정보보호론

1. 정보보호시스템이 제공하는 보안서비스 개념과 그에 대한 설명으로 옳은 것은?

ㄱ. 기밀성(Confidentiality): 데이터가 위·변조되지 않아야 함
ㄴ. 무결성(Integrity): 권한이 있는 자는 서비스를 사용하여야 함
ㄷ. 인증(Authentication): 정당한 자임을 상대방에게 입증하여야 함
ㄹ. 부인방지(Nonrepudiation): 거래사실을 부인할 수 없어야 함
ㅁ. 가용성(Availability): 비인가자에게는 메시지를 숨겨야 함

① ㄱ, ㄴ
② ㄱ, ㅁ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
⑤ ㄹ, ㅁ

2. 서버 관리자가 해커의 공격이 발생하고 있음을 감지하고 tcpdump 프로그램으로 네트워크 패킷을 캡처하였다. 다음의 요약된 캡처 정보가 나타내는 공격으로 옳은 것은?

```
13:07:13. 639870 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 670484 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 685593 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 693481 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 712833 192.168.1.73.2321 > 192.168.1.73.http ...
```

① Smudge 공격
② LAND 공격
③ Ping of Death 공격
④ Smurf 공격
⑤ Port Scan 공격

3. 메시지 인증 코드와 전자서명에 대한 설명으로 옳은 것은?

① 전자서명은 대칭키가 사전에 교환되어야 사용할 수 있다.
② 메시지 인증 코드와 전자서명 모두 무결성과 부인방지 기능을 제공한다.
③ 전자서명은 서명 생성자를 인증하는 기능이 있다.
④ 메시지 인증 코드값을 검증하는 데 공개키가 필요하다.
⑤ 전자서명은 서명-후-해시(Sign-then-Hash) 방식이다.

4. 아래 그림은 TLS(Transport Layer Security)를 통해 쇼핑몰에 로그인하는 화면이다. 이에 대한 설명으로 옳지 않은 것은?

① TLS는 현재 1.1 버전까지 발표되었다.
② TLS는 SSL을 기반으로 한 IETF 인터넷 표준이다.
③ 서버 인증서를 통해 서버를 인증하고 키교환을 한다.
④ 상호 교환된 키로 사용자의 패스워드는 암호화된다.
⑤ 주소창에 있는 자물쇠를 클릭하면 서버 인증서를 볼 수 있다.

5. TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은?

① 하드웨어 기반으로 안전한 저장공간과 실행영역을 제공한다.
② 난수발생기, 암·복호화 엔진, RSA 키 생성기 등을 포함한다.
③ 비휘발성 메모리 영역에 최상위 루트 키가 탑재된다.
④ 단계적으로 인증된 절차로 운영체제가 부팅되도록 한다.
⑤ 국내 공인인증서 저장 시 서명키를 저장하는 표준방식이다.

6. CPU의 NX(No-Execute) 비트 기술을 활용하여 효과적으로 차단할 수 있는 공격 유형으로 옳은 것은?

① Cross-Site Scripting 공격
② Denial of Service 공격
③ ARP Spoofing 공격
④ SQL Injection 공격
⑤ Buffer Overflow 공격

7. IPsec에 대한 설명으로 옳지 않은 것은?

① IPsec 정책 설정 과정에서 송·수신자의 IP주소를 입력한다.
② AH(Authentication Header) 프로토콜은 무결성을 제공한다.
③ 트랜스포트(Transport) 모드에서는 IP헤더도 암호화된다.
④ 재전송 공격을 막기 위해 IP패킷별로 순서번호를 부여한다.
⑤ IKE(Internet Key Exchange) 프로토콜로 세션키를 교환한다.

8. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 규정하는 정보보호 관리체계의 인증권자와 개인정보보호 관리체계의 인증권자를 순서대로 나열한 것으로 옳은 것은?

① 미래창조과학부장관, 방송통신위원회
② 미래창조과학부장관, 한국인터넷진흥원
③ 방송통신위원회, 방송통신위원회
④ 방송통신위원회, 한국인터넷진흥원
⑤ 한국인터넷진흥원, 한국인터넷진흥원

9. 해커가 리눅스 서버에 침입 후 백도어를 설치하였다. 백도어와 연관된 포트가 열려있는지 확인하기 위해 사용할 수 있는 프로그램으로 옳은 것은?

① ps
② nmap
③ nslookup
④ traceroute
⑤ ping

10. 암호학적 해시함수에 대한 설명으로 옳지 않은 것은?

① MD5나 SHA-1은 취약점이 발견되어 더 이상 사용하지 않는 것이 바람직하다.
② 해시함수는 출력값에 대응하는 입력값을 구하기 어렵다.
③ 해시함수의 내부 알고리즘에 관계없이 충돌저항성을 분석하는 방법으로 생일공격(Birthday Attack)이 있다.
④ 패스워드와 난수를 해시한 값을 전송할 때, 난수가 노출되어도 사전공격(Dictionary Attack)에 안전하다.
⑤ 최근에는 가상화폐인 비트코인(Bitcoin)을 채굴하는 알고리즘에 사용된다.

11. 공개키 암호와 대칭키 암호에 대한 설명으로 옳은 것은?

