2018년 서울시 7급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

1. 해시 알고리즘의 특징에 대한 설명으로 가장 옳은 것은?

① 해시 값이 같으면서 입력 값이 서로 다른 충돌 쌍을 찾는 것은 계산상 불가능하다.
② 고정길이의 입력 메시지를 임의 길이의 출력 값으로 압축시킨 함수이다.
③ 주어진 해시 값 y에 대해서 hash(x)=y 식을 만족하는 x를 찾는 것이 계산적으로 가능하다.
④ 메시지의 거대화 방지 및 데이터의 은닉에 사용된다.

답 ①

① 해시 알고리즘의 특징 중 강한 충돌 내성(strong collision resistance)에 대한 설명이다.
(= 충돌 저항성 = 충돌 회피성)
출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없어야 한다.

<오답 체크> ② 대부분의 해시 함수는 가변 길이의 입력을 받아, 고정 길이의 값을 출력한다.

③ 해시값 y에 대해서 hash(x)=y 식을 만족하는 x(원본 메시지)를 찾는 것이 계산적으로 불가능해야 한다.(일방향성 = 역상 저항성)

④ 해시 알고리즘은 데이터 무결성을 보장하기 위해 사용할 뿐, 데이터 은닉(기밀성) 기능은 없다.

2. 소프트웨어 취약점 공격에 해당하지 않는 것은?

① 버퍼 오버플로우 공격
② 힙 버퍼 오버플로우 공격
③ 크로스 사이트 스크립팅 공격
④ 웹 세션 하이재킹

답 ④

④ 세션 하이재킹은 네트워크 취약점을 이용한 공격에 해당한다.

○ **세션 하이재킹**(Session Hijacking) 공격
서버에 연결중인 공격대상의 세션을 가로채 인증 절차를 거치지 않고 서버에 접속하여, 자신이 공격 대상인 척 행세하는 공격이다.

<오답 체크> ① **버퍼 오버플로우**(buffer overflow) 공격
프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.

② 힙 버퍼 오버플로우 공격
힙 데이터 영역에서 발생하는 버퍼 오버플로우 공격이다. 힙 영역은 프로그램 실행 중 필요에 의해 동적으로 할당되는 데이터 영역을 말한다.

③ **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)는 웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.
XSS 공격은 온라인을 통해 이루어지는 공격이라 소프트웨어 취약점을 이용한 공격이 아니라고 생각할 수도 있는데, 사용자 웹 브라우저에서 악성코드가 실행되는 것이 컴퓨터 시스템의 취약점을 이용하는 것이다. 컴퓨터가 소프트웨어적으로 취약점이 없다면, 아무리 악성코드를 많이 심어놓더라도 실행되지 않는다.

3. 메시지 송수신 상황에서 <보기>의 조치를 취했을 경우에 지켜질 수 있는 정보보호 서비스로 옳은 것끼리 짝지어진 것은?

> 〈 보 기 〉
> 송신자 앨리스는 밥에게 보낼 메시지를 먼저 자신의(앨리스) 개인키로 암호화하였다. 이렇게 암호화된 암호문을 수신자인 밥의 공개키로 한 번 더 암호화를 한 뒤에 수신자인 밥에게 보냈다.

① 무결성, 인증, 부인방지
② 기밀성, 무결성, 부인방지
③ 기밀성, 무결성, 인증, 부인방지
④ 무결성, 인증, 가용성, 부인방지

답 ③

앨리스가 자신의 개인키로 암호화
-> 자신이 보냈다는 걸 증명하는 전자 서명에 해당한다. 여기에서 지켜질 수 있는 서비스는 **인증, 무결성, 부인방지**이다.
앨리스가 수신자인 밥의 공개키로 암호화
-> 아무나 보지 못하도록 숨기는 암호화에 해당한다. 여기에서 지켜질 수 있는 서비스는 **기밀성**이다.
<오답 체크> ④ 가용성은 정당한 권한이 있는 사용자가 서비스를 이용할 수 있어야 한다는 것을 말하며, 가용성을 지키기 위한 방법으로는 데이터 백업 및 복원이 있다.

4. 공인인증서에 대한 설명으로 가장 옳은 것은?

