2014-지방직-정보보호론-A형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

1. 정보보호의 주요 목표 중 하나인 인증성(Authenticity)을 보장하는 사례를 설명한 것으로 옳은 것은?
① 대학에서 개별 학생들의 성적이나 주민등록번호 등 민감한 정보는 안전하게 보호되어야 한다. 따라서 이러한 정보는 인가된 사람에게만 공개되어야 한다.
② 병원에서 특정 환자의 질병 관련 기록을 해당 기록에 관한 접근 권한이 있는 의사가 이용하고자 할 때 그 정보가 정확 하며 오류 및 변조가 없었음이 보장되어야 한다.
③ 네트워크를 통해 데이터를 전송할 때는 데이터를 송신한 측이 정당한 송신자가 아닌 경우 수신자가 이 사실을 확인할 수 있어야 한다.
④ 회사의 웹 사이트는 그 회사에 대한 정보를 얻고자 하는 허가받은 고객들이 안정적으로 접근할 수 있어야 한다.
정답 체크 :
(3) 네트워크 : 인증성 - 상대방의 신원을 확인시켜 준다. 사용자 인증(시스템 접근 통제)과 데이터 출처 인증(MAC)이 있다.
오답 체크 :
(1) 대학 : 기밀성 - 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.
(2) 병원 : 무결성 - 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(4) 회사 : 가용성 - 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.

2. 시스템 계정 관리에서 보안성이 가장 좋은 패스워드 구성은?
① flowerabc
② P1234567#
③ flower777
④ Fl66ower$
정답 체크 :
(4) Fl66ower$: 대문자, 소문자, 숫자, 특수문자로 구성(9글자) (크래킹에 4주 걸림)
오답 체크 :
(1) flowerabc : 소문자로만 구성(9글자) (크래킹에 2분 걸림)
(2) P1234567# : 대문자, 숫자, 특수문자로 구성(9글자) (크래킹에 16시간 걸림)
(3) flower777 : 소문자, 숫자로 구성(9글자) (크래킹에 42분 걸림)
Tip! : 패스워드는 글자 수와 어떤 문자들을 많이 섞었는지에 따라 보안의 강도가 정해진다. 크래킹에 걸리는 시간은 https://howsecureismypassword.net/에서 계산하였다.

3. 다음은 정보통신기반 보호법 의 일부이다. 본 조의 규정 목적으로 옳은 것은?

제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.
… 중략 …
2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스.논리폭탄 등의 프로그램을 투입하는 행위 제28조(벌칙)
① 제12조의 규정을 위반하여 주요정보통신기반시설을 교란.마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.
② 제1항의 미수범은 처벌한다.

① 명예훼손 방지
② 개인정보 보호 침해 방지
③ 인터넷 사기 방지
④ 웜 피해 방지

정답 체크 :
(4) 컴퓨터 바이러스·논리폭탄 등의 프로그램을 투입 : 웜 피해 방지

4. 다음 설명에 해당하는 것은?

기업이 개인정보 보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로서, 한국인터넷진흥원(KISA)에서 시행 중인 인증제도

① TCSEC
② CC
③ PIMS
④ ITSEC

정답 체크 :
(3) PIMS : 국민들에게는 개인정보를 안전하게 관리하는 조직에게 객관적으로 식별할 수 있는 기준을 제시하여 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계이다.

오답 체크 :
(1) TCSEC : 흔1983년에 미국에서 제정되었고, 표지가 오렌지색이라 오렌지북이라 불린다. 보안등급은 크게는 A, B, C, D 4단계, 세부적으론 A1, B3, B2, B1, C2, C1, D 총 7단계로 나뉜다. 4가지 요구사항은 정책(Security Policy), 책임성(Accountability), 보증(Assurance), 문서(Documentation)이다. TNI, TDI, CSSI 등 시스템 분류에 따라 적용 기준이 다르다.
(2) CC : CC라는 기준으로 TCSEC과 ITSEC은 통합되었다. 1996년에 초안이 나와 1999년에 국제 표준으로 승인되었다. PP, ST, TOE라는 인증 과정을 거친다.
(4) ITSEC : 1991년 5월 유럽 국가들이 발표한 공동 보안 지침서이다. TCSEC이 기밀성만을 강조한 것과 달리 무결성과 가용성을 포괄하는 표준안을 제시하였다.

