정 보 보 호 론

1. 다음 중 정보 보안 시스템을 설계하거나 운영할 때의 목표로 옳지 않은 것은?

① 기밀성 보장
② 무결성 보장
③ 가용성 보장
④ 책임회피성 보장
⑤ 사용자 인증

2. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은?

① 공개된 채널을 통하여 서로 정보를 교환하는 것만으로 공통의 비밀키를 만들어 낼 수 있다.
② 부인방지를 제공하는 전자서명이 가능하다.
③ 인수분해 문제에 기반한 알고리즘이다.
④ 중간자 공격을 수행하는 것이 불가능하다.
⑤ 키 생성 시 사용된 난수가 노출되어도 비밀키는 안전하다.

3. OWASP(The Open Web Application Security Project)에서 2013년에 발표한 10대 웹 취약점에 속하지 않는 것은?

① 인젝션
② 크로스 사이트 요청 변조
③ 인증 및 세션 관리 취약점
④ 취약한 간접 객체 참조
⑤ 검증되지 않은 리다이렉트 및 포워드

4. 다음 중 TCP 세션 하이재킹에 대한 설명으로 옳은 것은?

① 서버와 클라이언트의 통신에서 TCP의 송신 포트 제어에 문제가 발생하도록 공격한다.
② 서버와 클라이언트의 통신에서 TCP의 ACK 넘버 제어에 문제가 발생하도록 공격한다.
③ 서버와 클라이언트의 통신에서 TCP의 시퀀스 넘버 제어에 문제가 발생하도록 공격한다.
④ 서버와 클라이언트의 통신에서 TCP의 수신 포트 제어에 문제가 발생하도록 공격한다.
⑤ 서버와 클라이언트의 통신에서 TCP의 체크섬 제어에 문제가 발생하도록 공격한다.

5. <보기>는 XSS(Cross-site Scripting) 공격을 수행하기 위한 각 단계들을 나타낸다. ㄱ~ㅁ을 순서에 맞게 나열한 것으로 옳은 것은?

<보 기>

ㄱ. 사용자 시스템에서 XSS 코드가 실행된다.
ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.
ㄷ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.
ㄹ. 결과가 공격자에게 전달된다.
ㅁ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.

① ㄴ-ㄱ-ㄷ-ㄹ-ㅁ
② ㄴ-ㄱ-ㄹ-ㄷ-ㅁ
③ ㄴ-ㄷ-ㅁ-ㄱ-ㄹ
④ ㄷ-ㄴ-ㄱ-ㅁ-ㄹ
⑤ ㄷ-ㄴ-ㅁ-ㄱ-ㄹ

6. ECC(Elliptic Curve Cryptography) 암호시스템에 대한 설명으로 옳지 않은 것은?

① 타원곡선 상의 이산대수 문제에 기반을 둔다.
② 키 교환, 암호화, 전자서명에 모두 사용 가능하다.
③ RSA보다 짧은 공개키를 이용하여 비슷한 수준의 보안레벨을 제공한다.
④ 임베디드 플랫폼 등과 같은 경량 응용분야에는 적합하지 않다.
⑤ 비슷한 수준의 보안레벨에서는 RSA보다 전자서명 생성 속도가 빠르다.

7. <보기>에서 설명하는 해시함수(H)의 특성으로 옳은 것은?

<보 기>

주어진 메시지 x에 대해, H(x)=H(y)인 x≠y를 만족하는 두 개의 메시지 x, y를 찾는 것이 어려울 때, 해시함수가 이 성질을 가지고 있다고 한다.

① Second Pre-image Resistance
② Collision Resistance
③ Integrity
④ Onewayness
⑤ Uniform Distribution

8. 시스템 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM (Trusted Platform Module)이 있다. TPM이 지원하지 않는 기능은?

① 암호키 생성 및 저장
② 인증된 부트(Authenticated Boot)
③ 디바이스 및 플랫폼 인증
④ 원격 검증(Remote Attestation)
⑤ 감사(Audit)

9. 네트워크에서 서비스를 제공하는 서버 혹은 시스템은 동시 접속할 수 있는 사용자 수를 제한한다. 이러한 특성을 이용하여 다수의 존재하지 않는 사용자가 시스템에 접속한 것처럼 속여 다른 사용자가 서비스를 받지 못하게 하는 공격으로 옳은 것은?

① Ping of Death
② SYN Flooding
③ Boink
④ TearDrop
⑤ Smurf

10. 메시지 인증 코드(MAC: Message Authentication Code)에 대한 설명으로 옳지 않은 것은?

① MAC 검증을 통하여 메시지의 위조 여부를 판별할 수 있다.
② MAC을 이용하여 송신자 인증이 가능하다.
③ MAC 검증을 위해서는 메시지와 공개키가 필요하다.
④ 해시함수를 이용하여 MAC을 생성할 수 있다.
⑤ MAC 생성자와 검증자는 동일한 키를 사용한다.