① 공인인증서는 공개키와 소유자를 연결시켜주는 전자문서로 오늘날 사용되는 대부분의 인증서는 X.509 인증서(버전3)를 표준으로 따른다.
② 공인인증서의 기본 영역은 버전, 일련번호, 서명 알고리즘, 발급자, 주체, 주체키 식별자, 기관 정보 액세스, 키 사용 용도, 인증서 정책 등을 포함하고 있다.
③ 누구나 사용자의 인증서를 획득하고, 공개키를 획득할 수 있으며 누구나 자유롭게 인증서를 수정/발급할 수 있다.
④ 인증서 폐기 목록은 보통 폐기된 인증서에 관한 정보만 유지하는데, 이를 나쁜 목록(bad-list) 방법이라고 한다. 나쁜 목록 방법은 좋은 목록(good-list) 방법보다 안전하지만 상대적으로 용량이 매우 크다.

답 ①

① X.509는 공인인증서 관련한 표준이며, 대부분의 인증서가 이 표준을 따르고 있다.
<오답 체크> ② 주체키 식별자, 기관 정보 액세스, 키 사용 용도, 인증서 정책은 인증서 확장 영역에 해당한다.

◈ **인증서의 기본 영역**
(1) **버전** (2) **일련번호**
(3) **서명 알고리즘** (4) **발급자**
(5) **유효기간** (6) **주체**
(7) **공개키**

◈ **인증서의 확장 영역**
(1) **기관 키 식별자** (2) **주체 키 식별자**
(3) **주체 대체 이름** (4) CRL **배포 지점**
(5) **기관 정보 액세스** (6) **키 사용 용도**
(7) **인증서 정책** (8) **손도장 알고리즘**
(9) **손도장**

③ 인증서 발급은 인증 기관(CA)이 담당한다.
④ 인증서 폐기 목록은 용량과 속도, 효율성 때문에 대부분 나쁜 목록(bad-list) 방법을 사용한다. 다만 나쁜 목록 방법은 좋은 목록 방법에 비해 상대적으로 안전성이 떨어진다.
건물에 출입하는 인원을 통제할 때, 출입증을 가진 인원만 허용하는 경우(good-list)와 위험 인물로 등록된 인원을 제외한 모두를 허용하는 경우(bad-list) 중 어느 경우가 더 안전한지를 생각해보면 된다. 나쁜 목록 방법에서는 아직 위험 인물로 알려지지 않은 경우는 통제할 수 없기 때문이다.

5. 보안 등급 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)에 대한 설명으로 가장 옳은 것은?

① E1~E6까지 6등급으로 구분한다.
② 기밀성, 무결성, 가용성을 평가한다.
③ 유럽의 신뢰성 있는 컴퓨터 시스템 평가기준이다.
④ 각 클래스별로 기능 요구사항과 보증 요구사항을 정의·포함한다.

답 ④

<오답 체크> ① TCSEC은 A1~D으로 구분하며, E6(최고)~E1(최저)까지 6등급으로 구분하는 것은 ITSEC이다.
② TCSEC은 기밀성을 중심으로 평가하며, 기밀성과 무결성, 가용성까지 평가하는 건 ITSEC이다.
③ TCSEC은 미국의 정보보호 시스템 평가 제도이며, 유럽의 정보보호 시스템 평가 제도는 ITSEC이다.

6. <보기>의 패킷 로그가 검출된 공격은?

〈 보 기 〉
Source: 203.211.11.11
Destination: 203.211.11.11
Protocol: 6
Src Port: 21845
DST Port: 21845

① Teardrop
② Land attack
③ Ping of Death
④ SYN flooding

답 ②

② 패킷 로그를 보면 출발지(Source) IP 주소와 목적지(Destination) IP 주소가 같은데, 이것은 Land 공격을 당했다는 얘기다.

◈ **Land 공격**(Land Attack)
패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격자의 IP 주소 값으로 만들어 전송하는 공격이다. 출발지 주소와 목적지 주소가 같기 때문에 이 패킷의 응답 은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가는데, SYN Flooding처럼 동시 사용자 수를 점유해버리며 CPU 자원을 고갈시킨다.

