1. DES(Data Encryption Standard)에 대한 설명으로 가장 옳은 것은?
① 블록 암호이며, 블록의 크기는 128비트이다.
② 페이스텔(Feistel) 구조 기반이다.
③ 암호화 키는 공개하고, 복호화 키는 공개하면 안 된다.
④ 현재 데이터 암호화에 가장 권장되는 알고리즘이다.

2. 메시지 인증 코드(MAC)와 디지털 서명에 대한 설명으로 가장 옳은 것은?
① MAC의 검증자는 생성에 사용된 비밀키를 공유하고 있으므로, 검증자도 유효한 MAC 값을 생성할 수 있다.
② MAC 값은 검증자의 공개키만으로 생성할 수 있다.
③ 디지털 서명은 서명자와 검증자가 동일한 비밀키를 공유하여야 한다.
④ MAC은 제3자에 대한 부인방지(non-repudiation)를 제공한다.

3. 단순 네트워크 관리 프로토콜(SNMPv1)의 동작에 대한 설명으로 가장 옳지 않은 것은?
① 관리 시스템의 일반적인 정보 요청은 에이전트(agent)의 UDP 161번 포트로 전달되며, 에이전트가 생성한 Trap 메시지는 관리 시스템의 UDP 162번 포트로 전달된다.
② Get Request는 관리 시스템이 에이전트에 특정 정보를 요청할 때 사용한다.
③ Get Next Request는 관리 시스템이 에이전트에 다음 변수의 값을 요청할 때 사용한다.
④ Get Response는 관리 시스템이 에이전트의 특정 변수 값을 변경하도록 요청할 때 사용한다.

4. RSA 암호 시스템에서 두 소수 $p=11$, $q=13$을 사용한다고 할 때, 공개지수 e로 사용할 수 있는 값은?
① 7 ② 12
③ 20 ④ 30

5. 위험 대응 방법에 대한 설명으로 가장 옳은 것은?
① 위험 수용(risk acceptance)은 위험성을 수용하여 추가 보안대책을 설치하는 것이다.
② 위험 전가(risk transference)는 위험한 업무를 수행하지 않음으로써 위험을 전가하는 것이다.
③ 위험 회피(risk avoidance)는 위험한 활동을 수행하지 않는 대신 그 활동의 이익도 포기하는 것이다.
④ 위험 감소(risk reduction)는 보험에 가입하여 사고 손실을 감소시키는 것이다.

6. 접근 제어 모델에 대한 설명으로 가장 옳지 않은 것은?
① 강제적 접근 제어는 관리자가 정의한 규칙과 보안 레이블을 기반으로 접근을 통제하며, 일반 사용자가 접근 통제 규칙을 임의로 변경하기 어렵다.
② Bell-LaPadula 모델에서는 주체가 자신보다 보안 수준이 낮거나 같은 객체를 읽을 수 있고, 자신보다 보안 수준이 높거나 같은 객체에 쓸 수 있다.
③ Biba 모델에서는 주체가 자신보다 무결성 수준이 높거나 같은 객체를 읽을 수 있고, 자신보다 무결성 수준이 낮거나 같은 객체에 쓸 수 있다.
④ 임의적 접근 제어는 사용자의 역할을 기준으로 권한을 부여하므로, 조직이 변경되면 사용자에게 할당된 역할만 변경하여 접근 권한을 조정할 수 있다.

7. ARP 포이즈닝(ARP poisoning)에 대한 설명으로 가장 옳지 않은 것은?
① ARP는 같은 네트워크에서 IP 주소를 MAC 주소로 변환하는 데 사용된다.
② 공격자는 위조된 ARP 응답을 지속적으로 전송하여 호스트의 ARP 테이블을 변경할 수 있다.
③ ARP 요청과 응답에는 기본적으로 강력한 인증과 전자서명 검증이 적용된다.
④ ARP 포이즈닝을 이용하면 공격자가 호스트와 게이트웨이 사이의 통신을 중간에서 가로챌 수 있다.

8. 인증서에 대한 설명으로 가장 옳은 것은?
① 인증기관의 비밀키를 검증하기 위한 기술이다.
② 우리나라에서는 주로 X.509 규격을 사용하고 있다.
③ 인증서가 해킹되어 인증기관이 해당 인증서를 CRL에 추가하고 사용자에게 통지하여도 유효기간까지는 계속 사용 가능하다.
④ 인증서 내부에는 사용자의 비밀키와 공개키 쌍이 저장되어 있다.

9. <보기>에서 설명하는 암호 공격 모델로 가장 옳은 것은?

<보기>

갑은 을이 전송하는 암호 통신을 도청하여 여러 개의 암호문(ciphertext)을 수집하였다. 이후 갑은 을이 매일 전송하는 문서의 평문(plaintext)이 동일한 양식으로 작성되며, 각 평문의 첫 부분이 항상 "DAILY-REPORT:"라는 사실을 알게 되었고, 이를 이용하여 암호키나 나머지 평문에 관한 정보를 추론하려고 한다.

