2018년 교행 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
②	②	④	③	④	①	③	②	③	③
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
①	②	②	①	④	②	④	①	①	③

1. 다음 설명을 모두 만족하는 정보보호의 목표는?

> ◦ 인터넷을 통해 전송되는 데이터 암호화
> ◦ 데이터베이스와 저장 장치에 저장되는 데이터 암호화
> ◦ 인가된 사용자들만이 정보를 볼 수 있도록 암호화

① 가용성 ② 기밀성
③ 무결성 ④ 신뢰성

답 ②

② 암호화는 기밀성을 보장하기 위한 대표적인 보안 방법이다.
기밀성(Confidentially)은 권한이 없는 사용자에겐 정보가 노출되지 않아야 한다는 것이다.

<오답 체크> ① 가용성(Availability): 권한이 있는 자는 서비스를 사용하여야 함

③ 무결성(Integrity): 데이터가 위·변조되지 않아야 함

2. 다음은 신문기사의 일부이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

> ㉠ 은(는) 하나의 PC로 제어되는 대규모 온라인 기기 모음이며, 악성 소프트웨어를 이용해 빼앗은 다수의 좀비 컴퓨터로 구성되는 네트워크라고 볼 수 있다. 일반적으로 PC, 공유기, 스마트 폰, 웹캠, 태블릿 등을 악성코드에 감염시켜 사용한다. ㉠ 은(는) 특정 온라인 서버를 표적으로 다운시키거나 대규모 스팸 캠페인을 전달하는 DDoS 공격에 사용할 수 있다. 또한 사용자는 자신의 기기에 있는 악성코드를 인식하지 못하기 때문에 사생활 침해 사기에 개인 정보를 쉽게 도용당할 수 있다.
>
> — 2017년 ○월 ○일자 —

① 웜(worm)
② 봇넷(botnet)
③ 루트킷(rootkit)
④ 랜섬웨어(ransomware)

답 ②

② **봇넷**(botnet)
악성코드 등에 감염되어 소유자 모르게 해커의 명령을 받아 사이버 범죄에 동원되는 좀비PC들로 구성된 네트워크

✠ DDoS 공격에서 공격자는 악성코드를 통해 다수의 시스템을 감염시켜 좀비PC로 만든 뒤, 그 다수의 좀비PC를 이용해 공격 대상 시스템에 많은 양의 트래픽을 보내 시스템 자원을 고갈시키는 공격을 감행한다. 공격 대상 시스템은 여러 곳으로부터 공격을 받기 때문에, 공격의 근원지를 찾기 매우 어려워진다.

<오답 체크> ① 컴퓨터 웜(computer worm)
스스로를 복제하는 컴퓨터 프로그램이다. 다른 프로그램에 기생하지 않고 독자적으로 실행되며 네트워크를 통해 자신의 복사본을 전파할 수 있다.

③ **Root Kit**(루트킷)
해커들이 컴퓨터나 또는 네트웍에 침입한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득하는데 사용하는 도구의 모음이다.

④ **랜섬웨어**(Ransomware)
인질의 몸값을 뜻하는 ransom과 제품을 뜻하는 ware의 합성어로, 컴퓨터에 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.

3. 다음 스푸핑(spoofing) 공격에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

(가) 공격 대상이 잘못된 IP 주소로 웹 접속 유도
(나) 권한 획득을 위하여 다른 사용자의 IP 주소 강탈
(다) MAC 주소를 속여 클라이언트에서 서버로 가는 패킷이나 그 반대 패킷의 흐름을 왜곡

	(가)	(나)	(다)
①	IP 스푸핑	ARP 스푸핑	DNS 스푸핑
②	ARP 스푸핑	IP 스푸핑	DNS 스푸핑
③	ARP 스푸핑	DNS 스푸핑	IP 스푸핑
④	DNS 스푸핑	IP 스푸핑	ARP 스푸핑

답 ④

(가) **DNS Spoofing**(DNS 스푸핑)
공격 대상자가 접속하려는 URL 주소 이름을 요청할 때, 거짓 IP 주소를 반환하여 사용자가 의도하지 않은 주소로 접근하게 만드는 공격이다.
DNS 스푸핑을 하는 방법에는 스니핑을 통해 DNS 서버보다 빨리 거짓 응답을 사용자에게 전달하는 방법, 대상자의 PC에 저장된 host파일을 수정하는 방법, DNS 서버가 가진 IP 주소 자체를 변조시키는 방법 등이 있다.

(나) **IP Spoofing**(IP 스푸핑)
단말 사이가 IP 주소 기반의 트러스트 관계일 경우 인증 절차를 생략한다는 취약점을 이용한 공격으로, 공격자가 자신의 IP를 다른 사람의 IP로 속여 다른 사람 행세를 하는 것이다.
공격자는 클라이언트의 IP주소를 확보하여 서버에 패스워드 없이 접근이 가능해지며, 서비스 거부 공격이나 세션 차단 등의 공격에도 사용된다.