<오답 체크> ① **Teardrop**
패킷의 순서번호가 중복되도록 조작하는 공격이다.
목표 대상 시스템은 이렇게 보내진 패킷들을 재조합하려고 시도하지만, 계속 실패하여 시스템 자원이 고갈되어 서비스 불능 상태에 빠진다.

③ **Ping of Death**
icmp 패킷을 정상보다 매우 크게 만들어 공격하는 DoS 공격이다.
크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

④ **SYN flooding**(SYN 플러딩)
TCP 3-way hancshaking을 이용한 DoS공격
공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

7. 유럽의 정보보호 전문기관인 ENISA(European Network and Information Society Agency)에서 분류한 SNS 관련 보안 위협 중 <보기>에서 설명하는 것으로 가장 옳은 것은?

〈 보 기 〉
· SNS를 이용한 스팸 증가
· 크로스 사이트 스크립팅 및 웜 · 바이러스 등에 대한 취약성 증가
· 다양하게 통합되는 SNS 포털들이 정보수집기로 이용되어 보안 취약성이 증가

① 프라이버시 보안 위협
② 네트워크 상의 보안 위협
③ ID 관련 보안 위협
④ 사회적 위협

답 ②

② 보기의 내용은, SNS에서 공격 대상의 관심사를 파악한 뒤, 공격 대상이 관심 가질 만한 정보에 바이러스나 악성 코드를 숨겨 스팸을 보내거나, 악성 코드를 삽입한 게시물로 유인하여 악성 코드에 노출되게 만드는 XSS 공격 등을 의미한다. 이것들은 네트워크 상의 보안 위협에 해당한다.
ENISA에서 분류한 보안 위협과 세부 항목들을 보면 각 항목들이 애매하거나 정확히 분류가 이해되지 않는 부분들이 있으니 주의해야 한다.

▷ 프라이버시 위협
- 개인프로파일 수집
- 2차 데이터 수집
- 얼굴 인식
- 콘텐츠 기반 이미지 검색
- 완전한 계정 삭제의 어려움

▷ 기존 네트워크 보안 위협
- SNS 스팸
- XSS, 웜, 바이러스

▷ ID 관련 위협
- SNS를 이용한 피싱
- 네트워크 침입을 통한 정보유출
- ID 도용에 의한 프로파일 위조 및 명예훼손

▷ 사회적 위협
- 사이버 스토킹
- 사이버 괴롭힘
- 산업스파이

8. 정보보안의 위험 관리 과정에서 조직의 보안 요구사항에 대한 효과적인 식별 및 효율적인 위험의 감소를 실현하기 위해 세부적인 위험 분석 방법들이 존재한다. <보기>에서 설명하는 ㈎에 해당하는 위험 분석 방법으로 가장 옳은 것은?

〈 보 기 〉
㈎은 모든 시스템에 대하여 표준화된 보안 대책을 제시하며 체크리스트 형태로 보안 대책이 있는지 없는지를 판단하여 적용되어 있지 않은 보안대책을 적용하는 방법으로 수행하는 위험 분석 방법

① 비정형 접근법
② 복합 접근법
③ 상세위험 분석
④ 베이스라인 접근법

답 ④

④ **기준선 접근법**(베이스라인 접근법)은 보호 대책에 대한 항목별로 체크리스트를 작성해 평가하는 방법으로, 국제정보보호관리체계, 정보보호관리체계(ISMS), 개인정보보호관리체계(PIMS) 등과 같은 인증 심사 때 많이 사용한다.

<오답 체크> ① **비정형 접근법**은 구조적인 체계 없이 컨설턴트의 경험과 지식을 이용하여 위험 분석을 하는 접근법이다.

② **통합 접근법**(복합 접근방법)은 고위험 영역은 상세 위험분석을 수행하고, 그 외 영역은 기준선 접근법을 사용한다.

③ **상세 위험 분석 접근법**은 자산 식별, 위협 분석, 취약점 분석을 단계별로 수행하여 위험을 분석하는 방법이다.

9.「개인정보 보호법 시행령」에서 규정한 개인정보 영향평가 대상에 대한 설명으로 가장 옳지 않은 것은?

