1. 해시함수를 사용하여 변환 가능한 모든 해시값을 계산한 뒤, 이 정보를 사용하여 비밀번호를 공격하는 기법은?
① 무차별 대입(Brute-Force) 공격
② 퍼징(Fuzzing) 공격
③ 알려진 평문(Known Plaintext) 공격
④ 레인보우 테이블(Rainbow Table) 공격

2. 블록 암호의 운용 모드에 대한 설명으로 가장 옳은 것은?
① Electronic Codebook 모드는 초기화 벡터가 필요하다.
② Cipher Feedback 모드는 재전송 공격에 취약하다고 알려져 있다.
③ Cipher Block Chaining 모드는 복호화 과정에서도 암호화 알고리즘이 사용된다.
④ Counter 모드에서 암호문의 중간 부분을 복호화하기 위해서는 해당 부분 이전의 모든 블록들을 복호화해야 한다.

3. Single-Sign On을 실현하기에 적합한 기술로 가장 옳은 것은?
① DTLS ② TLS
③ OCSP ④ Kerberos

4. 방화벽(Firewall), 침입탐지시스템(IDS) 및 침입방지시스템(IPS)에 대한 설명으로 가장 옳지 않은 것은?
① Shodan은 stateful inspection을 수행하는 2세대 방화벽의 일종이다.
② Snort는 대표적인 오픈소스 IPS이다.
③ IPtables는 linux의 패킷 필터 기반 방화벽의 규칙들을 관리하는 도구이다.
④ UFW는 linux에서 사용되는 방화벽 설정 툴이다.

5. <보기>에서 설명하는 것으로 가장 옳은 것은?

<보기>
- 공개적으로 알려진 사이버보안 취약점을 규격화된 목록으로 만들어 식별하는 체계이다.
- 목록에는 취약점의 명칭(일련 번호 포함), 취약성 및 노출 개요, 대응 참조 사항 등이 포함된다.

① Honeypot ② CVE
③ VPN ④ UTM

6. RSA에서 모듈로 연산에 사용되는 n=91이고 어떤 사용자의 비밀키에 사용되는 d=7이라고 할 때, 이 사용자의 공개키에 사용되는 e로 가장 옳은 것은?
① 13 ② 31
③ 41 ④ 존재하지 않는다.

7. IPSec에 대한 설명으로 가장 옳지 않은 것은?
① IPSec은 전송모드와 터널모드로 동작할 수 있다.
② IPSec은 데이터 송신자에 대한 인증과 재전송(Replay) 공격 방지 기능을 제공할 수 있다.
③ IPSec의 키 관리 프로토콜에서는 Diffie-Hellman 기법을 개선한 Oakley 기법을 사용하여 키 교환을 수행할 수 있다.
④ IPSec은 전송 계층인 TCP 계층의 상위 계층인 세션 계층 암호화 기법이므로, 응용 프로그램에 대한 투명성(transparency)을 갖는다.

8. 포맷 스트링(format string) 공격에 대한 설명으로 가장 옳지 않은 것은?
① 취약한 함수를 이용한다는 점에서 버퍼 오버플로우와 공통점이 있으나, 버퍼 오버플로우 공격이 알려지기 훨씬 이전에 발견되었다.
② C 언어의 printf 함수가 대표적인 공격 대상이다.
③ %x 토큰을 적절히 활용하면 공격자는 메모리 내용을 출력하여 확인할 수 있다.
④ %n 토큰을 적절히 활용하면 공격자는 메모리의 내용을 변경할 수 있다.

9. AES에 대한 설명으로 가장 옳은 것은?
① AES-192는 한 번의 수행으로 192비트의 평문 블록을 암호화한다.
② Daemen과 Rijmen이 설계한 Rijndael 알고리즘에 기반한다.
③ 유한체 $GF(2^{256})$ 상의 연산을 이용하여 설계되었다.
④ 치환(substitution) 및 전치(permutation) 연산을 반복하는 페이스텔(Feistel) 구조를 사용한다.

10. <보기>의 설명에 맞는 접근 제어 모델로 가장 옳은 것은?

<보기>
- 정보 소유자가 정보의 보안 수준을 결정하고 이에 대한 접근 권한도 설정할 수 있는 모델이다.
- 이 모델의 대표적인 사례로는 Linux 및 Windows 운영체제에서 파일 시스템 접근 권한을 설정하는 방법이 있다.

① 임의적 접근 제어(Discretionary Access Control) 모델
② 강제적 접근 제어(Mandatory Access Control) 모델
③ 역할기반 접근 제어(Role-Based Access Control) 모델
④ 벨-라파둘라(Bell-LaPadula) 모델

11. DoS공격에 대한 설명으로 가장 옳지 않은 것은?
① HTTP GET Flooding 공격: TCP 3-Way 핸드셰이킹 과정을 통해 공격 대상 시스템에 정상적으로 접속한 뒤 HTTP의 GET Method로 특정 페이지를 무한 실행한다.
② 동적 HTTP Request Flooding 공격: 요청 페이지를 변경하여 웹 페이지를 지속적으로 요청한다.
③ Slow HTTP Header DoS(Slowloris) 공격: 웹 서버에 ID 및 Password, 게시글, 첨부 파일 등을 전송할 때 사용하는 HTTP POST 메시지에서 헤더의 Content-Length 필드에 임의의 큰 값을 설정하여 전송한다.
④ Mail Bomb: 각 사용자에게 할당된 디스크 공간 이상의 메일을 보내 더 이상 메일을 받을 수 없게 하는 공격이다.