11. 수동적 보안 공격에 해당하는 것을 <보기>에서 모두 고르면?

<보 기>

ㄱ. 신분 위장 ㄴ. 메시지 변경 ㄷ. 도청
ㄹ. 트래픽 분석 ㅁ. 서비스 거부

① ㄱ, ㄴ
② ㄴ, ㅁ
③ ㄷ, ㄹ
④ ㄱ, ㄷ, ㄹ
⑤ ㄷ, ㄹ, ㅁ

12. 디지털 포렌식(Digital Forensic)을 통해 획득된 증거가 법적인 효력을 갖기 위해서는 증거를 발견(Discovery), 기록(Recording), 획득(Collection), 보관(Preservation)하는 절차가 적절해야 한다. 이를 만족하기 위해 지켜야 하는 기본 원칙으로 옳지 않은 것은?

① 최량 증거의 원칙
② 재현의 원칙
③ 정당성의 원칙
④ 신속성의 원칙
⑤ 연계보관성의 원칙

13. 와이파이(Wi-Fi) 보안 기술에 대한 설명으로 옳지 않은 것은?

① IEEE 802.11 표준 기반의 무선 랜 기술이다.
② WEP 방식은 현재 보안상 취약점이 발견되었다.
③ WEP 방식은 MAC(Media Access Control) 주소 인증 프로토콜을 사용한다.
④ WPA 방식은 TKIP(Temporal Key Integrity Protocol)를 사용한다.
⑤ WPA2 방식은 AES-CCMP(Counter Mode CBC-MAC Protocol)를 사용한다.

14. 접근 제어 모델에 대한 설명으로 옳지 않은 것은?

① DAC(Discretionary Access Control)는 정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.
② MAC(Mandatory Access Control)는 사용자 계정에 기반하며, 자원의 소유자가 다른 사용자의 보안 레벨을 수정할 수 있다.
③ BLP(Bell-LaPadula) 모델은 자신보다 높은 보안 레벨의 문서에 쓰기는 가능하지만, 보안 레벨이 낮은 문서에는 쓰기 권한이 없다.
④ BLP의 보안 목적은 기밀성이지만, Biba 모델은 정보의 무결성을 높이는 데 있다.
⑤ RBAC(Role Based Access Control)는 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

15. <보기>에서 설명하는 블록암호 운영모드로 옳은 것은?

<보 기>

- '한 단계 앞의 암호 알고리즘의 출력을 암호화한 값'과 '평문 블록'을 XOR 연산하여 암호문 블록을 생성하는 운영모드이다.
- 암호화와 복호화가 같은 구조를 가지고 있다.
- 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트에만 에러가 발생한다.

① ECB
② CBC
③ CFB
④ OFB
⑤ CTR

16. 다음 중 캐싱(Caching) 장비가 응답하지 않도록 설정된 다수의 HTTP GET 패킷을 특정 시스템에 전송하여 서비스를 마비시키는 공격으로 옳은 것은?

① Slowloris 공격
② HTTP GET Flooding 공격
③ ARP Spoofing 공격
④ DNS Spoofing 공격
⑤ HTTP CC(Cache-control) 공격

17. 다음 지문의 ㉠에 들어갈 말로 옳은 것은?

리눅스 시스템에서 관리자(root) 권한이 필요 없는 프로그램에 소유자가 관리자로 되어 있으면서 (㉠)가 설정된 경우에는 시스템의 보안에 허점을 초래할 수 있다. 실제로 이것이 설정된 파일은 백도어 및 버퍼 오버플로우 등 여러 공격에 이용된다.

① SetUID
② SetGID
③ Sticky Bit
④ Finger
⑤ Shadow

18. 다음 중 버퍼 오버플로우(Buffer Overflow)에 취약한 C언어 함수로 옳지 않은 것은?

① int scanf (const char *format, ...);
② char *gets (char *buf);
③ int strcmp (const char *str1, const char *str2);
④ char *realpath (const char *path, char *resolved_path);
⑤ char *strcat (char *dest, const char *src);

19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공하는 경우, 이용자에게 알리고 동의를 받아야 하는 내용으로 옳지 않은 것은?

① 개인정보를 제공 받는 자
② 제공하는 개인정보의 항목
③ 개인정보를 제공 받는 자의 개인정보 이용 목적
④ 개인정보를 제공 받는 자의 개인정보 보호책임자
⑤ 개인정보를 제공 받는 자의 개인정보 보유 및 이용기간

20. <보기>에서 설명하는 SSL 프로토콜로 옳은 것은?

<보 기>

이 프로토콜을 이용하여 서버와 클라이언트가 서로를 인증하고, 암호와 MAC 알고리즘, 그리고 SSL 레코드 안에 보낼 데이터를 보호하는 데 사용할 암호키를 협상할 수 있다.

① Alert Protocol
② Handshake Protocol
③ Record Protocol
④ Change Cipher Spec Protocol
⑤ Encapsulating Security Payload Protocol