① 5만 명 이상의 정보주체에 대한 민감 정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
② 내부 또는 외부에서 구축·운용하는 다른 개인정보파일과 연계하려는 경우, 연계 결과 10만 명 이상의 정보주체에 관한 개인정보파일
③ 100만 명 이상의 정보주체에 관한 개인정보파일
④ 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하는 경우, 변경된 부분

답 ②

②「개인정보 보호법 시행령」 제35조 제2항
다른 개인정보파일과 연계하려는 경우로서 **연계 결과 50만명 이상**의 정보주체에 관한 개인정보파일
<오답 체크> ①「개인정보 보호법 시행령」 제35조 제1항
③「개인정보 보호법 시행령」 제35조 제3항
④「개인정보 보호법 시행령」 제35조 제4항

「개인정보 보호법 시행령」

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 **5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보**의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 **구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상**의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. **구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상**의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 **변경된 부분으로 한정**한다.

「개인정보 보호법」

제33조(개인정보 영향평가)

① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.
② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.
1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항
③ 행정안전부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.
④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.
⑤ 행정안전부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.
⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.
⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

10. <보기>에서 설명하는 포렌식(Forensic)의 기본 원칙에 해당하는 것으로 가장 옳은 것은?

〈 보 기 〉

증거는 획득하고 난 뒤 '이송·분석·보관·법정 제출'이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능 해야 한다. 이를 만족하려면 증거를 전달하고 전달받는 데 관여한 담당자와 책임자를 명시해야 한다.

① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 무결성의 원칙

답 ③

◈ 포렌식의 원칙
▷ **재현**의 원칙
증거를 복구하는 과정에서 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함
▷ **정당성**의 원칙
모든 증거는 적법한 절차를 거쳐서 획득하여야 함
▷ **신속성**의 원칙
시스템 안의 디스크 또는 메모리 정보가 휘발되기 전에 빠르게 획득하여야 함
▷ **연계보관성**의 원칙
증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 함
▷ **무결성**의 원칙
증거가 위조/변조되어서는 안 됨

11. <보기>에서 설명하고 있는 시스템 관련 보안으로 가장 옳은 것은?

〈 보 기 〉

시스템은 계정과 패스워드 관리, 권한 관리, 접근 제어 등의 다양한 시스템 관련 보안 기능을 충분히 갖추고도 보안적인 문제가 발생할 수 있는데, 이는 컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 운영체제 설계상의 허점으로 인한 것이다. 이러한 시스템 자체의 결함을 체계적으로 관리하는 통합적인 개념이다.

① 세션 관리 ② 로그 관리
③ 취약점 관리 ④ 패치 관리

답 ③

③ 보안 기능을 충분히 갖추고도 발생할 수 있는, 시스템 자체의 문제점을 관리하는 것은 **취약점 관리**이다.

◈ 시스템 보안
▷ 계정과 패스워드 관리
권한을 가진 사용자 식별을 위한 가장 기본적인 인증 수단
시스템에서는 계정과 패스워드 관리가 보안의 시작
▷ 세션 관리
활성화된 접속에 대한 관리
비인가자에 의한 세션 가로채기를 통제
▷ 접근 제어
네트워크 안에서 다른 시스템으로부터 보호되도록 접근통제
▷ 권한 관리
사용자가 적절한 권한으로 정보 자산에 접근할 수 있도록 통제
▷ 로그 관리
시스템 내부/외부에서 시스템에 미치는 사항을 기록
▷ 취약점 관리
잘 구성된 시스템 보안 하에서도 문제 발생 가능함
이는 시스템 자체의 결함에 의한 것으로, 이를 체계적으로 관리하는 것이 취약점 관리

12. 악성코드에 대한 설명으로 가장 옳은 것은?

① 바이러스(virus)는 다른 프로그램을 감염시키지는 않지만 네트워크를 통해 자기 복제를 하며 전파된다.
② 트로이목마(Trojan horse)는 자기 복제 능력은 없으면서 정상적인 기능을 하는 프로그램 속에 숨어서 정보를 빼내거나 사용자 PC를 원격으로 제어할 수 있게 한다.
③ 애드웨어(adware)는 사용자의 브라우저를 원하지 않은 사이트로 이동시키면서 팝업창을 띄운다.
④ 드로퍼(dropper)는 사용자의 동의를 얻어 설치되었으나 프로그램 목적과 상관없이 시작 페이지 변경, 광고 노출, 과도한 리소스 사용으로 시스템 성능 저하를 가져오거나 존재하지 않는 위험을 가지고 사용자를 위협하여 결제를 유도한다.