(다) **ARP Spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.
공격자는 클라이언트와 서버 사이의 패킷을 읽고 확인한 후 정상적인 목적지로 향하도록 다시 돌려보내 연결이 유지되도록 한다.

4. 리눅스 시스템에서 침해사고 분석 시 wtmp 로그파일에서 확인할 수 있는 정보로 <보기>에서 옳은 것만을 모두 고른 것은?

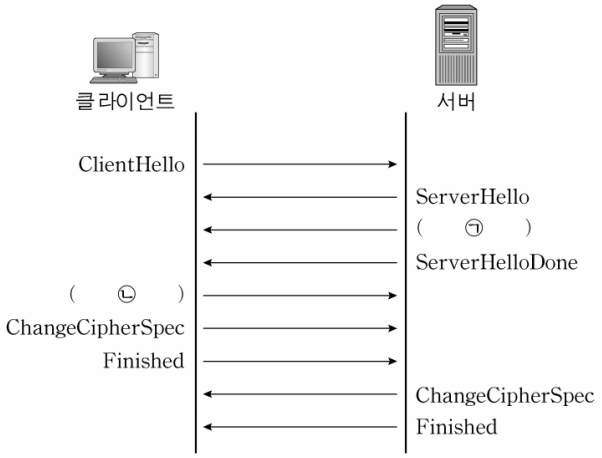
ㄱ. 재부팅 시간 정보
ㄴ. 사용자의 로그인/로그아웃 정보
ㄷ. 로그인에 실패한 사용자의 IP 주소

① ㄱ ② ㄴ
③ ㄱ, ㄴ ④ ㄱ, ㄴ, ㄷ

답 ③

ㄱ. ㄴ. wtmp 로그는 로그인/로그아웃에 대한 정보를 기록한다.
사용자들의 로그인/로그아웃 내역을 누적 형태로 저장하며, 시스템의 셧다운, 부팅 내역까지 포함하고 있다.
'last' 명령을 이용하여 그 내용을 확인할 수 있다.
<오답 체크> ㄷ. 실패한 로그인 시도 정보를 담고 있는 로그 파일에는 btmp, loginlog, failedlog 파일이 있다.

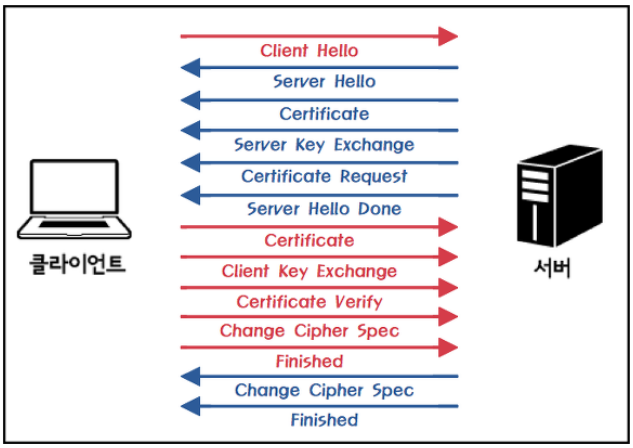
5. 그림은 SSL/TLS에서 상호인증을 요구하지 않는 경우의 핸드쉐이크(handshake) 과정이다. ㉠, ㉡에 들어갈 SSL/TLS 메시지를 바르게 짝지은 것은?



㉠	㉡
① ClientRequest	ClientHelloDone
② ServerKeyExchange	ClientHelloDone
③ ClientKeyExchange	ServerKeyExchange
④ ServerKeyExchange	ClientKeyExchange

답 ④

◈ **SSL**(Secure Sockets Layer, 보안 소켓 레이어) 또는 **TLS**(Transport Layer Security, 전송 계층 보안)
응용 계층과 전송 계층 사이에서 통신 과정에서 종단간 보안과 클라이언트와 서버 간 상호 인증, 기밀성, 무결성 서비스를 제공하는 보안 프로토콜



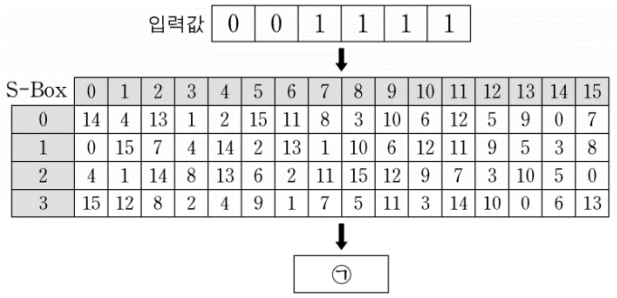
1) **Client Hello** (Client -> Server)
자신이 사용할 SSL의 버전정보, Cipher suite list, 클라이언트 난수를 생성해서 보낸다

2) **Server Hello** (Client <- Server)
암호화 방법을 선택하고 서버난수를 생성해서 보낸다
3) Server Certificate (Client <- Server)
4) **Server Key Exchange** (Client <- Server)
클라이언트는 클라이언트와 서버의 난수를 각각 사용해 PMS(Pre-Master Secret) 값을 생성한다
PMS를 서버의 공개키로 암호화해서 서버에게 보내면 서버는 개인키를 사용해 해당 암호문을 복호화한다.
5) **Certificate Request** (Client <- Server)
클라이언트에게 인증서를 요구한다.
6) **Server Hello Done** (Client <- Server)
서버가 클라이언트에게 보낼 메시지를 모두 보냈음을 의미한다.