① 암호문 단독 공격(ciphertext-only attack)
② 기지 평문 공격(known-plaintext attack)
③ 선택 평문 공격(chosen-plaintext attack)
④ 선택 암호문 공격(chosen-ciphertext attack)

10. 서비스가 모든 사용자의 비밀번호를 솔트(salt) 없이 SHA-256으로 해시하여 저장하였다. 데이터베이스가 유출되자 동일한 비밀번호를 사용하는 계정들의 해시값이 같았고, 공격자는 미리 계산한 해시 목록을 여러 계정에 반복 적용하였다. 사용자별 솔트를 도입했을 때 기대되는 효과로 가장 옳은 것은?

① 같은 비밀번호의 해시값을 다르게 하여 미리 계산한 결과의 대량 재사용을 어렵게 한다.

② 솔트를 비밀 복호키로 사용하므로, 솔트 값을 알아야 해시값에서 원래 비밀번호를 안전하게 복원할 수 있다.

③ 모든 사용자에게 하나의 고정 솔트를 적용하면 온라인 비밀번호 추측 공격도 완전히 막을 수 있다.

④ 솔트는 비밀번호 길이를 늘리는 암호화 방식이므로 해시함수의 일방향성과는 관련이 없다.

11. IEEE 802.11i 키 구조에서 각 키의 역할에 대한 설명으로 가장 옳은 것은?

① EAPOL-KCK는 GTK를 암호화하여 전송하기 위한 키이다.

② EAPOL-KEK는 RSN 연결 과정에서 GTK 등의 키 자료를 암호화하기 위해 사용된다.

③ TK(Temporal Key)는 EAPOL 메시지의 무결성 검증 및 메시지 인증 코드(MIC) 생성을 위해 사용된다.

④ GTK(Group Temporal Key)는 STA와 AP 간의 유니캐스트(unicast) 데이터를 보호하기 위한 키이다.

12. 포맷 스트링(format string) 공격에 대한 설명으로 가장 옳지 않은 것은?

① 외부 입력값이 검증되지 않은 채 printf() 함수의 포맷 문자열로 사용될 때 발생할 수 있다.

② %x 등의 서식 지정자를 이용하여 스택의 값을 출력하도록 유도할 수 있다.

③ %n 지정자는 출력 전용이므로 메모리 값을 읽을 수는 있으나 변경하는 데는 이용될 수 없다.

④ printf("%s", user_input)와 같이 포맷 문자열을 고정하는 것이 대응 방법이 될 수 있다.

13. TLS 1.2와 비교한 TLS 1.3(RFC 8446)의 특징에 대한 설명으로 가장 옳지 않은 것은?

① 0-RTT 모드가 추가되었다.

② 정적 RSA 키 전송 방식이 제거되었다.

③ ServerHello 다음에 전송되는 핸드셰이크(handshake) 메시지는 암호화된다.

④ 블록 암호의 CBC 운영모드를 사용하는 암호 스위트(cipher suite)를 기본으로 사용한다.

14. 파밍(pharming)에 대한 설명으로 가장 옳은 것은?

① 방어 기술의 하나로 DNSSEC이 있다.

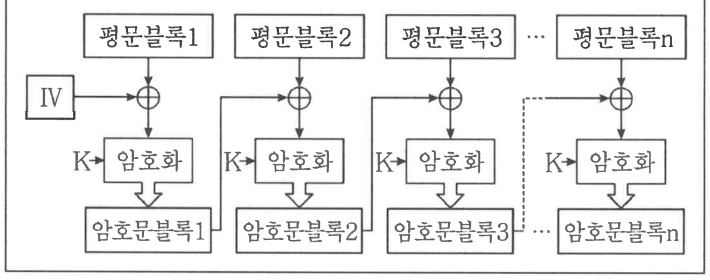
② 서비스 거부 공격의 한 형태이다.

③ 비슷한 도메인 네임(domain name)을 이용하여 다른 웹사이트로 유도하는 기술이다.

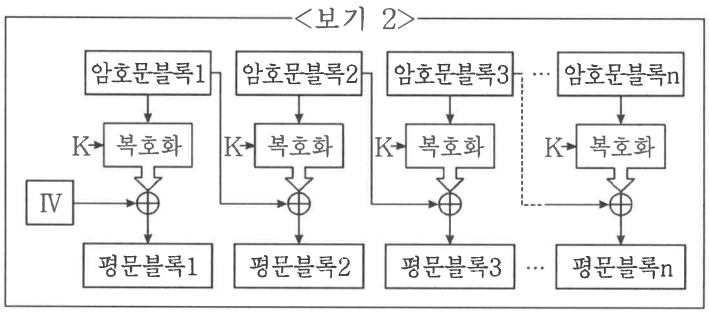
④ 예방을 위하여 비밀번호는 길게 설정하고 대문자와 소문자, 숫자 및 특수문자를 조합해야 한다.