답 ②

② ▷ **트로이목마**(Trojan Horse)
정상적인 프로그램으로 가장한 악성 프로그램으로, 다른 시스템으로 전파되지는 않는다. 트로이목마는 보통 해커들이 대상 컴퓨터의 인증이나 백신을 우회하여 시스템 내부에 침투하기 위해 사용한다.

<오답 체크> ① 웜에 대한 설명이다.
바이러스는 스스로 복제하여 다른 프로그램을 감염시킨다.

③ **하이재커**(Hijacker)
의도치 않은 사이트로 이동을 시키고 팝업창을 띄우는 악성 소프트웨어

▶ **애드웨어**(Adware)
광고를 포함한 소프트웨어를 말한다.
사용자에게 광고를 보여줌으로써 프로그래머는 소프트웨어 개발 비용을 충당할 수 있고, 사용자는 무료 또는 저렴한 가격으로 프로그램을 이용할 수 있게 만들어준다. 따라서 악성코드가 아닌 합법적인 애드웨어도 있다.
하지만 이러한 애드웨어가 무분별하게 사용자의 동의 없이 컴퓨터에 설치되어 광고 화면을 무분별하게 띄워 불편을 초래하는 악성코드가 될 수 있다.

④ 가짜 백신 프로그램
백신 소프트웨어를 사칭하여, 사용자 컴퓨터의 성능을 저하시키고 오작동을 일으켜 컴퓨터에 악성코드가 감염되었다는 거짓 내용을 띄워서 사용자를 속여 결제하게끔 하는 경우가 많다. 랜섬웨어가 가짜 백신 프로그램을 겸하는 경우도 있다.

▶ **드로퍼**(Dropper)
파일 자체 내에는 악성코드가 없으나, 파일 실행 시 바이러스를 다운받아 악성코드를 실행하고 사용자 시스템을 감염시키는 형태의 프로그램

13. <보기>에서 설명하는 정보 은닉 기술로 가장 옳은 것은?

〈 보 기 〉
비밀 정보를 기존의 이미지 파일, 음악 파일, 동영상 파일 등에 숨겨서 전송하는 정보 은닉(information hiding) 기술의 일종이다. 이 기술은 저작권 보호보다는 정보를 은밀하게 전달하기 위한 목적이 크다.

① 워터마크(watermark)
② 스테가노그래피(steganography)
③ 스파이웨어(spyware)
④ 섀도(shadow)

답 ②

② **스테가노그래피**(steganography)
보통의 데이터에 또 다른 정보나 데이터를 보이지 않게 삽입하는 기술

<오답 체크> ① **워터마크**(watermark)
콘텐츠에 저작권자의 정보를 삽입하여, 불법 유출시 원본과 출처에 대한 정보를 추적할 수 있도록 해주는 기술

③ **스파이웨어**(Spyware)
사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어로, 신용 카드와 같은 금융 정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집하는 기능을 한다.

④ **섀도 데이터**(shadow data)
다양한 클라우드 프로그램들이 빠르게 도입되고, 직원들 개개인이 조직의 승인을 받지 않은 프로그램이나 데이터를 취급하는 경우가 늘어나면서, IT 담당 직원들조차 회사 내에서 다른 직원들이 어떤 데이터를 수집하고 관리하는지 알 수 없게 되었다. IT 관리자들이 파악하지 못한 이러한 데이터들을 섀도 데이터라고 한다. 섀도 데이터는 정보관리자가 통제하지 못하여, 조직의 보안 시스템에 위험요소가 될 수 있다.

14. 이메일 보안의 사실상의 표준으로 사용되고 있는 PGP (Pretty Good Privacy)에 대한 설명으로 가장 옳은 것은?