7) **Client Certificate** (Client -> Server)
8) **Certificate Verify** (Client -> Server)
클라이언트가 인증서를 개인키로 암호화(전자서명)하여 전송하고 서버는 클라이언트의 공개키를 사용하여 확인한다.
해당 메시지를 통해서 서버는 클라이언트의 인증서의 공개키가 유효한지 확인한 후 클라이언트 인증을 마친다
9) **Client Key Exchange** (Client -> Server)
클라이언트는 PMS, Client 난수, Server 난수 세 값을 이용해 암호화 키와 메시지 인증 코드용 공유키를 생성한다

10) **Change Cipher Spec** (Client <-> Server)
이후에 전송되는 모든 메시지는 서버와 협상된 알고리즘과 키를 이용해 암호화하겠다고 서버에 알린다
11) **Finished** (Client <-> Server)
클라이언트와 SSL서버간의 SSL 핸드쉐이크를 종료한다

6. 그림은 DES(Data Encryption Standard)에서 S-Box를 통과하는 과정이다. 입력 값이 001111(2)일 때 출력 비트 ㉠은?



S-Box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

① $0001_{(2)}$ ② $0010_{(2)}$
③ $0110_{(2)}$ ④ $0111_{(2)}$

답 ①

DES에서 S-Box는 6비트 입력값을 받아 4비트 출력값을 출력한다.
6비트 입력 중 앞·뒤 1번째와 6번째 비트가 행의 값
가운데 2, 3, 4, 5번째 비트가 열의 값이다.

S[0] ($X_0, X_1, X_2, X_3, X_4, X_5$) -> (Y_0, Y_1, Y_2, Y_3) 에서
밑줄이 없는 ' X_0 X_5 ' 가 행의 값
밑줄 친 ' X_1, X_2, X_3, X_4 ' 가 열의 값이다.

문제에서 입력값 S[0]: (0, 0, 1, 1, 1, 1) 이므로
행 01 = 1
열 0111 = 7

S-Box에서 행 3, 열 7에서 출력값을 찾으면 1이 된다.

S[0] (0, 0, 1, 1, 1, 1) = 1 = **$0001_{(2)}$**

7. 블록암호 운영모드 중 CTR(counter) 모드에 대한 설명으로 <보기>에서 옳은 것만을 모두 고른 것은?

〈 보 기 〉
ㄱ. 운영모드에서 시프트 레지스터를 사용한다.
ㄴ. 패딩이 필요 없으며 평문 블록과 키 스트림을 XOR 연산하여 암호문을 생성한다.
ㄷ. 암호화는 각 블록에 독립적으로 적용되기 때문에, 블록 단위 에러 발생 시 해당 블록에 영향을 준다.

① ㄱ ② ㄱ, ㄴ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

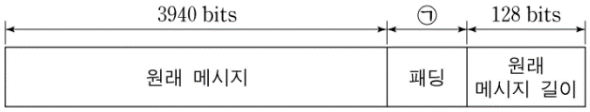
답 ③

ㄴ. **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.
또한 CFB, OFB, CTR 모드는 패딩이 필요 없다.

ㄷ. CTR 모드에서 각각의 블록들은 독립적으로 처리가 가능하기 때문에 병렬 처리가 가능하며 오류 전파가 없다.

<오답 체크> ㄱ. 시프트 레지스터를 사용하는 모드는 **CFB**(cipher feedback, 암호 피드백) 모드이다.
CFB 모드는 CBC의 변형으로, 이전 단계의 암호문 블록을 암호화한 후 현재의 평문 블록과 XOR 한다. 첫 번째 평문 블록의 경우에는 초기화 벡터(IV)를 암호화한 것과 XOR 한다.

8. 해시함수 SHA-512를 이용하여 해시값을 구하려고 한다. 원래 메시지가 3940 비트일 때, 그림에서 ㉠ 패딩의 비트 수는?



① 24 ② 28 ③ 32 ④ 36

답 ②

- 패딩(padding)이란 블럭 단위의 암호화 알고리즘에서 평문을 블록 크기에 맞춰 나누어야 하는데, 평문이 블록의 배수가 아닐 때 부족한 길이만큼 임의의 비트열로 채워 블록의 배수로 만드는 과정이다.
  SHA-512 알고리즘은 1024비트 블록 단위로 처리한다. 따라서 전체가 1024의 배수가 되도록 패딩하면 된다.

  원래 메시지 3940비트 + 원래 미시지 길이 128비트이므로, 현재 길이는 4068비트이다.