① 공개키를 교환하기 위해 대칭키 암호를 이용한다.
② 128비트 RSA 공개키와 2048비트 대칭키는 안전도가 비슷하다.
③ 두 암호 모두 기밀성과 무결성을 동시에 보장한다.
④ 긴 메시지 암호화에는 하이브리드 방식의 암호가 효율적이다.
⑤ 공개키 암호는 대칭키 암호에 비해 처리속도가 빠르다.

12. 사용자 인증 방식에 대한 설명으로 옳지 않은 것은?

① 패스워드 인증은 서버 측에서 인증시스템 구축이 용이하다는 장점이 있다.
② 시각 동기화 OTP(One Time Password)는 두 사용자가 사전에 대칭키를 공유해야 한다.
③ 전자서명 방식은 도전-응답(Challenge-Response) 프로토콜과 결합하여 사용자를 인증한다.
④ 생체인증은 생체정보를 인식할 때마다 발생할 수 있는 에러처리가 중요하다.
⑤ I-PIN은 주민등록번호 대신 사용할 수 있는 일회용 사용자 식별번호이다.

13. DNS(Domain Name System)의 보안 위협과 DNSSEC(Domain Name System Security Extensions) 대응에 대한 설명으로 옳지 않은 것은?

① Cache Poisoning 공격은 DNS 캐시에 저장된 정보를 오염시켜 공격자가 지정한 주소로 유도한다.
② DNS Spoofing은 서버에서 응답하는 IP 주소를 변조하여 의도하지 않은 주소로 유도한다.
③ DNSSEC는 서버의 응답에 전자서명을 부가함으로써 서버인증 및 무결성을 제공한다.
④ DNSSEC는 인증체인 형태로 확장되어 계층적 구조의 DNS 서버에도 적용될 수 있다.
⑤ DNSSEC는 서버의 응답을 숨기지는 않지만, 서비스 거부 공격을 막는 효과가 있다.

14. TCSEC(Trusted Computer System Evaluation Criteria)에 따라 보안 등급을 평가할 때 보안 수준이 높은 순서대로 나열한 것으로 옳은 것은?

① Structured Protection > Labeled Security Protection > Controlled Access Protection
② Discretionary Security Protection > Controlled Access Protection > Minimal Protection
③ Minimal Protection > Structured Protection > Labeled Security Protection
④ Discretionary Security Protection > Labeled Security Protection > Minimal Protection
⑤ Controlled Access Protection > Discretionary Security Protection > Structured Protection

15. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① 이메일 보안이나 파일 암호화에 사용된다.
② 공개키 인증을 위해 PGP 인증서를 사용한다.
③ 자신의 공개키를 전달하는 데 인증기관의 서명이 필요하다.
④ 이메일에 서명할 때, 서명자의 패스워드를 요구한다.
⑤ 이메일 관리 프로그램에 플러그인도 가능하다.

16. 자원의 접근제어 방법 중 강제적 접근제어(Mandatory Access Control)에 해당하는 것으로 옳은 것은?

① 자원마다 보안등급이 부여된다.
② 사용자별로 접근권리를 이전할 수 있다.
③ UNIX 운영체제의 기본 접근제어 방식이다.
④ 조직의 역할에 따라 접근권한을 부여하는 방식이다.
⑤ 자원의 소유자가 자원에 대한 접근권한을 설정한다.

17. 다음 용어에 대한 설명으로 옳지 않은 것은?

① Rootkit: 시스템 침입 후의 공격을 도와주는 프로그램들의 집합
② Obfuscation: 코드를 분석하기 어렵도록 변조하는 행위
③ Ransomware: 복호화를 조건으로 금전을 요구하기 위해 피해자의 데이터를 암호화하는 악성코드
④ Cross-Site Scripting: 웹 애플리케이션의 데이터를 악성 스크립트 코드로 변조하는 공격
⑤ Sandbox: 악성코드가 시스템 자원에 쉽게 접근하도록 만든 백도어

18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정한 개인정보의 보호조치로 옳지 않은 것은?

① 개인정보를 안전하게 저장할 수 있는 암호화 기술 등을 이용
② 개인정보에 대한 불법적인 접근을 차단하기 위한 접근 통제장치의 설치
③ 접속기록의 변조 방지를 위한 조치
④ 개인정보를 안전하게 취급하기 위한 내부관리계획의 공개
⑤ 컴퓨터바이러스에 의한 침해 방지 조치

19. 국내 정보보호 관리체계(ISMS) 인증에 관한 평가 기준 중 시스템 개발보안에 대한 통제사항으로 옳지 않은 것은?

① 정보시스템 설계 시 사용자 인증에 관한 보안 요구사항을 고려하여야 한다.
② 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
③ 소스 프로그램은 운영환경에 보관하는 것을 원칙으로 하고, 인가된 사용자만 소스 프로그램에 접근하여야 한다.
④ 개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
⑤ 운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고, 실행코드는 시험과 사용자 인수 후 실행하여야 한다.

20. ISO/IEC 17799와 같은 정보보호 관리체계 표준에서 나열된 보안 통제사항들을 근거로 시스템에 대한 보안 위험을 분석하는 방법으로 옳은 것은?

① 비정형화된 접근법(Informal Approach)
② 기준 접근법(Baseline Approach)
③ 상세 위험 분석(Detailed Risk Analysis)
④ 통합 접근법(Combined Approach)
⑤ 시나리오 접근법(Scenario Approach)