, 서버는 클라이언트가 알려준 포트들 중 하나를 골라 데이터를 전송한다.

28. DNSSEC는 DNS(Domain Name System)가 갖고 있는 보안 취약점을 극복하기 위한 DNS 확장 표준프로토콜이다. DNSSEC이 예방할 수 있는 공격기법은 무엇인가?

① 파밍(Pharming)
② 피싱(Phishing)
③ 스미싱(Smishing)
④ 랜섬웨어(Ransomware)

답 ①

◈ DNSSEC(DNS Security Extensions)은 DNS 데이터 대상의 '데이터 위조-변조 공격'을 방지하기 위한 인터넷 표준기술이다.
DNS는 설계 당시 보안성을 충분히 고려하지 않아, DNS정보의 위·변조가 가능하다는 문제가 꾸준히 제기되어 왔다. DNSSEC은 이와 같은 '데이터 위-변조 침해공격'에 취약한 DNS의 문제점을 근본적으로 보완 개선하기 위해 국제인터넷표준화기구인 IETF에서 1990년대 후반부터 논의를 시작, 2005년경 완성된 국제표준기술로, 다양한 시험을 거쳐 2010년에는 전세계 최상위 DNS인 '루트DNS'에도 적용되면서, 전세계적으로 적용이 확대되고 있다.
① DNSSEC에서 가장 중점적으로 예방하고자 하는 공격은 '데이터 위·변조 공격'이다.
만일 악의적인 공격에 의해 도메인 네임에 대한 IP 주소가 위·변조된다면, 이 DNS를 이용하는 인터넷 이용자들은 의도치 않은 IP주소로 연결되어 피해를 볼 수 있다. 이러한 네트워크 공격을 **파밍**(pharming) 공격이라고 하며, DNSSEC는 이 파밍 공격 예방를 가장 중요하게 여긴다.
<오답 체크> ② **피싱**(phishing)
인터넷 사용자에게 가짜 도메인을 알려주어, 가짜 사이트로 접속하도록 유도하는 공격이다.
③ **스미싱**(Smishing)
문자 메시지(SMS)와 피싱(Phishing)의 합성어로, 스마트폰 사용자에게 가짜 사이트 주소 링크를 문자 메시지(SMS)로 보내 스마트폰 정보나 소액결제를 유도하는 공격이다.
④ **랜섬웨어**(Ransomware)
인질의 몸값을 뜻하는 ransom과 제품을 뜻하는 ware의 합성어로, 컴퓨터에 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.

29. 웹 서비스 공격기법에 관한 다음 설명 중 공격기법을 바르게 짝지은 것은 무엇인가?

(가) 게시판의 글에 원본과 함께 악성코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 함으로써 클라이언트의 정보를 유출하는 공격기법
(나) 공격자의 악의적인 데이터로 예상하지 못한 명령을 실행하거나 적절한 권한없이 데이터에 접근하도록 인터프리터를 속이는 공격기법
(다) 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격기법

① (가) CSRF (나) Injection (다) XSS
② (가) XSS (나) Injection (다) CSRF
③ (가) CSRF (나) XSS (다) File Upload
④ (가) XSS (나) File Upload (다) Injection

답 ②

(가) **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)는 웹사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.
(나) **Injection**(삽입) 공격은 클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격이다.
(다) **CSRF**(Cross-site request forgery, 크로스사이트 요청 변조) 로그인 된 피해자의 세션 쿠키를 위조하여, 피해자가 의도않은 요청을 웹사이트로 보내 피해입히는 공격이다.

30. 데이터베이스 보안 요구사항에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 부적절한 접근방지 - 인가된 사용자의 접근만이 허락되고 모든 접근요청은 DBMS가 검사한다.
② 추론방지- 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 해야 하는 것을 의미한다.
③ 사용자 인증 - 별도의 엄격한 사용자 인증방식이 필요하다.
④ 다단계 보호 - 데이터에 대한 등급분류를 통하여 책임추적성을 보장한다.

답 ④

④ 다단계 보호는 기밀성과 무결성을 보장한다.
책임추적성을 보장하는 건 시스템 감사(system audit) 기능이다.