  1024 X 3 = 3072
  1024 X 4 = 4096

  4블록으로 나누기 위해 4096비트로 만들어야 하므로,
  4096 - 4068 = **28 비트를 패딩**하면 된다.

- '원래 메시지 길이 128비트'라는 부분은, 패딩하기 전 원래 메시지의 길이를 기록해두는 부분이다.
  패딩을 하기 전 원래 메시지의 길이가 몇 비트였는지 기록해두어, 어디까지가 원문 메시지이고 어디부터가 패딩된 비트열인지 구분이 가능하다.

9. 데이터베이스 서버와 어플리케이션 서버로 분리하여 운용할 경우, 데이터베이스 암호화 방식 중 암·복호화가 데이터베이스 서버에서 수행되는 방식으로 <보기>에서 옳은 것만을 모두 고른 것은?

> ㄱ. API 방식
> ㄴ. 플러그-인 방식
> ㄷ. 필터(filter) 방식
> ㄹ. TDE(Transparent Data Encryption) 방식

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄹ ④ ㄴ, ㄷ, ㄹ

답 ③

ㄴ. **플러그 인**(Plug-In) (컬럼 단위 암호화)
애플리케이션단이 아닌 DBMS 자체에 플러그인 방식으로 암·복호화 모듈을 설치해 운영하는 방식.
애플리케이션으로부터 독립성을 제공하므로 응용 프로그램의 수정이 적다. 모든 작업이 GUI 기반으로 이루어져 관리 편의성이 높고 암호화 컬럼에 대한 일치검색, 범위검색 인덱스 지원이 용이하다.
하지만 DB 서버에 직접적인 부하가 발생해 성능이 저하된다.

ㄹ. **TDE**(Transparent Data Encryption) 방식 (블록 단위 암호화)
응용 프로그램의 수정 없이 DB 내부에서 칼럼, 테이블스페이스 레벨의 암호화를 하여, 암호를 풀 수 있는 암호화 키를 DB 서버에 파일 형태로 두는 방식.
속도가 빠르고 애플리케이션을 수정하지 않아도 된다.
하지만 DB 서버에 과부하가 많이 걸리고, DB 서버 해킹 시 키가 유출될 수 있으며, 키 관리가 어렵다.

<오답 체크> ㄱ. **API** 방식 (컬럼 단위 암호화)
DB단이 아닌 외부 애플리케이션 영역에서 암·복호화를 수행하는 방식.
DB 외부에서 암·복호화가 수행되므로, 암·복호화 수행시에도 DB 서버에 부하가 걸리지 않는다.
하지만 DB 내부에서 수행되는 연산 처리 과정에서 암호화한 데이터 처리가 불가능하고 DB 내부에서 업무 처리가 필요한 경우 별도의 DBMS API 모듈이 필요하다. 또한 암호화 대상 데이터와 관련된 모든 소스 영역의 수정이 필요하다.

ㄷ. **필터**(filter) 방식
독립된 프로세스로 구동하여 애플리케이션과 DBMS 중간에서 암·복호화를 처리하는 방식으로, API 방식과 동일하게 애플리케이션 서버에서 암·복호화를 처리한다. JAVA기반의 애플리케이션에서 소스 수정 없이 암·복호화를 할 수 있다.
하지만 등록된 SQL만 암·복호화가 가능하여, 암·복호화 대상이 되는 SQL의 수집 및 변경이 필요하다.
암·복호화 작업을 수행하는 Agent를 별도의 서버에 탑재하여 암·복호화 작업을 수행하는 것이 가능하다.

◈ **이외 DB 암호화 방식**

✠ 하이브리드 방식 (컬럼 단위 암호화)
성능이 우선시 되는 환경에서는 API를 적용하고, 성능 영향이 덜 민감한 환경에는 플러그 인 방식을 적용하는 방식
하지만 구축 투자 비용이 상대적으로 높다는 단점이 있다.

✠ **File** 방식 (블록 단위 암호화)
DB 파일을 통째로 암호화하는 방식
응용프로그램의 수정이 없다.
하지만 통째로 암호화하기 때문에 암호화가 필요없는 부분까지 암호화를 수행해 전반적인 성능 저하가 야기되고, 접근제어, 감사 이력 등이 지원이 안 되기 때문에 별도의 접근제어 솔루션을 도입해야 한다.

✠ **Secure Proxy** 방식
독립된 프로세스로 구동하여 애플리케이션과 DBMS의 중간에 위치하여 암호화하는 방식으로, 플러그 인 방식과 동일하게 DBMS에서 암·복호화를 수행하나 뷰 또는 트리거를 사용하지 않고 암·복호화 함수를 사용하여 테이블의 데이터를 입력 또는 조회할 수 있다.
DB 서버 부하 등을 보완하기 위해 암·복호화 작업을 수행하는 Agent를 별도의 서버에 탑재하여 암·복호화를 수행하는 것이 가능하다.

