2022-국회직-정보보호론-해설-곽후근

1. 방화벽의 기능으로 옳지 않은 것은?
① 접근제어
② 로깅 및 감사 추적
③ 인증
④ 암호화
⑤ 시그니처 기반의 침입 탐지

정답 체크
(5) IDS의 기능이다.
오답 체크
(1) 스크리닝 라우터의 기능이다.
(2), (3) 베스천 호스트의 기능이다.
(4) VPN의 기능이다.

2. 접근제어 모델에 대한 설명으로 옳지 않은 것은?
① 임의적 접근제어 기법은 자원의 소유자가 접근 주체를 결정한다.
② 강제적 접근제어 기법은 자원이 소속된 조직의 관리자가 접근권한을 결정한다.
③ 임의적 접근제어 기법은 보안 레이블을 기반으로 접근 가능 여부를 판단한다.
④ 강제적 접근제어 기법은 원래의 객체에 부여된 허가권이 복사된 객체에서도 동일하게 유지된다.
⑤ 임의적 접근제어 기법은 대부분의 운영체제에서 파일의 접근규칙을 정의할 때 활용한다.

정답 체크
(3) 강제적 접근제어 기법을 의미한다.
오답 체크
(1) 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
(2) 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(4) 제약 사항이 복사된 객체에 전파된다.
(5) 유닉스에서 사용된다.

3. 공격자가 자신의 공격시도나 침투 흔적을 숨기기 위해 사용하는 악의적인 프로그램의 집합 혹은 악성 프로그램은?
① 루트킷(Rootkit)
② 스파이웨어(Spyware)
③ 트로이 목마(Trojan Horse)
④ RAT(Remote Administration Tool)
⑤ 랜섬웨어(Ransomware)

정답 체크
(1) 컴퓨터 소프트웨어 중에서 악의적인 것들의 모음으로써, 자신의 또는 다른 소프트웨어의 존재를 가림과 동시에 허가되지 않은 컴퓨터나 소프트웨어의 영역에 접근할 수 있게 하는 용도로 설계되었다.
오답 체크
(2) 설치된 시스템의 정보를 주기적으로 원격지의 특정한 서버에 보내는 프로그램이다.
(3) 사용자가 의도치 않은 코드를 정상적인 프로그램에 삽입한 프로그램이다.
(4) 원격 조정자로 하여금 해당 시스템에 물리적으로 접근권이 있는 것처럼 시스템을 제어하게 해주는 소프트웨어 및 프로그래밍 모음이다.
(5) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.

4. 공개키 기반 구조(PKI)의 특징으로 옳지 않은 것은?
① 디지털 서명의 검증
② 전송 메시지의 암호화
③ 공개키를 인증기관에 등록
④ 등록한 공개키의 암호화
⑤ 공개키와 개인키 쌍의 생성

정답 체크
(4) 등록한 공개키의 서명이다.
오답 체크
(1) 인증기관의 서명을 검증한다.
(2) 공인인증서로부터 얻은 공개키로 암호화를 수행한다.
(3) 공개키를 등록하려는 자가 공개키를 인증기관에 등록한다.
(5) 이용자 또는 인증기관이 생성 가능하다.

5. 솔트(Salt)에 대한 설명으로 옳지 않은 것만을 모두 고르면?

ㄱ. 패스워드 원본 뒤에 추가로 덧붙이는 랜덤 데이터이다.
ㄴ. 단방향 함수에 동일한 패스워드가 입력되어도, 같이 입력된 솔트 값의 차이를 통해 서로 다른 출력 값이 생성된다.
ㄷ. 솔트 값은 패스워드의 길이와 동일하거나, 그보다 길어야 한다.
ㄹ. 솔트 값은 단방향 함수에 패스워드와 함께 입력된 다음, 저장 공간 확보를 위해 삭제된다.
ㅁ. 솔트 값을 적용하면 패스워드의 보안성이 향상된다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ

④ ㄷ, ㄹ
⑤ ㄹ, ㅁ

정답 체크
(4) ㄷ : 패스워드보다 짧다.
ㄹ : 삭제되지 않는다(어떤 salt인지 모르면 패스워드를 확인할 수 없음).
오답 체크
(1), (2), (3) ㄱ : 뒤나 앞에 붙인다(붙인 위치만 알면 됨).
ㄴ : key space가 커지는 효과가 있다.