12. ElGamal 등과 같이 이산 대수 문제를 기반으로 하는 암호화 기법에서 비밀키로 공개키를 계산할 때 원시근이 사용된다. 사용되는 소수가 13일 때, 원시근으로 사용될 수 있는 값은?
① 6 ② 8
③ 10 ④ 12

13. SSL/TLS에서 레코드 프로토콜의 동작단계로 가장 옳은 것은?
① 압축 → 암호화 → MAC 추가 → 단편화
② 압축 → MAC 추가 → 암호화 → 단편화
③ 암호화 → 단편화 → 압축 → MAC 추가
④ 단편화 → 압축 → MAC 추가 → 암호화

14. 해시 함수에 대한 설명으로 가장 옳지 않은 것은?
① 160비트 길이의 해시 출력값을 갖는 SHA-1 해시 함수는 안전하지 않다고 알려져 있다.
② 키를 갖는 해시함수(Keyed Hash Function)는 메시지 인증 목적으로 사용될 수 있다.
③ 안전한 해시함수는 특정 해시값 h=H(x)를 갖는 x를 찾는 것이 어렵다는 충돌 회피성(collision resistance)을 가져야 한다.
④ NIST에서는 기존의 SHA-2와 원천적으로 다른 구조를 갖는 SHA-3(Keccak)를 표준화하였다.

15. 디지털 서명에 대한 설명으로 가장 옳은 것은?
① 디지털 서명 기법에서 서명의 크기는 원본 데이터의 크기에 비례한다.
② RSA를 사용하는 경우 공개키로 서명하고 개인키로 서명을 검증한다.
③ X.509 인증서에는 공개키를 인증하기 위한 인증기관의 서명이 포함되어 있다.
④ 서명 과정에서 메시지에 해시함수를 적용하면 원본으로 복구가 불가능하므로, 해시함수는 서명에 사용하지 않는 것이 좋다.

16. DB 접근통제 방식 중 <보기>에서 설명하는 것은?

<보기>
네트워크 선로 상의 패킷들을 TAP 방식과 패킷 미러링 방식을 통해 분석 로깅하는 방식으로 사후 감사의 의미에 비중을 두는 보안 방식이다.

① 에이전트 방식 ② 프록시 방식
③ 인라인 방식 ④ 스니핑 방식

17. FTP 서버를 안전하게 운영하기 위한 방법으로 가장 옳은 것은?
① 파일과 사용자에 대한 보안을 위하여 익명(anonymous) FTP로 설정한다.
② 사용자가 본인의 홈디렉터리보다 상위 디렉터리에 접근할 수 있도록 설정한다.
③ 파일 내용이 인가되지 않은 방법으로 수정되지 않도록 Everyone 계정을 제거해야 한다.
④ 출장이나 재택근무 등을 대비하여 모든 IP주소 대역에서 접근할 수 있도록 한다.

18. 소프트웨어 보안 약점 유형에 대한 설명으로 가장 옳은 것은?

① 코드 오류: 의도하지 않은 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안 약점(예: DNS lookup에 의존한 보안결정)

② 에러 처리: 프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안 약점(예: SQL 삽입, XQuery 삽입, LDAP 삽입 등)

③ 시간 및 상태: 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않은 사용자에게 데이터 누출이 가능해지는 보안 약점(예: 잘못된 세션에 의한 데이터 또는 시스템 데이터 정보 노출 등)

④ 보안 기능: 인증, 접근제어, 암호화 등의 기능을 부적절하게 구현 시 발생할 수 있는 보안 약점(예: 부적절한 인가, 하드코드된 암호화키 등)

19. <보기>의 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제2조 발췌문에서 (가)에 들어갈 기관은?

<보기>

"정보보호 및 개인정보보호 관리체계 인증"이란 인증신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 ____(가)____ 또는 인증기관이 증명하는 것을 말한다.

① 국가정보원

② 한국인터넷진흥원

③ 개인정보 보호위원회

④ 과학기술정보통신부

20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 대한 설명으로 가장 옳지 않은 것은?

① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우, 이 접근권한이 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우에는 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실을 이용자에게 알리고 이용자의 동의를 받아야 한다.

② 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우, 이 접근권한이 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우에도 접근권한이 필요한 이유를 이용자에게 알리고 이용자의 동의를 받아야 한다.

③ 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 「전자상거래 등에서의 소비자보호에 관한 법률」로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.

④ 과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 침해사고에 대한 긴급조치를 수행할 수 있다.

이 면은 여백입니다.