① RSA, DSA 등의 알고리즘을 사용한 디지털 서명을 통해 보낸 사람에 대한 인증과 부인방지 기능을 제공한다.
② AES, IDEA 등의 대칭키 암호화 알고리즘을 사용하여 이메일의 내용이 외부에 노출되는 것을 방지하는 기밀성은 제공하나, 이메일의 내용이 전송 중에 변경되지 않았다는 무결성은 보장하지 못한다.
③ PGP는 송신자의 대용량 이메일을 작은 메시지로 분할하지 않고 수신자에게 전송한다.
④ PGP는 이메일의 내용만 암호화하고, 첨부되는 문서는 암호화하지 못하여 다른 기법을 추가로 사용해야 한다.

답 ①

① **PGP**(Pretty Good Privacy)는 전자우편 서비스에 대한 보안 기술로, 인증기관을 사용하지 않고 개개인의 신뢰 관계를 이용하여 인증하는 방식이다.
PGP는 RSA 버전과 Diffie-Hellman 버전 등이 있다.
RSA 버전에서는 전체 메시지를 암호화하는데 사용되는 짧은 키의 생성을 위해 IDEA 대칭키 알고리즘을 사용하며, 짧은 키를 암호화하기 위해 RSA 공개키 알고리즘를 사용한다.
Diffie-Hellman 버전은 전체 메시지를 암호화하기 위한 짧은 키를 위해 CAST 대칭키 알고리즘을 사용하며, Diffie-Hellman 알고리즘을 사용해 짧은 키를 암호화하기 위한 키를 생성한다.
PGP는 대칭키 암호화 단독 방식뿐 아니라, 대칭키와 공개키를 같이 사용하는 하이브리드 암호화 방식 또한 지원하여 기밀성, 인증, 무결성에 부인방지 기능까지 지원한다.

<오답 체크> ② PGP는 기밀성, 인증, 무결성에 부인방지 기능까지 지원한다.

③ 전자메일은 보통 최대 메시지 길이에 제한이 있다.(50,000byte) 따라서 PGP에서도 50,000byte 이상의 메시지를 단편화하여 전송한다.

④ PGP는 첨부파일까지 암호화할 수 있다.

15. <보기>에서 설명하는 시스템 공격에 해당하는 것으로 가장 옳은 것은?

〈 보 기 〉

2014년 4월에 발견된 오픈 소스 암호화 라이브러리인 OpenSSL의 소프트웨어 버그로 전 세계 웹 사이트 가운데 2/3 정도가 사용하는 OpenSSL에서 발견된 치명적인 결함을 말한다. 이 공격은 주로 아이디, 비밀번호, 주민등록번호 등 개인정보와 SSL 서버 비밀키, 세션키, 쿠키 등을 탈취한다.

① 스쿨버스
② 루트킷
③ 하트블리드 공격
④ 무차별 공격

답 ③

③ **하트블리드**(HeartBleed)
2014년 4월 OpenSSL 1.0.1 버전에서 발견된 매우 심각한 버그
OpenSSL을 구성하고 있는 TLS/DTLS의 HeartBeat 확장규격에서 발견된 취약점으로, 해당 취약점을 이용하면 서버와 클라이언트 사이에 주고받는 정보들을 탈취할 수 있다.

<오답 체크> ① **스쿨버스**(School Bus)
전형적인 트로이목마 해킹툴로서 백오리피스(BackOrifice)나 넷버스(NetBus)처럼 강력하면서 사용하기도 쉬운 프로그램이다.
서버 파일과 클라이언트 파일로 이루어져 있으며, 서버파일이 상대방 컴퓨터에 설치되어 있어야만 클라이언트 파일을 이용하여 서버파일이 설치된 컴퓨터를 원격 조정할 수 있다.
스쿨버스를 이용해 상대방 컴퓨터의 자료를 빼오거나 손상시키는 것 등의 피해를 줄 수 있다.

② **루트킷**(RootKit)
해커들이 컴퓨터나 또는 네트웍에 침입한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득하는데 사용하는 도구의 모음이다.

④ **무차별 공격**(Brute Force Attack)
특정 패턴을 사용하지 않고, 패스워드로 사용 가능한 모든 문자열, 숫자열을 대입해가는 공격 방법이다.

16. 위협(Threats), 취약성(Vulnerability), 자산가치(Asset Value), 위험(Risk)의 상관관계 표현으로 가장 옳은 것은?