15. <보기 1>과 <보기 2>는 블록 암호 중 암호 블록 체인(cipher block chaining) 모드의 암·복호화 과정이다. 이에 대한 설명으로 가장 옳은 것은? (단, IV는 초기화 벡터(initialization vector), K는 키, ⊕은 XOR 연산이다.)

<보기 1>



<보기 2>



① 공개키 암호에서 사용되는 방식이다.

② 암호화 과정은 무작위 순서로 수행해도 된다는 장점이 있다.

③ 복호화 키가 있으면 바로 전 암호문 블록이 없어도 복호화가 가능하다.

④ 중간의 암호문 블록 하나가 파손되었지만 블록의 길이는 동일하게 유지되고 있다면, 두 개 이하의 블록만 복호화를 실패하고 나머지 블록들은 복호화가 성공적으로 이루어진다.

16. 리눅스의 파일 링크(file link)와 레이스 컨디션(race condition) 공격에 대한 설명으로 가장 옳지 않은 것은?

① 관리자 권한으로 실행되는 프로그램이 임시 파일을 생성하여 처리하는 경우, 공격자가 임시 파일의 이름을 알고 파일 확인과 사용 사이의 시간 간격을 이용하면 레이스 컨디션 공격이 가능할 수 있다.

② 하드 링크(hard link)된 두 파일은 동일한 데이터를 공유하므로 한 파일을 수정하면 다른 파일에도 수정 내용이 반영되며, 한 파일을 삭제하더라도 다른 파일의 데이터는 유지된다.

③ 심볼릭 링크(symbolic link)가 가리키는 원본 파일을 삭제하면 해당 링크를 통해 파일 내용에 접근할 수 없지만, 동일한 경로와 이름으로 파일을 다시 생성하면 기존 심볼릭 링크가 새로 생성된 파일을 가리킬 수 있다.

④ 프로그램이 임시 파일의 존재 여부를 먼저 확인한 후 별도의 단계에서 해당 파일에 접근하면, 확인한 파일과 실제 접근하는 파일의 동일성이 보장되므로 그 사이에 심볼릭 링크로 교체되더라도 프로그램의 처리 결과에는 영향을 주지 않는다.

17. <보기>는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의3의 일부이다. (가)와 (나)에 들어갈 기관을 옳게 짝지은 것은?

<보기>

제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 __(가)__ 이나/나 __(나)__ 에 신고하여야 한다. 이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.

	(가)	(나)
①	과학기술정보통신부장관	한국인터넷진흥원
②	방송통신위원회	한국인터넷진흥원
③	개인정보보호위원회	한국지능정보사회진흥원
④	국가정보원장	금융보안원

18. <보기>에서 공격자가 사용한 공격 기법으로 가장 옳은 것은?

<보기>

공격자는 목표 인공지능 모델의 내부 파라미터(parameter)와 학습 데이터에는 접근할 수 없으나, 목표 모델에 입력을 질의하고 그에 대한 예측 결과를 얻을 수 있다. 공격자는 대량의 입력을 질의하여 얻은 입력-분류 결과 쌍을 학습 데이터로 사용하여, 목표 모델의 기능을 모방하는 대체 모델(substitute model)을 학습하였다. 이후 공격자는 목표 모델에 대한 추가 질의를 보내거나 API 사용료를 지불하지 않고도, 대체 모델을 이용해 목표 모델과 유사한 서비스를 자체적으로 제공할 수 있었다.

① 데이터 오염 공격(data poisoning attacks)
② 멤버십 추론 공격(membership inference attacks)
③ 모델 추출 공격(model extraction attacks)
④ 모델 역전 공격(model inversion attacks)

19. <보기>의 기준 URL과 출처(origin)가 동일한 URL은?

<보기>

기준 URL: https://example.com/account/index.html

① http://example.com/account/list.html
② https://example.com/profile/list.html
③ https://shop.example.com/account/index.html
④ https://example.com:8443/account/index.html

20. 병원 A와 병원 B는 각 기관이 보유한 환자의 가명정보를 결합하여 대학 연구팀과 질병 통계 연구를 수행하려 한다. 연구 도중 한 참여자는 결합된 정보에 연락처를 추가해 특정 환자를 찾아내어 건강상품 홍보에도 활용하자고 제안하였다. 「개인정보 보호법」상 가장 옳은 것은?

① 가명처리를 거치면 목적 제한이 사라지므로 연구와 상품 홍보 모두에 정보주체의 동의가 필요하지 않다.
② 내부 규정에 따른 승인 절차를 거친 경우, 가명결합 후 재식별은 허용될 수 있다.
③ 연구 목적의 가명정보 처리는 가능하며, 각 병원이 보유한 가명정보의 결합은 전문기관을 통해 수행해야 한다.
④ 가명정보를 제3자에게 제공할 때에는 재식별에 필요한 정보를 함께 제공해야 한다.