✠ **인 플레이스**(In-Place) 방식
플러그 인 방식에서 더 나아가 DB 엔진 내부에서 암·복호화 기능을 수행하는 방식.
애플리케이션 환경에서 완벽한 독립성을 제공하고 플러그 인 방식보다 더 빠른 암호화 성능을 제공한다.
하지만 암호화 이외의 접근제어, 보안감사 등 DB 보안 기능 지원을 위해 별도의 패키지를 사용해야 하는 단점이 있다.

10. 다음의 개인정보보호법 제17조 ①항에 따라 개인정보처리자가 정보주체의 개인정보를 수집한 목적범위 안에서 제3자에게 제공할 수 있는 경우로 <보기>에서 옳은 것만을 모두 고른 것은?

> **제17조(개인정보의 제공)** ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다

〈 보 기 〉

ㄱ. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

ㄴ. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

ㄷ. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

① ㄱ ② ㄷ

③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

답 ③

개인정보보호법 제17조에 의거, 개인정보를 제3자에게 제공할 수 있는 경우는 정보주체의 동의를 받거나, 제15조 제1항의 2호·3호·5호에 해당하는 경우이다. **(1호·4호·6호는 안 된다)**

ㄴ. 제15조 제1항 제3호에 해당하여 옳은 경우이다.

ㄷ. 제15조 제1항 제2호에 해당하여 옳은 경우이다.

<오답 체크> ㄱ. 제15조 제1항 제4호에 해당하여 옳은 경우가 아니다.

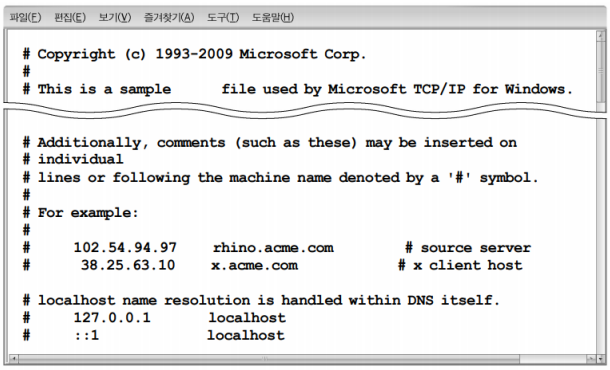
제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

11. 그림은 DNS 보다 우선 적용되는 파일로, 해커는 이 파일을 변조하여 파밍(pharming)에 사용할 수 있다. 이 파일명으로 옳은 것은?



① hosts ② networks
③ protocol ④ services

답 ①

① hosts 파일에는 사용자가 방문했던 사이트들의 ip주소와 도메인명의 쌍이 들어있다.
사용자가 웹 브라우저에 도메인을 입력하면 시스템은 우선 hosts 파일을 검색하여 해당하는 도메인이 있을 경우 그 IP 주소를 응답한다. hosts 파일에 해당 도메인이 없을 경우, DNS 서버에 요청을 하여 해당 IP주소를 반환 받고, 그 정보를 시스템의 host파일에 기록한다.
따라서 사용자가 올바른 도메인을 입력하여도 가짜 사이트로 접속을 유도하는 파밍 공격은 이 hosts 파일을 변조하는 것과 관련련이 있다.

<오답 체크> ④ services 파일에는 네트워크 서비스 이름과 그와 함께 사용할 포트 번호/프로토콜 유형의 쌍이 들어있다.
ex) telnet(텔넷) 23/TCP

DNS Spoofing(DNS 스푸핑) 공격
공격 대상자가 접속하려는 URL 주소 이름을 요청할 때, 거짓 IP 주소를 반환하여 사용자가 의도하지 않은 주소로 접근하게 만드는 공격이다.
DNS 스푸핑을 하는 방법에는 스니핑을 통해 DNS 서버보다 빨리 거짓 응답을 사용자에게 전달하는 방법, 대상자의 PC에 저장된 hosts파일을 수정하는 방법, DNS 서버가 가진 IP 주소 자체를 변조시키는 방법 등이 있다.

12. 다음 설명을 모두 만족하는 공개키 기반구조 (PKI)의 구성요소는?

> ◦ LDAP을 이용하여 X.500 디렉터리 서비스 제공
> ◦ 인증서와 사용자 관련 정보, 상호 인증서 쌍, CRL 등을 저장하고 검색하는 데이터베이스

① 사용자(user)
② 저장소(repository)
③ 등록기관(registration authority)
④ 인증기관(certification authority)

답 ②

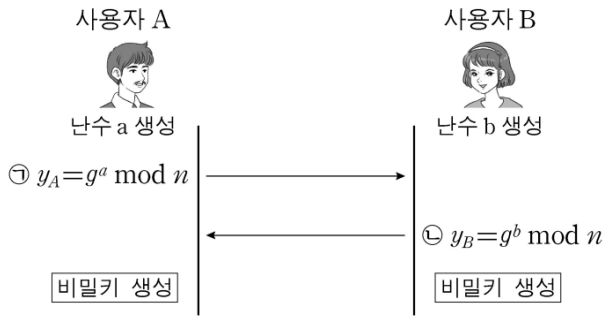
② **저장소**(Repository)
공개된 저장소 역할 (저장 및 검색 등)
DAP 및 LDAP 등을 이용하여 X.500 디렉터리 서비스를 제공

<오답 체크> ③ **등록 기관**(RA, Registration Authority)
인증기관과 사용자 사이에서 사용자 신분 확인, 인증서 발급을 중개, 전달한다.
신원확인, 고객데이터 유지 등 인증기관의 확인 업무를 대행하며, 사용자의 인증서 발급 요청을 등록한다.