패스워드에 사용자의
◈ 데이터베이스 보안 요구사항
▷ 기밀성(confidentiality)
부적절하게 데이터가 노출되는 것을 방지하는 것
▷ 부적절한 접근 방지
승인된 사용자의 접근요청을 DBMS에 의해 검사
▷ 추론방지(inference control)
사용자가 겉에 보이는 일반적 데이터로부터 숨겨둔 비밀정보를 획득하는 추론이 불가능하도록 보호하는 것
▷ 데이터 무결성(data integrity)
부적절하게 데이터가 변경되지 않도록 하는 것
데이터베이스의 일관성 유지
▷ 감사 기능(audit)
데이터베이스에 대한 모든 접근의 감사기록을 생성해야 한다.
▷ 사용자 인증(authentication)
정당한 상대방인지, 진짜인지 가짜인지를 확인하는 것
DBMS는 운영체제의 사용자 인증보다 엄격한 인증 요구
▷ 다단계 보호(Multilevel Protection)
데이터에 대한 등급분류를 통해 기밀성과 무결성을 보장

31. 다음 지문은 무엇에 관한 설명인가?

> 가. 기기 내부에 암호화 및 복호화 그리고 전자서명을 위한 프로세스 및 연산장치가 내장되어 있어 암호화와 관련된 키의 생성 및 검증 등이 가능하다.
> 나. 보안토큰을 말하는 것으로 USB토큰 형태 이외에도 칩 형태, PCMCIA토큰 형태 등을 갖는다.

① OTP(One Time Password)
② TPM(Trusted Platform Module)
③ PKI(Public Key Infrastructure)
④ HSM(Hardware Security Module)

답 ④

④ **HSM**(Hardware Security Module)에 대한 설명이다.
암호화 키를 생성하고 저장하는 역할을 하는 전용 하드웨어이다.
암호화 키를 필요로 하는 다양한 애플리케이션이 있을 경우 관련 키 생성 및 저장을 애플리케이션이 아니라 물리적인 전용 장치를 통해 하는 것이다. HSM에 들어 있는 정보는 원천적으로 외부 복사 및 재생성이 되지 않는다.

<오답 체크> ① **OTP**(One-Time Password, 일회용 비밀번호)
한 번 생성되면 그 인증값이 임시적으로 한 번만 유효한 비밀번호 인증 방식으로, 재사용이 불가능하기 때문에 보안에 안전하다.
하드웨어형 OTP(OTP 토큰)의 경우에도 일회용 비밀번호(OTP, One-Time Password)를 생성할 수 있도록 프로세스와 연산기능이 내장된 장치로 HSM의 한 형태로 볼 수 있다.
하지만 OTP 토큰의 경우 키의 생성만 할 뿐 검증은 하지 못하며, 선지의 'OTP'는 일회용 비밀번호 자체를 뜻하기 때문에 비밀번호 생성기를 묻는 문제의 답으로는 부족하다.

② **TPM**(Trusted Platform Module, 신뢰할 수 있는 플랫폼 모듈)
암호화 키를 포함하여 외부의 공격이나 내부의 다른 요인에 의해 하드웨어의 변경이나 손상을 방지하는 등의 보안 관련 기능을 제공하는 기술이다.

③ **PKI**(Public Key Infrastructure,공개 키 기반구조)는 공개 키 암호 방식을 바탕으로 한 디지털 인증서를 활용하는 소프트웨어, 하드웨어, 사용자, 정책 및 제도 등을 총칭하여 일컫는다.

32. 다음 지문은 무엇에 관한 설명인가?

> 신용카드 기반 지불시스템인 SET(Secure Electronic Transaction)에서는 상점이 카드 사용자의 계좌번호와 같은 정보를 모르게 하는 동시에, 상점에 대금을 지불하는 은행은 카드 사용자가 구매한 물건을 알지 못하지만 상점이 요구한 결제 대금이 정확한지 확인할 수 있게 하기 위해 사용하는 방식이다.

① 인증서(Certificate)
② 전자봉투(Digital Envelop)
③ 이중서명(Dual Signature)
④ 지불게이트웨이(Payment Gateway)

답 ③

③ **이중 서명**(Dual Signature)
전자상거래에서 은행에는 상품 주문정보를 숨기고, 상인에게는 결제정보를 숨기기 위해 상품 주문정보와 결제정보를 각각 암호화하는 서명 방식이다.
고객이 결제 정보를 상인에게 보낼 때 주문정보는 상인의 공개키를 이용 암호화하고, 지불정보는 은행의 공개키를 이용 암호화하여 상인은 지불정보를 보지 못하게 한다.