5. 보안 공격 중 적극적 보안 공격의 종류가 아닌 것은?
① 신분위장(masquerade) : 하나의 실체가 다른 실체로 행세를 한다.
② 재전송(replay) : 데이터를 획득하여 비인가된 효과를 얻기위하여 재전송한다.

③ 메시지 내용 공개(release of message contents) : 전화 통화, 전자우편 메시지, 전송 파일 등에 기밀 정보가 포함되어 있으므로 공격자가 전송 내용을 탐지하지 못하도록 예방해야 한다.
④ 서비스 거부(denial of service) : 통신 설비가 정상적으로 사용 및 관리되지 못하게 방해한다.
정답 체크 :
(3) 메시지 내용 공개 : 기밀성을 해치는 소극적 공격에 해당한다.
오답 체크 :
(1) 신분위장 : 무결성을 해치는 적극적 공격에 해당한다.
(2) 재전송 : 무결성을 해치는 적극적 공격에 해당한다.
(4) 서비스 거부 : 가용성을 해치는 적극적 공격에 해당한다.
Tip! : 다음은 공격 방법, 적극적/소극적, 기밀성/무결성/가용성 관점에서 정리한 표이다.

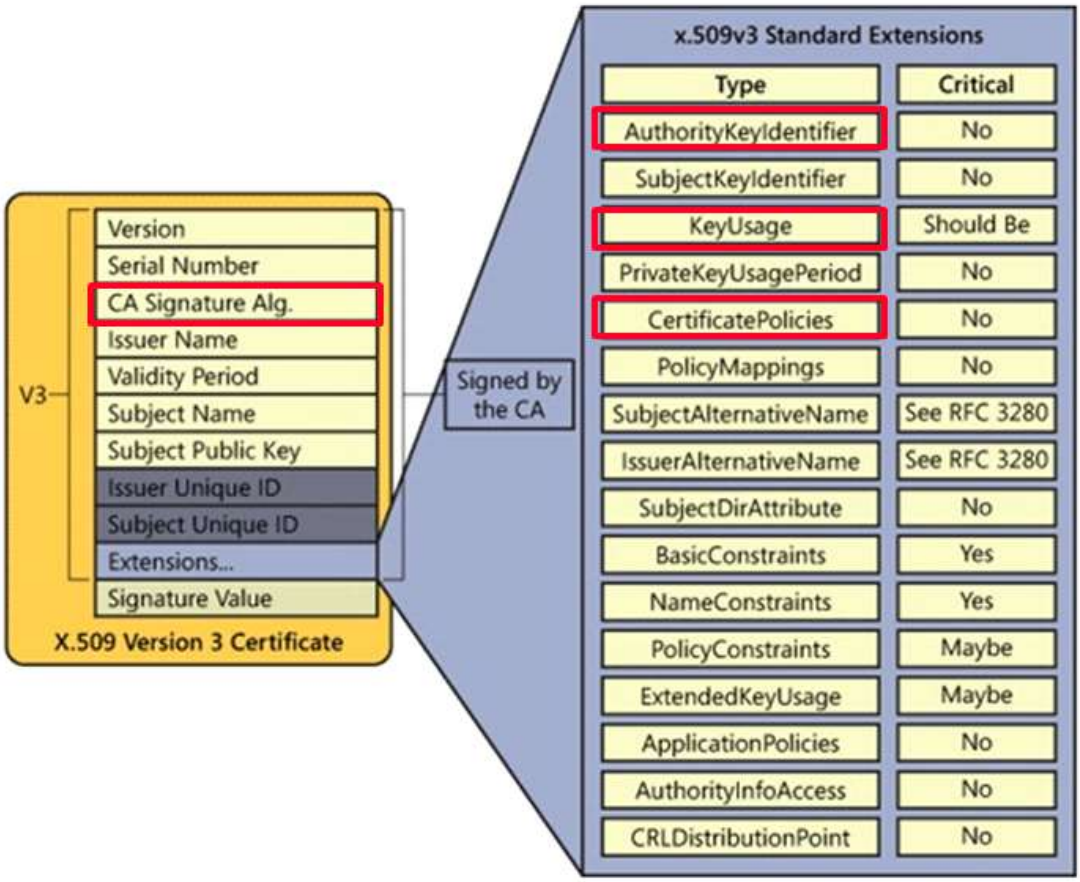
Attacks	*Passive/Active*	*Threatening*
Snooping (Sniffing) Traffic analysis	Passive	Confidentiality
Modification Masquerading (Spoofing) Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