④ **인증 기관**(CA, Certification Authority)
공개키 인증서와 인증서 폐기목록을 생성하고 발급한다.
공개키에 대한 공신력있는 인증기관

(주의! 13번과 14번 순서 바꿈)

[13 ~ 14] 그림은 Diffie-Hellman의 키 교환 방법이다. 다음 그림을 보고 물음에 답하시오.



14. 위 그림에서 사용자 A, B가 생성하는 비밀키 값과 동일한 값을 구하는 식은? (단, mod는 나머지를 구하는 연산자이고, Φ(n) 는 오일러의 Totient 함수이다.)

① $g^{a \times b} \bmod n$ ② $g^{a+b} \bmod n$

③ $g^{a \times b} \bmod \Phi(n)$ ④ $g^{a+b} \bmod \Phi(n)$

답 ①

✠ 디피 헬만 키 교환 순서

1. 앨리스가 충분히 큰 소수 p와 g를 선택하여 밥에게 전송한다. g는 1부터 p-1 사이의 수이다.
2. 앨리스가 정수 a를 선택한다. 이 정수는 외부에 공개되지 않으며, 밥 또한 알 수 없다.
3. 앨리스가 $A = g^a \bmod p$, 즉 g^a를 p로 나눈 나머지를 계산한다.
4. 밥이 마찬가지로 정수 b를 선택하여 $B = g^b \bmod p$ 를 계산한다.
5. 앨리스와 밥이 서로에게 A와 B를 전송한다.
6. 앨리스가 $B^a \bmod p$를, 밥이 $A^b \bmod p$를 계산한다.
   $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$
   $A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$

   이로써 앨리스와 밥은 공통의 비밀키 $g^{ab} \bmod p$ 를 갖게 된다.

13. 위 그림의 식 ㉠, ㉡에서 *n* 이 7일 때, *g* 로 사용할 수 있는 것은?

① 2 ② 3 ③ 4 ④ 7

답 ②

많은 이론서와 인터넷 백과 사전 등에 따르면 g는 1과 p-1 사이의 정수라고만 나와 있다.(문제에서 p 대신 n이 쓰였다)

그런데 2018년 국가직 시험 디피 헬만 알고리즘 문제를 보면 '소수 p와 **p의 원시근 g**에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고...' 라고 서술 되어 있다.
따라서 g는 p의 원시근에 해당하며, 곧 이 문제는 p의 원시근을 구하는 문제이다.
(문제에서는 n = 7의 원시근을 구하는 것)

과연 전산직을 준비하는 수험생 중 원시근이 무엇인지, 어떻게 구하는지 아는 수험생은 거의 없을 것이다. 따라서 이 문제는 n이 7일 때, g는 7보다 작은 정수라고 알고, ④번은 답이 아니겠으니 나머지 셋 중에서 찍고 넘어가면 충분하다.

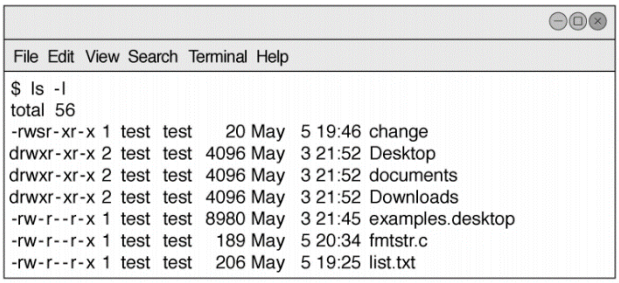
풀이) 소수 n에 대한 원시근을 검증해보면, a^k mod n = 1 을 만족하는 최소의 k가 n-1일 때의 a값을 n의 원시근이라고 한다.
따라서 a^k mod 7 = 1 을 만족하는 최소의 k가 6일 때의 a값을 찾으면 된다.

① 2^2 mod 7 = 4 mod 7 = 4
2^3 mod 7 = 8 mod 7 = 1
mod 7 = 1 을 만족하는 최소의 k가 3이므로 2는 7의 원시근이 아니다.

③ 3^2 mod 7 = 9 mod 7 = 2
3^3 mod 7 = 27 mod 7 = 6
3^4 mod 7 = 81 mod 7 = 4
3^5 mod 7 = 243 mod 7 = 5
3^6 mod 7 = 729 mod 7 = 1
mod 7 =1 을 만족하는 최소의 k가 6이므로 **3은 7의 원시근에 해당한다.**

④ 4^2 mod 7 = 16 mod 7 = 2
4^3 mod 7 = 64 mod 7 = 1
mod 7 = 1 을 만족하는 최소의 k가 3이므로 4는 7의 원시근이 아니다.