6. 공격자가 일정 부분의 평문과 이에 대응하는 암호문을 모두 알고 있을 때 비밀키를 알아내기 위한 공격은?
① 기지 평문 공격
② 선택 암호문 공격
③ 선택 평문 공격
④ 암호문 단독 공격
⑤ 전수조사 공격

정답 체크
(1) 기지 평문이란 일정 부분의 평문을 미리 알고 있었다는 뜻이다.
오답 체크
(2) 해독자가 암호 복호화기에 접근할 수 있어 암호문(C)에 대응하는 평문(P)을 얻어내어 해독하는 방법이다.
(3) 해독자가 사용된 암호화기에 접근할 수 있어 평문(P)을 선택하여 평문에 대응하는 암호문(C)을 얻어 키(K)나 평문(P)을 해독하는 방법이다.
(4) 해독자는 단지 암호문 C만을 갖고 이로부터 평문(P)이나 키(K)를 찾아내는 방법이다.
(5) 모든 키의 조합을 다 대입해 보는 공격이다.

7. 백도어 탐지 방법으로 옳지 않은 것은?
① 현재 동작 중인 프로세스 및 열린 포트 확인
② SetUID 파일 검사
③ 백신 등 바이러스 탐지 툴 사용
④ 무결성 검사
⑤ 실행파일 패킹

정답 체크
(5) 안티-리버싱을 위해서 수행한다.
오답 체크
(1) 이상 프로세스 및 허가되지 않은 개방된 포트를 확인한다.
(2) 불필요하게 SetUID가 설정된 파일이 있는지 확인한다.
(3) 바이러스 탐지 툴을 이용하여 백도어를 탐지한다.

(4) 변경된 파일이 있는지 확인한다.

8. 64bit 키를 사용하는 RC4 암호알고리즘을 기반으로 동작하며 IV(Initialization Vector) 헤더를 모아 분석할 경우 키가 노출되는 취약점을 갖는 무선랜 보안방식은?

① WEP
② WPA
③ WPA2
④ TKIP
⑤ CCMP

정답 체크
(1) 전사 공격에 취약하다.
오답 체크
(2), (3) 128비트 키를 사용한다(전사 공격 대비 최소 비트수).
(4) WPA에서 사용된다.
(5) WPA2에서 사용된다.

9. 다음에서 설명하는 AES 운영 모드는?

○ 블록단위로 동작한다. ○ 각 블록을 병렬적으로 처리할 수 있다. ○ 블록이 독립적으로 동작하여 한 블록에서의 에러가 다른 블록에 영향을 주지 않는다.

① CTR
② OFB
③ CFB
④ CBC
⑤ ECB

정답 체크
(5)
오답 체크
(1) 스트림단위로 동작한다.
(2) 스트림단위로 동작한다. 사전 준비를 하면 병렬 처리가 가능하다.
(3), (4) 암호화시에 병렬처리가 안되고, 복호화시 에러가 전파된다.

10. 암호학적 해시 알고리즘에 대한 설명으로 옳지 않은 것은?

① 해시 결과값을 이용하여 해시 입력값을 역으로 찾아내는 것은 계산상으로 불가능해야 한다.
② MD5 및 SHA-1 알고리즘은 취약점이 발견되지 않아 지금도 많이 사용되고 있다.
③ 충돌 저항성(Collision Resistance)은 동일한 출력값(해시값)을 생성하는 두 가지 입력값을 구하는 것이 계산적으로 어렵다는 것을 의미한다.

④ SHA-224은 출력의 길이가 224비트이다.
⑤ 해시 알고리즘은 어떠한 길이의 입력값이 들어오더라도 일정한 길이의 해시값을 출력한다.

정답 체크
(2) 취약점이 발견되어 지금은 거의 사용되지 않는다.
오답 체크
(1) 일방향성 또는 pre-image attack이다.
(3) 약한 충돌과 강한 충돌이 존재한다.
(4) 뒤의 숫자가 출력 비트 길이다.
(5) 입력이 8bit 또는 1Tbit라도 일정 길이의 해시값을 출력한다.