6. 피싱(Phishing)에 대한 설명으로 옳지 않은 것은?
① Private Data와 Fishing의 합성어로서 유명 기관을 사칭하거나 개인 정보 및 금융 정보를 불법적으로 수집하여 금전적인 이익을 노리는 사기 수법이다.
② Wi-Fi 무선 네트워크에서 위장 AP를 이용하여 중간에 사용자의 정보를 가로채 사용자인 것처럼 속이는 수법이다.
③ 일반적으로 이메일을 사용하여 이루어지는 수법이다.
④ 방문한 사이트를 진짜 사이트로 착각하게 하여 아이디와 패스워드 등의 개인정보를 노출하게하는 수법이다.
정답 체크 :
(2) 위장 AP : 이블 트윈(Evil Twin, 악의적 쌍둥이) 공격 기법에 해당한다. 이블 트윈은 가짜 페이스북 ID를 의미하기도 한다.
오답 체크 :
(1) Private Data + Fishing : 개인정보(private data)와 낚시(fishing)를 합성한 조어(造語)라고 하는 설과 그 어원은 fishing이지만 위장의 수법이 '세련되어 있다(sophisticated)'는 데서 철자를 'phishing'으로 쓰게 되었다는 설이 있다.
(3) 이메일 : 이메일의 발신자 이름을 금융기관의 창구 주소로 한 메일을 무차별적으로 보내는 것이 있다. 메일 본문에는 개인정보를 입력하도록 촉구하는 안내문과 웹사이트로의 링크가 기재되어 있는데, 링크를 클릭하면 그 금융기관의 정규 웹사이트와 개인정보입력용 팝업 윈도가 표시된다.

(4) 진짜 사이트로 착각 : 메인윈도에 표시되는 사이트는 '진짜'이지만, 팝업 페이지는 '가짜'이다. 진짜를 보고 안심한 사용자가 팝업에 표시된 입력란에 인증번호나 비밀번호, 신용카드 번호 등의 비밀을 입력·송신하면 피싱을 하려는 자에게 정보가 송신된다.

7. 국내 기관에서 주도적으로 개발한 암호 알고리즘은?
① IDEA
② ARIA
③ AES
④ Skipjack
해설) 암호학
정답 체크 :
(2) ARIA : 경량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다.
오답 체크 :
(1) IDEA : 1990년에 ETH(스위스)의 라이(Lai)와 매시(Massey)가 개발한 알고리즘이다.
(3) AES : 2000년에 미국 표준 기술 연구소(NIST)에 의해 제정된 암호화 방식이다. AES의 후보로서 다수의 대칭 암호 알고리즘을 제안했지만, 그 중에서 Rijndael(라인델)이라는 대칭 암호 알고리즘이 선정되었다.
(4) Skipjack : 미 국가안보국(NSA, National Security Agency)에서 개발한 Clipper 칩에 내장된 블록 알고리즘이다.

8. 공개키 기반 구조(PKI, Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?
① 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보 보호 방식이다.
② 인증서의 폐지 여부는 인증서 폐지목록(CRL)과 온라인 인증서 상태 프로토콜(OCSP) 확인을 통해서 이루어진다.
③ 인증서는 등록기관(RA)에 의해 발행된다.
④ 인증서는 버전, 일련번호, 서명, 발급자, 유효 기간 등의 데이터 구조를 포함하고 있다.
정답 체크 :
(3) 등록기관(RA) : 인증기관(CA)의 일 중 「공개키의 등록과 본인에 대한 인증」을 대행하는 기관이다. 인증서의 발행과 폐지는 인증기관에서 수행한다.
오답 체크 :
(1) 공개키 암호시스템 : PKI는 공개키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택 사양의 총칭이다.
(2) CRL & OCSP : CRL은 인증서 폐지 목록으로 주기적으로 갱신해야만 한다. OCSP는 인증서 폐지 및 효력 정지 상태를 파악해 사용자가 실시간으로 인증서를 검증할 수 있는 프로토콜이다.
(4) 인증서 내용 : 인증서의 내용은 다음과 같다.