① 위험=자산가치/위협×취약성
② 위험=위협/취약성×자산가치
③ 위험=위협×취약성/자산가치
④ 위험=위협×취약성×자산가치

답 ④

④ 위험은 자산가치와 위협, 취약성의 곱으로 표시할 수 있다.
위협이 증가하면 위험도 커지고, 취약성이 증가해도 위험이 커지고, 자산가치가 증가해도 위험이 커진다. 위협, 취약성, 자산가치 모두 위험과 정비례 관계에 있으므로 모두 곱으로 표시할 수 있다.

17. 컴퓨터 및 네트워크에서 서비스가 더 이상 진행되지 못하도록 하는 경우로써 <보기>에서 설명하고 있는 공격 방법으로 가장 옳은 것은?

〈 보 기 〉
- 핑(ping)을 사용하여 현재 동작 중인 노드가 에코 메시지를 보내게 한다.
- 공격자가 발신주소를 공격하고자 하는 목적지의 IP 주소로 위장하여 ICMP 에코 메시지를 요청하여 다량의 패킷이 목적지로 전송되도록 한다.
- 목표시스템은 과부하가 발생하여 정상적인 서비스가 불가능하게 된다.

① 스머프(smurf) 공격
② 중간자(man-in-the-middle) 공격
③ 포맷 스트링(format string) 공격
④ 프래글(fraggle) 공격

답 ①

① **Smurf**(ICMP flooding) 공격
출발지 IP주소를 공격대상의 IP주소로 위장하여 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상으로 많은 양의 ICMP Echo 응답 패킷이 몰리게 만들어 시스템 자원이 고갈되도록 만드는 공격이다.

<오답 체크> ② **중간자**(Man-In-The-Middle, MITM) 공격
연결하는 두 송수신자 사이에 중간자가 침입하여 한쪽에서 전달된 정보를 도청한 뒤 이를 다른 쪽에 전달하는 공격이다.
두 송수신자는 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며, 중간자는 해당 정보를 도청만 한 뒤 그대로 보낼 수도 있고, 조작하여 보낼 수도 있다.

③ **Format String**(포맷 스트링) 공격
결과를 출력하기 위하여 사용되는 printf() 함수에서 지시자를 제대로 지정하지 않아 의도적으로 버그를 발생시켜, 메모리의 특정 위치의 값을 다른 것으로 변경시키는 공격이다. 해커는 이렇게 포맷 스트링의 취약점을 악용해 시스템의 권한을 획득하거나 특정 동작을 수행하게 만든다.

④ **프래글**(fraggle) 공격
Smurf와 유사하지만 ICMP대신에 UDP를 사용한다.
공격자는 확장 네트워크에서 출발지 IP 주소가 공격 대상 IP 주소로 위조된 UDP 패킷을 브로드캐스트하여, UDP 패킷의 응답이 공격 대상 시스템에 몰리게 하여 시스템을 마비시키는 공격이다.

18. <보기>에서 설명하고 있는 APT(Advanced Persistent Threats) 공격 기법으로 가장 옳은 것은?

〈 보 기 〉

조사된 정보를 바탕으로 정보시스템, 웹 어플리케이션 등의 알려지지 않은 취약점 및 보안시스템에서 탐지되지 않는 악성코드 등을 감염시키는 것이다. 해당 취약점에 의해 악성 코드에 감염된 PC는 동일한 취약점을 보유하고 있는 PC를 스캔하여 감염시킨다

① 사전조사(Reconnaissance)
② 사회 공학(Social engineering)
③ 제로데이(Zero-day) 공격
④ 적응(Adaption)

답 ③

③ **제로데이**(Zero Day) 공격
운영체제나 소프트웨어의 보안 취약점이 아직 알려지지 않아 업데이트 패치가 나오기 전에, 그 취약점을 이용하여 공격하는 방법