15. 그림은 리눅스에서 ls – l 명령을 실행한 결과이다. change 파일에 대한 설명으로 옳은 것은?



① change 파일은 setGID 비트가 설정되어 있다.
② change 파일의 접근 권한을 8진수로 표현하면 754 이다.
③ test 외의 사용자는 change 파일에 대해 쓰기 권한을 가진다.
④ change 파일은 test 외의 사용자가 실행할 때 유효 사용자 ID(effective UID)는 test가 된다.

답 ④

④ change 파일의 실행 권한을 보면 권한이 rwsr-xr-x 로 설정되어 있다.
실행 권한 rwxr-xr-x 에서 소유자의 실행 권한이 x 대신 s 로 쓰여있는 것을 볼 수 있다.
이것은 이 파일에 **setUID(Set UserID)가 설정**되어 있다는 것이다. 파일에 setUID가 설정되어 있으면, 사용자들은 해당 파일을 실행하는 동안 그 파일의 소유자(또는 그룹)의 권한을 가지게 된다. 이 파일의 소유자는 test이므로, 파일을 실행하는 동안 사용자들은 유효 아이디 test를 갖게 된다.

<오답 체크> ① setUID가 설정되어 있다.

② 접근 권한을 8진수로 표현할 때 특수 권한은 소유자 권한의 앞자리에 표시한다.
setUid 설정은 소유자 권한 앞자리에 4로 표기한다.
(setGid 설정은 2, Sticky bit(스티키 비트) 설정은 1
setUID와 setGID 동시에 설정되어 있을 시 4 + 2 = 6)

rwxr-xr-x는 8진수로 755로 표시되므로,
위 문제에서 setUID가 설정이 된 rwsr-xr-x는 앞에 4를 붙여 **4755**로 표시한다.

③ 권한이 rwxr-xr-x 이므로, 소유자 이외에는 쓰기(w) 권한이 없다.

16. AES(Advanced Encryption Standard) 알고리즘에서 사용되는 함수들이다. 암호화 과정의 마지막 라운드 에서 수행되는 함수를 <보기>에서 옳은 것만을 모두 골라, 호출 순서대로 바르게 나열한 것은?

〈 보 기 〉
ㄱ. SubBytes( ) /* 바이트 치환 */
ㄴ. ShiftRows( ) /* 행 이동 */
ㄷ. MixColumns( ) /* 열 혼합 */
ㄹ. AddRoundKey( ) /* 라운드 키 더하기 */

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

답 ②

② AES는 각 단계에서 바이트 치환(SubBytes), 행 이동(ShiftRows), 열 혼합(MixColumns), 키 덧셈(AddRoundKey)의 4단계를 거친다.
단, 마지막 단계에서는 열 혼합을 제외한 3단계만 수행한다.

◈ **AES**(Advanced Encryption Standard)
SPN구조
블록 128비트(16바이트)
키 길이 128비트 – 10라운드
키 길이 192비트 – 12라운드
키 길이 256비트 – 14라운드

17. 네트워크 기반 침입탐지시스템(Intrusion Detection System)의 특징에 대한 설명으로 <보기>에서 옳은 것만을 모두 고른 것은?

> ㄱ. 어플리케이션 서버에 설치되어 관리가 간단하다.
> ㄴ. 네트워크상의 패킷을 분석하여 침입을 탐지한다.
> ㄷ. 방화벽 내부의 내부 네트워크와 방화벽 외부의 DMZ에 모두 배치 가능하다.

① ㄱ ② ㄴ
③ ㄱ, ㄷ ④ ㄴ, ㄷ

답 ④

ㄴ. 네트워크 기반 IDS(NIDS)는 네트워크 트래픽을 감시하는 역할을 수행한다.
ㄷ. NIDS는 방화벽 내부 외무 모두 설치가 가능하다.
<오답 체크> ㄱ. 어플리케이션 서버에 설치되는 것은 호스트 기반 IDS(HIDS)이다.

◈ **NIDS**(Netw ork IDS, 네트워크 기반 침입 탐지 시스템)
네트워크 트래픽을 감시하고 패킷을 분석하는 IDS 시스템
서비스 거부 공격(DoS 공격), 포트 스캔, 컴퓨터를 크랙하려는 시도 등과 같은 악의적인 동작들을 탐지하는 IDS 시스템
별도의 호스트에 설치

◈ **HIDS**(Host IDS, 호스트 기반 침입 탐지 시스템)
네트워크 트래픽이 아닌, 컴퓨터 시스템의 동작이나 상태 등 컴퓨터 시스템의 내부를 감시하고 분석하는 데 더 중점을 두는 IDS 시스템
기존 서버에 설치되며, 별도의 호스트가 필요 없다.

18. 다음 설명을 모두 만족하는 OTP(One-Time Password) 생성 방식은?