<오답 체크> ① **인증서**(Certificate)는 공개키나 공개키의 정보를 포함하는 전자 증명서이다.

② **전자 봉투**(Digital Envelop)
전달하고자 하는 메시지와 그 메시지를 암호화한 키의 묶음을 의미한다.
일반적으로 하이브리드 암호화 방식에서 메시지를 일회용 대칭키(세션키)로 암호화한 뒤 그 세션키를 공개키로 암호화하여, 메시지와 암호화된 세션키를 함께 전송한다. 이 때 그 메시지와 암호화된 세션키의 묶음이 전자 봉투가 된다.
대칭키로 암호화한 전자 봉투도 존재한다.

④ **지불 게이트웨이**(Payment Gateway), 지불 중계기관
가맹점 및 다양한 금융시스템의 거래 사이에서 중재자 역할을 하는 기관이다. 판매자로부터 카드정보 결제 요청을 받아 금융기관에 승인 및 결제를 요청한다.

33. 다음 중 전자화폐의 요구사항에 포함되지 않는 것은 무엇인가?

① 이중 사용방지(Double-Spending)
② 양도성(Transferability)
③ 온라인성(On-Line)
④ 분할성(Divisibility)

답 ③

③ 온라인성이 아니라 오프라인성(off-line)이다.

◈ 전자 화폐(Electronic Cash)의 요구사항
▷ 안전성 (Security)
- 물리적 안전성 : 위조의 어려움
- 논리적 안전성 : 모든 참여자들은 자신을 제외한 나머지 참여자들의 공모 공격(collusion attack)에 대해 안전해야 한다.

▷ 프라이버시 (Privacy)
- Untraceability(불추적성): 사용자의 거래 내용은 상점은 물론 은행에 의해서도 추적될 수 없다. (사용자의 익명성 보장)
- Unlinkability(불연계성): 두가지의 지불이 같은 사용자에 의한 것임을 알 수 없다.

▷ 이중사용 방지(Double-spending, Unreusability)
부정한 사용자가 전자화폐를 불법적으로 복사하여 여러 번 반복적으로 사용하는 부정한 행위는 은행에 의해 검출될 수 있어야 한다.

▷ 오프라인(Off-line)
사용자와 상점의 거래는 은행의 개입 없이 일어난다.(일반적으로 전자화폐 시스템은 오프라인으로도 사용 가능해야 한다)

▷ 양도성(Transferability)
타인에게 양도가 가능해야 한다.

▷ 분할성(divisibility)
큰 단위의 화폐는 작은 단위의 화폐로 나누어질 수 있어야 한다.

34. 다음 지문은 무엇에 관한 설명인가?

> 일반적인 정보검색엔진에서는 검색되지 않지만 특정한 환경의 웹 브라우저에서만 접속되어 검색되는 사이트를 가리킨다. 주로 사이버 범죄가 이루어지는 공간이다.

① 웹 쉘(Web Shell)
② 다크 웹(Dark Web)
③ 스턱스넷(StuxNet)
④ 고스트넷(GhostNet)

답 ②

② **다크 웹**(Dark Web)은 암호화된 네트워크에 존재하며 일반적인 검색 엔진이나 일반적인 브라우저를 사용해서는 찾거나 방문할 수 없는 특정 부류의 웹 사이트를 가리킨다.
다크 웹에 접속하기 위해서는 특정 소프트웨어가 필요하며, 여러 계층으로 암호화되어 있기 때문에 범죄나 해커들의 정보 교환 통로로 쓰인다.

◈ 다크 웹과 혼동해서 쓰이는 용어로 딥 웹이 있다.
딥 웹(Deep Web)은 검색 엔진이 찾지 못하는 모든 웹 페이지를 나타낸다. 사용자 데이터베이스, 웹메일 페이지, 등록이 필요한 웹 양식, 유료 결제를 통과해야 하는 페이지도 포함한다. 따라서 다크웹도 딥 웹의 한 형태라고 볼 수 있지만, 둘은 엄연히 다르다.

<오답 체크> ① **웹 쉘**(Web Shell)
공격자가 공격 대상 서버에 악의적으로 제작한 스크립트 파일을 업로드하여 관리자 권한을 획득하는 해킹법이다.
주로 asp, php, jsp, cgi 등 웹스크립트 파일을 통해 이루어진다.