11. 「개인정보 보호법」 제25조에 따라 공개된 장소에서의 영상정보 처리기기 설치가 예외적으로 허용되는 경우가 아닌 것은?
① 법령에서 구체적으로 허용하고 있는 경우
② 범죄의 예방 및 수사를 위하여 필요한 경우
③ 시설안전 및 화재 예방을 위하여 필요한 경우
④ 교통단속을 위하여 필요한 경우
⑤ 통계작성·과학적 연구·공익적 기록보존 등을 위하여 필요한 경우

정답 체크
(5) 해당 경우는 존재하지 않는다.
오답 체크
(1), (2), (3), (4) 제25조(영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치 · 운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집 · 분석 및 제공을 위하여 필요한 경우

12. 다음은 리눅스의 /etc/passwd 파일의 일부이다. 이에 대한 설명으로 옳지 않은 것만을 모두 고르면?

root:x:0:0:root:/root:/bin/bash

(1) (2) (3) (4) (5) (6) (7)

ㄱ. (1)과 (5)는 사용자 계정에 관한 정보들로 반드시 동일한 값이어야 한다.
ㄴ. (2)는 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타낸다.
ㄷ. (3)은 사용자 번호(User ID)를 나타내며, 계정마다 다른 값을 가져야 한다.
ㄹ. 이 파일을 통해 현재 시스템에 등록된 계정 정보를 확인할 수 있다.
ㅁ. (7)은 사용자의 홈 디렉터리 정보를 나타낸다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄱ, ㅁ
④ ㄷ, ㄹ
⑤ ㄷ, ㅁ

정답 체크
(3) ㄱ : (5)는 바꿀 수 있다.
ㅁ : 사용자의 쉘을 나타낸다.
오답 체크
(1), (2), (4), (5) ㄴ : 예전에는 포함되었으나 보안상의 이유로 shadow로 이동하였다.
ㄷ : (4)는 Group ID이다.
ㄹ : 사용자 계정 정보를 확인할 수 있다.

13. 버퍼 오버플로(Buffer Overflow) 공격에 대한 설명으로 옳지 않은 것은?
① 데이터 길이에 대한 불명확한 정의를 악용한 공격이다.
② 버퍼 오버플로 공격에 취약한 함수로 strcpy, strcat, gets, scanf 등이 있다.
③ printf와 같은 함수에서 포맷스트링이 포함된 문자열을 통해 공격이 이루어진다.
④ 스택 버퍼 오버플로 공격으로 해커의 공격 코드가 실행되지 않도록, 스택 가드(Stack Guard), 스택 쉴드(Stack Shield) 등의 방어 기법이 적용될 수 있다.
⑤ 입력 데이터의 길이에 대한 정의를 포함하는 snprintf, fgets 등의 함수 사용이 권장된다.

정답 체크
(3) 포맷 스트링 공격이다.
오답 체크
(1) 데이터 길이를 정하면 버퍼 오버플로우 공격을 막을 수 있다.
(2) 해당 함수에는 데이터 길이에 대한 제한이 없다.
(4) 가드는 카나리아를 이용하고, 쉴드는 특수 스택을 이용한다.
(5) 취약하지 않은 함수는 strncpy, strncat 등이다.

14. 보안 제품 평가 및 기준에 대한 설명으로 옳은 것은?
① CC는 EAL1부터 EAL6까지 6개의 등급으로 구분한다.
② ITSEC에서 최상위 레벨의 보안등급은 A1이다.

③ TCSEC은 유럽 4개국이 작성한 보안 기준이다.
④ ITSEC은 기밀성, 무결성, 가용성을 포괄하는 표준안을 제시한다.
⑤ CC 보증 등급에서 EAL4는 준정형적 설계 및 시험을 요구한다.

정답 체크
(4) TCSEC는 기밀성을 강조하고, ITSEC는 기밀성, 무결성, 가용성을 강조한다.
오답 체크
(1) EAL1부터 EAL7까지 7개의 등급으로 구분한다.
(2) E6이다.
(3) ITSEC에 대한 설명이다.
(5) EAL5이다.

15. SSL/TLS에 대한 설명으로 옳지 않은 것은?
① TCP 프로토콜 상위계층에 위치하여, TCP 프로토콜을 통해 전송하는 데이터를 안전하게 전달하는 것을 목적으로 한다.
② Heartbleed 취약점은 OpenSSL 라이브러리에서 발견된 바 있다.
③ 레코드 프로토콜은 상위계층에서 오는 데이터를 전달한다.
④ TLS 1.3에서는 더 이상 RSA를 키 교환 알고리즘으로 지원하지 않는다.
⑤ TLS 1.3은 TLS 1.2 혹은 그 이하 버전과 비교하여 Handshake 과정에서 주고받는 메시지 교환 횟수가 더 많아졌다.

