

정 보 보 호 론

1. 방화벽의 기능으로 옳지 않은 것은?

- ① 접근제어
- ② 로깅 및 감사 추적
- ③ 인증
- ④ 암호화
- ⑤ 시그니처 기반의 침입 탐지

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.

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)

4. 공개키 기반 구조(PKI)의 특징으로 옳지 않은 것은?

- ① 디지털 서명의 검증
- ② 전송 메시지의 암호화
- ③ 공개키를 인증기관에 등록
- ④ 등록된 공개키의 암호화
- ⑤ 공개키와 개인키 쌍의 생성

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

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

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

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

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

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.

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

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

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.

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.

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.

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)

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

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

	<u>SYN Flooding 공격</u>	<u>ARP Spoofing 공격</u>
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

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

<u>—<보 기>—</u>	
㉠ 키 생성 및 교환을 위한 알고리즘	
㉡ 데이터 암호화 알고리즘	

	<u>㉠</u>	<u>㉡</u>
①	SHA	RSA
②	RSA	AES
③	AES	SHA
④	SEED	RSA
⑤	RSA	SHA

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