③ **스턱스넷**(Stuxnet)
독일 지멘스사의 원격 감시 제어 시스템인 SCADA의 제어 소프트웨어 및 장비를 공격한다. 스턱스넷은 산업시설을 감시하고 파괴하는 악성 소프트웨어로는 최초이다.

④ **고스트넷**(GhostNet)은 2009년 발견된 거대하고 광범위한 규모의 사이버 스파이 시스템이다. 최소 103개국 1295개의 컴퓨터가 고스트넷의 공격에 당했는데, 이는 특정 목표 대상을 오랜 기간 지속적으로 공격하는 APT 공격과 관련이 있는 것으로 추정된다. 고스트넷 시스템의 근원지는 동북아시아의 한 국가에 집중 배치되어 있다는 사실이 확인되었다.

35. OECD 개인정보보안 8원칙에 포함되지 않는 것은 무엇인가?

① 이용제한의 원칙
② 정보 정확성의 원칙
③ 비공개의 원칙
④ 안전성 확보의 원칙

답 ③

③ 비공개의 원칙이 아니라, 공개의 원칙이다.

◈ OECD 개인정보보호 8원칙

① 수집 제한의 법칙(Collection Limitation Principle) : 개인정보는 적법하고 공정한 방법을 통해 수집되어야 한다.
② 정보 정확성의 원칙(Data Quality Principle) : 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.
③ 목적 명시의 원칙(Purpose Specification Principle) : 개인정보는 수집 과정에서 수집 목적을 명시하고, 명시된 목적에 적합하게 이용되어야 한다.
④ 이용 제한의 원칙(Use Limitation Principle) : 정보 주체의 동의가 있거나, 법규정이 있는 경우를 제외하고 목적 외 이용되거나 공개될 수 없다.
⑤ 안전성 확보의 원칙(Security Safeguard Principle) : 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전 조치를 확보해야 한다.
⑥ 공개의 원칙(Openness Principle) : 개인정보의 처리 및 보호를 위한 정책 및 관리자에 대한 정보는 공개되어야 한다.
⑦ 개인 참가의 원칙(Individual Participation Principle) : 정보주체의 개인정보 열람/정정/삭제 청구권은 보장되어야 한다.
⑧ 책임의 원칙(Accountability Principle) : 개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

36.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조(벌칙) 내용이 아닌 것은 모두 몇 개인가?

가. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
나. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.
다. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 다른 사람을 모욕한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
라. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 사자의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 3천만원 이하의 벌금에 처한다.

① 1개 ② 2개 ③ 3개 4개

답 ②

가. 제70조 1항
나. 제70조 2항
<오답 체크> 다. 정보통신망법에는 모욕죄에 대해 따로 규정되어 있지 않다.
라. 정보통신망법에는 사자의 명예훼손에 대해 따로 규정되어 있지 않다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제70조(벌칙) ① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
② 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.
③ 제1항과 제2항의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.

37.「전자서명법」 제21조(전자서명생성정보의 관리) 제4항의 내용 중 ( ) 안에 들어갈 단어로 바르게 짝지은 것은 무엇인가?

> 공인인증기관은 자신이 이용하는 전자서명(가)정보를 안전하게 보관·관리하여야 한다. 이 경우 당해 전자서명(나)정보가 분실 · 훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 (다)에(게) 통보하고 인증업무의 안전성과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.

① (가) 생성 (나) 생성 (다) 인터넷진흥원
② (가) 검증 (나) 생성 (다) 인터넷진흥원
③ (가) 생성 (나) 생성 (다) 이용자
④ (가) 생성 (나) 검증 (다) 이용자

답 ①

① 전자서명생성정보는 개인키를, 전자서명검증정보는 공개키를 의미한다.
안전하게 보관·관리하고 도난·유출되지 않도록 해야 하는 키는 개인키(전자서명생성정보)이다. 공개키(전자서명검증정보)는 공개된 정보이므로 유출되어도 상관없다.