◈ APT공격 절차
1. **사전조사**(Reconnaissance)
해커가 표적으로 정한 공격대상을 분석하고 공격방법을 연구하는 등 최종 목표를 위하여 1차 침입 대상을 찾는 것으로, 주요 직원, 관리자, 사원 등 정보에 직·간접으로 접근할 수 있는 대상자를 찾는 과정
2. **제로데이**(Zero Day) 공격
운영체제나 소프트웨어의 보안 취약점에 대한 업데이트 패치가 나오기 전에, 그 취약점을 이용하여 공격하는 방법
3. **사회공학적**(Social engineering) 공격
기술적인 방법이 아닌 사람들간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법을 일컫는다.
4. **은닉**(Covert)
1차 침입에 성공한 후 내부 정상적인 사용자로 가장하여 현재 계정이 갖는 권한 내에서 얻을 수 있는 모든 정보를 수집
5. **권한 상승**(Privilege Escalation)
은닉을 통해 각종 정보를 수집 후 시스템에 접근하기 위해 접근 권한을 가진 계정 정보를 수집
6. **적응**(Adaption)
목표 시스템(DB, 개인정보, 관리자계정 등)에 접근한 뒤, 역추적을 방지하며 계속해서 정보를 유출하는 행위
7. **지속**(Persistent)
중요정보 유출 이후에도 해커가 공격대상에 지속적으로 접근할 수 있도록 다양한 백도어(Backdoor)를 설치하는 등의 행위

19. 전자정부 소프트웨어 개발 시 비밀번호를 설계할 때 고려해야 할 사항으로 가장 옳지 않은 것은?

① 패스워드를 설정할 때 한국인터넷진흥원『암호이용안내서』의 패스워드 설정규칙을 적용해야 한다.
② 패스워드 저장 시 솔트(salt)가 적용된 안전한 해시함수를 사용해야 하며 해시함수 실행은 클라이언트에서 해야 한다.
③ 네트워크를 통해 패스워드를 전송하는 경우 반드시 패스워드를 암호화하거나 암호화된 통신 채널을 이용해야 한다.
④ 패스워드 재설정·변경 시 안전하게 변경할 수 있는 규칙을 정의해서 적용해야 한다.

답 ②

② 해시함수 실행은 클라이언트가 아니라 서버에서 해야 한다.

비밀번호 관리

▶ 안전한 비밀번호 조합규칙(비밀번호 길이, 허용문자 조합 등)을 설정하고, 안전한 저장 정책, 재설정 및 변경 정책, 패스워드 관리규칙(주기적 변경 등)이 적용되도록 설계해야 한다.

① 패스워드를 설정할 때 한국인터넷진흥원의『암호이용안내서』의 패스워드 생성규칙을 적용해야 한다.
② 네트워크를 통해 패스워드를 전송하는 경우 반드시 패스워드를 암호화하거나 암호화된 통신 채널을 이용해야 한다.
③ 패스워드 저장시, 솔트가 적용된 안전한 해시함수를 사용해야 하며, 해시함수 실행은 서버에서 해야 한다.
④ 패스워드 재설정/변경시 안전하게 변경할 수 있는 규칙을 정의해서 적용해야 한다.
⑤ 패스워드 관리 규칙을 정의해서 적용해야 한다.

✠「안전한 SW 개발을 위한 소프트웨어 개발보안 가이드」개정본은 아래에서 다운받아 볼 수 있다.
문제의 내용은 94페이지에 나와있다.
http://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000015&nttId=57473

20.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정한 정보보호 최고책임자의 업무로 규정되지 않은 것은?

① 침해사고 대응
② 침해사고 정보 전파
③ 정보보호 사전보안성 검토
④ 정보보호 취약점 분석 및 개선

답 ②

②「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3의 4항에 정보보호 최고책임자의 업무가 규정되어 있는데, 침해사고 정보 전파는 명시되어 있지 않다.

✠ **정보보호 최고책임자의 업무**
1. **정보보호관리체계의 수립 및 관리·운영**
2. **정보보호 취약점 분석·평가 및 개선**
3. **침해사고의 예방 및 대응**
4. **사전 정보보호대책 마련 및 보안조치 설계·구현 등**
5. **정보보호 사전 보안성 검토**
6. **중요 정보의 암호화 및 보안서버 적합성 검토**
7. **그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행**

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제45조의3(정보보호 최고책임자의 지정 등)
① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.
② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.
③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.
④ **정보보호 최고책임자는 다음 각 호의 업무**를 총괄한다.
1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
5. 정보보호 사전 보안성 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행
⑤ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.
⑥ 정부는 제5항에 따른 정보보호 최고책임자 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.
⑦ 정보보호 최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.