정답 체크
(5) RTT-0(교환 횟수가 더 줄어듬)을 지원한다(기존은 RTT-1).
오답 체크
(1) 암호화를 수행한다.
(2) Heartbeat에서 문제가 발생한다.
(3) 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.
(4) DH를 이용한다.

16. 블루투스(Bluetooth) 연결을 통해 무선 기기에서 무단으로 정보에 접근하는 것을 말하며, 공격자가 OPP(OBEX Push Profile)를 사용하여 상대 기기에 있는 주소록이나 달력, 파일 등을 접근하는 공격은?
① 블루버그(Bluebug)
② 블루스나프(Bluesnarf)
③ 블루프린팅(Blueprinting)
④ 블루재킹(Bluejacking)
⑤ BIAS(Bluetooth Impersonation AttackS)

정답 체크
(2) OPP와 연관을 맺는다.
오답 체크

(1) 취약한 연결 관리와 연관을 맺는다.
(3) SDP와 연관을 맺는다.
(4) 블루투스를 통한 문자 메시지 전송과 이를 통해 해킹과 연관을 맺는다.
(5) 암호화 연결을 생성하기 위해서는 두 개의 블루투스 기기를 페어링할 때 링크 키를 사용해야 하는데, 기기와 물리적으로 근접한 무단 공격자는 이전에 페어링(연결된) 기기를 위조하여 링크 키 없이도 인증할 수 있다.

17. 위험분석 및 평가를 통해 도출된 위험에 대해 적절한 처리를 하고자 할 때, 접근 방법으로 옳지 않은 것은?
① 위험 수용
② 위험 감소
③ 위험 회피
④ 위험 전가
⑤ 위험 검사

정답 체크
(5) 해당 방법은 존재하지 않는다.
오답 체크
(1) 위험의 잠재 손실 비용을 감수하는 것이다.
(2) 위험을 감소시킬 대책을 마련하는 것이다.
(3) 위험이 존재하는 사업, 프로세스를 진행하지 않는 것이다.
(4) 보험이나 외주 등으로 잠재적 위험을 제3자에게 전가하는 방법이다.

18. SYN Flooding 공격과 ARP Spoofing 공격이 이루어지는 네트워크 OSI 계층으로 올바르게 짝지어진 것은?

	SYN Flooding 공격	ARP Spoofing 공격
①	Physical Layer	Network Layer
②	Network Layer	Transport Layer
③	Transport Layer	Data Link Layer
④	Data Link Layer	Network Layer
⑤	Network Layer	Data Link Layer

정답 체크
(3) SYN Flooding : TCP 3-way handshaking에서 발생한다.
ARP Spoofing : 공격자의 가짜 MAC을 알려준다.

19. 공개키 암호방식의 성능문제와 대칭키 암호방식의 키 관리 문제를 상호 보완하여 하이브리드 암호화 환경을 구축하고자 한다. 〈보기〉의 ㉠, ㉡에 해당하는 알고리즘으로 올바르게 짝지어진 것은?

〈보 기〉

㉠ 키 생성 및 교환을 위한 알고리즘

㉡ 데이터 암호화 알고리즘

	㉠	㉡
①	SHA	RSA
②	RSA	AES
③	AES	SHA
④	SEED	RSA
⑤	RSA	SHA

정답 체크

(2) ㄱ : 공개키를 사용한다.

ㄴ : 대칭키를 사용한다.

오답 체크

(1), (3), (4), (5) SHA : 해시 알고리즘이다.

SEED : 대칭키 알고리즘이다.

20. 사용자가 일시적으로 파일 소유자의 권한으로 특정 기능을 실행하고자 할 때, 사용 가능한 명령어로 옳은 것은?

① chmod u+rw testfile

② chmod 666 testfile

③ chmod o+r testfile

④ chmod 4755 testfile

⑤ chmod g+w testfile

정답 체크

(4) SetUID를 설정하기 위해 4---을 사용한다.

오답 체크

(1) 사용자에게 읽기, 쓰기 권한을 준다.

(2) 사용자, 그룹, 제3자에게 읽기, 쓰기 권한을 준다.

(3) 제3자에게 읽기 권한을 준다.

(5) 그룹에게 쓰기 권한을 준다.