「전자서명법」 제21조(전자서명생성정보의 관리)
① 가입자는 자신의 전자서명생성정보를 안전하게 보관·관리하고, 이를 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 그 사실을 공인인증기관에 통보하여야 한다. 이 경우 가입자는 지체없이 이용자에게 공인인증기관에 통보한 내용을 고지하여야 한다.
② 공인인증기관은 제1항의 규정에 의한 사실을 통보하거나 고지할 수 있는 수단을 제공하여야 한다.
③ 공인인증기관은 가입자의 신청이 있는 경우외에는 가입자의 전자서명생성정보를 보관하여서는 아니되며, 가입자의 신청에 의하여 그의 전자서명생성정보를 보관하는 경우 당해 가입자의 동의없이 이를 이용하거나 유출하여서는 아니된다.
④ 공인인증기관은 자신이 이용하는 **전자서명생성정보**를 안전하게 보관·관리하여야 한다. 이 경우 당해 **전자서명생성정보**가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 **인터넷진흥원**에 통보하고 인증업무의 안전성과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.

38. 다음 지문은 무엇에 관한 설명인가?

> 가. 자신에게 불리한 증거자료를 사전에 차단하려는 활동이나 기술
> 나. 데이터 복구 회피기법
> 다. 데이터 은닉(Steganography)

① Anti Forensic ② Digital Forensic
③ Root Kit ④ Stealth Scan

답 ①

① **Anti Forensic**(안티 포렌식)
디지털 포렌식 기술에 대응하여 자신에게 불리하게 작용할 가능성이 있는 증거물을 훼손하거나 차단하는 일련의 행위를 말한다.
◈ 안티 포렌식 기법
1. 데이터 파괴(Destruction)
2. 데이터 암호화(Encryption)
3. 데이터 은닉(Hiding)
4. 데이터 조작(Manipulation)
5. 풋프린트 최소화(Minimizing the Footprint)
6. 분석 시간 증가(Reducing analyzability)

<오답 체크> ② **Digital Forensic**(디지털 포렌식)
디지털기기를 매체로 발생하는 전자적 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 말한다.

③ **Root Kit**(루트킷)
해커들이 컴퓨터나 또는 네트웍에 침입한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득하는데 사용하는 도구의 모음이다.

④ **Stealth Scan**(스텔스 스캔)
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 스캔 했는지 확인할 수 없다.

39. 1998년 Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어인 엔케이스(EnCase) 고유의 포렌식 디스크 이미지 파일형식은 무엇인가?

① FTK ② dd
③ SHA ④ E0

답 ④

◈ EnCase(엔케이스) Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 포렌식 소프트웨어이다.
컴퓨터 관련 수사에서 디지털 증거의 획득과 분석 기능을 제공하며, 미국 법원으로부터 증거능력을 인정받았다.

④ EnCase로 이미징된 증거물들은 RAM이 아니라 디스크에 EnCase 증거파일 형식(E01, L01, Ex01, Lx01)으로 저장된다.
EnCase뿐 아니라, FTK, Tableau 등 많은 이미징 도구들은 E01 파일 형식을 지원한다.

<오답 체크> ① **FTK Imager**는 디지털 미디어를 수집하는 데 사용되는 무료 소프트웨어이다. 수집된 데이터 무결성 보장을 위해 비트 단위 또는 비트 스트림으로 알려진 복사본(포렌식 이미지)을 생성한다.

② dd 명령어는 리눅스에서 블록 단위로 파일을 복사하거나 파일 변환을 할 수 있는 명령어이다.
EnCase의 이미징 파일이 리눅스의 dd 명령어에 기초를 두고 있기는 하다.

③ **SHA**(Secure Hash Algorithm, 안전한 해시 알고리즘)은 서로 관련된 암호학적 해시 함수들의 모음이다. 이들 함수는 미국 국가안보국(NSA)이 1993년에 처음으로 설계했으며 미국 국가 표준으로 지정되었다.
SHA 함수군에 속하는 최초의 함수는 SHA-0이라고도 부르며, SHA-0의 변형인 SHA-1이 발표되었으며, 그 후에 SHA-224, SHA-256, SHA-384, SHA-512가 더 발표되었다. 이들을 통칭해서 SHA-2라고 하기도 한다.

40. 다음 지문에서 설명하는 디지털포렌식의 원칙은 무엇인가?

> 증거는 획득하고 난 뒤 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.

① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 무결성의 원칙

답 ③

◈ 포렌식의 원칙
- 재현의 원칙
  증거를 복구하는 과정에서 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함
- 정당성의 원칙
  모든 증거는 적법한 절차를 거쳐서 획득하여야 함
- 신속성의 원칙
  시스템 안의 디스크 또는 메모리 정보가 휘발되기 전에 빠르게 획득하여야 함
- 연계보관성의 원칙
  증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 함
- 무결성의 원칙
  증거가 위조/변조되어서는 안 됨