> ◦ 해시체인 방식으로 계산된다.
> ◦ 생성된 일회용 패스워드의 사용 횟수가 제한된다.
> ◦ 검증 시 계산량이 적기 때문에 스마트카드와 같은 응용에 적합하다.

① S/KEY 방식
② 시간 동기화 방식
③ 이벤트 동기화 방식
④ Challenge-Response 방식

답 ①

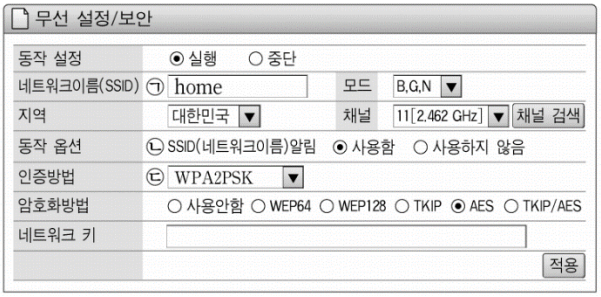
① **S/KEY 방식**
해시 체인에 기반하여 OTP를 생성하는 방식이다.
클라이언트에서 정한 임의의 비밀키를 서버로 전송하여, 해시 알고리즘을 통해 해시값을 구하는 작업을 n번 반복하고, 그렇게 생성된 n개의 OTP를 서버에 저장한다.
일회용이므로 재사용할 수 없으며, 그 다음 인증을 위해서는 그 전에 전송된 값보다 해시 함수가 한 번 적게 적용된 값을 사용해야 하는데, 해시의 일방향성 특징에 따라 그 값을 유추하는 것은 매우 어렵다.

<오답 체크> ② **시간 동기화 방식**
OTP를 생성하기 위해 사용하는 입력 값으로 시간을 사용하는 방식이다. 클라이언트는 현재 시각을 입력값으로 OTP를 생성해 서버로 전송하고, 서버 역시 같은 방식으로 OTP를 생성하여 클라이언트가 전송한 값의 유효성을 검사한다.

③ **이벤트 동기화 방식**
서버와 클라이언트가 카운트 값을 동일하게 증가시켜 가며, 해당 카운트 값을 입력값으로 OTP를 생성해 인증하는 방식이다.

④ **Challenge-Response 방식**
서버에서 난수 생성 등을 통해 임의의 수를 생성하여 클라이언트에 전송하면, 클라이언트가 그 값으로 OTP를 생성해 응답한 값으로 인증하는 방식이다.

19. 그림은 무선 AP(Access Point)를 설정한 결과 화면의 일부이다. ㉠~㉢에 대한 설명으로 옳지 않은 것은?



① ㉠의 'home'은 관리자가 변경할 수 없다.

② ㉡을 '사용함'으로 설정하였기 때문에, 클라이언트의 무선 네트워크 연결 목록에서 'home'을 볼 수 있다.

③ 무선 네트워크 연결 목록에서 'home'을 볼 수 없게 하여 접속시도를 줄이려면, ㉡을 '사용하지 않음'으로 설정을 변경한다.

④ ㉢을 'WPA2PSK'로 설정하였기 때문에, '암호화 방법'으로 AES를 사용할 수 있다

답 ①

① 무선 단말기의 SSID는 사용자가 임의로 변경하는 것이 가능하다.

<오답 체크> ②③ SSID 알림이 설정되어 있으면, 범위 안에 있는 사용자는 누구든 해당 AP를 검색하는 것이 가능하다.
스마트폰 와이파이 설정 메뉴에 연결가능한 공유기가 와이파이 목록이 표시되는데, 이것들이 SSID 알림이 설정되어 있는 AP들이다.

④ WPA2 방식은 암호화를 위해 AES-CCMP를 사용한다.

○ **WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용

○ **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용

○ **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증

20. 그림은 C 언어 소스코드의 일부이다. 이 소스코드 ㉠~㉣에서 오버플로우 취약점을 가진 행은?

```
#include 〈stdio.h〉
#include 〈stdlib.h〉
#include 〈string.h〉
#define BUFSIZE 10
int main(int argc, char **argv)
{
    char *dest = NULL ;  ------------------  ㉠
    dest = (char *)malloc(BUFSIZE);  -------  ㉡
    strcpy(dest, argv[1]);  -----------------  ㉢
    free(dest);
    return 0 ;  ---------------------------  ㉣
}
```

① ㉠ ② ㉡ ③ ㉢ ④ ㉣

답 ③

③ strcpy()는 오버플로우 공격에 취약한 함수이다.
그래서 오버플로우 공격에 대비해 **strncpy()**를 사용하길 권장한다.

✠ **버퍼 오버플로우 공격에 취약한 함수**
strcpy(), strcat(), gets(), getw d(), scanf(), fscanf(), sscanf(), vscanf(), vsscanf(), realpath(), sprintf(), vsprintf(), gethostbyname() 등

✠ **버퍼 오버플로우 공격에 안전한 함수**
strncpy(), strncat(), fgets(), fscanf(), vfscanf(), snprintf(), vsnprintf() 등