9. 소인수분해 문제의 어려움에 기초하여 큰 안전성을 가지는 전자 서명 알고리즘은?

① RSA

② ElGamal

③ KCDSA

④ ECDSA

정답 체크 :

(1) RSA : 큰 수의 소인수분해를 고속으로 행하는 방법이 없다는 것을 이용한다. 소인수분해란 소수 p, q가 주어졌을 때 n=pq를 구하는 것은 쉽지만, n이 주어졌을 때 소수 q, q를 구하는 것은 어렵다는 사실에 기반을 둔다.

오답 체크 :

(2) ElGamal : 이산 대수를 구하는 것이 어렵다는 것을 이용한다. 이산 대수란 g, x, p가 주어졌을 때 $y=g^x \bmod p$를 구하는 것은 쉽지만, g, y, p가 주어졌을 때 x를 구하는 것은 어렵다는 사실에 기반을 둔다.

(3) KCDSA : KISA(한국인터넷진흥원)에서 개발한 인증서 기반 부가형 전자서명 알고리즘으로, ElGamal 서명 방식의 변형으로 이산대수 문제에 안전성을 두고 있다.

(4) ECDSA : 전자 서명 알고리듬(DSA)에 타원 곡선 암호(ECC) 방식을 이용한 전자 서명 알고리이다. ECC는 이산대수 문제에 안정성을 두고 있다.

10. 디지털 포렌식의 기본 원칙에 대한 설명으로 옳지 않은 것은?
① 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐서 획득되어야 한다.
② 신속성의 원칙 : 컴퓨터 내부의 정보 획득은 신속하게 이루어져야 한다.
③ 연계보관성의 원칙 : 증거 자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.
④ 무결성의 원칙 : 획득된 정보는 위·변조되지 않았음을 입증할 수 있어야 한다.
정답 체크 :
(3) 연계보관성의 원칙 : 해당 설명은 재현의 원칙이고, 연계보관성의 원칙은 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.
오답 체크 :
(1) 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(2) 신속성의 원칙 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
(4) 무결성의 원칙 : 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 함을 의미한다.

11. 보안 공격에 대한 설명으로 옳지 않은 것은?
① Land 공격 : UDP와 TCP 패킷의 순서번호를 조작하여 공격 시스템에 과부하가 발생한다.
② DDoS(Distributed Denial of Service) 공격 : 공격자, 마스터, 에이전트, 공격 대상으로 구성된 메커니즘을 통해 DoS 공격을 다수의 PC에서 대규모로 수행한다.
③ Trinoo 공격 : 1999년 미네소타 대학교 사고의 주범이며 기본적으로 UDP 공격을 실시한다.
④ SYN Flooding 공격 : 각 서버의 동시 가용자 수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용할 수 없게 만드는 공격이다.
정답 체크 :
(1) Land : 해당 설명은 Teardrop, Boink, Bonk가 해당되고, Land는 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이다. (포트 번호도 같을 수 있다)
오답 체크 :
(2) DDoS : 악성코드(봇)에 의한 에이전트를 전파하고, 좀비 PC에 의한 공격을 수행한다. 좀비 PC로 구성된 네트워크를 봇넷(Botnet)이라고 한다. DoS는 1:1로 공격하지만, DDoS는 N:1로 공격을 수행한다.
(3) Trinoo : DDoS 공격을 수행하는 컴퓨터 프로그램들의 모음이다. 2000년도에 야후 웹사이트를 공격한 것으로 유명하다.
(4) SYN Flooding : 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.

12. 웹 브라우저와 웹 서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법은?
① PGP
② SSH
③ SSL
④ S/MIME
정답 체크 :
(3) SSL : 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜이다. 웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에 적용할 수 있다. (TLS도 동일한 답이 될 수 있다)
오답 체크 :
(1) PGP : 전자우편의 안전성을 위해 1991년 미국의 Phil Zimmermann에 의해 개발된 전자우편 보안 시스템이다.
(2) SSH : 두 호스트(Host) 사이의 통신 암호화 관련 인증 기술들을 사용하여, 안전한 접속과 통신을 제공하는 프로토콜을 의미한다.
(4) S/MIME : 안전한 전자메일 전송을 위한 산업체 표준 규약이다. 기존 MIME 형식의 전자메일 서비스에 암호 및 보안 서비스가 추가된 구조이다.

13. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 정보통신서비스 제공자의 정보보호 최고책임자가 총괄하는 업무에 해당하지 않는 것은? (단, 이 법에 명시된 것으로 한정 함)
① 정보보호관리체계 수립 및 관리·운영
② 주요정보통신기반시설의 지정
③ 정보보호 취약점 분석·평가 및 개선
④ 정보보호 사전 보안성 검토
정답 체크 :
(2)
“정보통신기반 보호법” 제8조(주요정보통신기반시설의 지정 등)에 명시된 주요정보통신기반시설로 지정할 수 있는 경우는 다음과 같다.
1. 중앙행정기관의 장은 소관분야의 정보통신기반시설중 5가지 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. 2. 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다. (회사의 임원이 주요정보통신기반시설을 지정할 수는 없다.)
오답 체크 :
(1), (3), (4)
“정보통신망 이용촉진 및 정보보호 등에 관한 법률” 제45조의3(정보보호 최고책임자의 지정 등)에 명시된 정보보호 최고책임자의 총괄 업무는 다음과 같다.
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 관

계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

14. 개인정보 보호법 상 자신의 개인정보 처리와 관련한 정보주체의 권리에 대한 설명으로 옳지 않은 것은?
① 개인정보의 처리에 관한 정보를 제공받을 수 있다.
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 수 있다.
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 수 있다.
④ 개인정보에 대하여 열람을 할 수 있으나, 사본의 발급은 요구할 수 없다.
정답 체크 :
(4)
"개인정보 보호법" 제4조(정보주체의 권리) 상 자신의 개인정보 처리와 관련한 정보주체의 권리는 다음과 같다.
1. 개인정보의 처리에 관한 정보를 제공받을 권리, 2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리, 3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리, 4. 개인정보의 처리 정지, 정정ㆍ삭제 및 파기를 요구할 권리, 5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리 (사본의 발급을 요구할 수 있다)

15. 침해사고가 발생하였을 경우 조직 내의 모든 사람들이 신속하게 대처하여 침해사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위한 단계는?
① 보안 탐지 단계
② 대응 단계
③ 사후 검토 단계
④ 조사와 분석 단계
정답 체크 :
(2) 대응 : 침해 사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위한 것으로 단기 대응, 백업 및 증거 확보, 시스템 복구 단계에 따라 수행된다.
오답 체크 :
(1) 보안탐지 : 침해 사고 발생을 실시간으로 식별하는 과정은 주로 침입 탐지 시스템(IDS)이나 침입 방지 시스템(IPS), 네트워크 트래픽 모니터링 장비(MRTG), 네트워크 관리 시스템(NMS)을 통해 이루어진다.
(3) 사후검토 : 침해 사고 식별과 대응 과정은 정해진 기록 문서에 따라 작성한다. 이렇게 작성된 문서와 포렌식 과정에서 획득한 자료를 기반으로 침해 사고에 대한 보고서를 작성한다. 침해 사고의 원인을 확인하고 그 대응책을 마련해야 한다(후속 조치 및 보고).
(4) 조사와 분석 : 최초 침해 사고 발생을 식별한 시스템 및 네트워크 이외에 추가로 침해 사고가 발생한 곳이 있는지 모두 확인하고 조치하는 단계이다(제거 및 복구).

16. 다음 설명에 해당하는 블루투스 공격 방법은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격 방법은 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX

Push Profile) 기능을 사용하여 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근하는 공격 방법이다.

① 블루스나프(BlueSnarf)
② 블루프린팅(BluePrinting)
③ 블루버그(BlueBug)
④ 블루재킹(BlueJacking)

정답 체크 :
(1) 블루스나프 : 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근한다. 공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환할 수 있는 OPP(OBEX Push Profile)를 사용하여 정보를 열람할 수 있다.

오답 체크 :
(2) 블루프린팅 : 블루투스 공격 장치의 검색 활동이다. 블루투스는 장치 간 종류를 식별하기 위해 서비스 발견 프로토콜(SDP : Service Discovery Protocol)을 보내고 받는다. 공격자는 이를 이용해 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.
(3) 블루버그 : 블루투스 장비 간 취약한 연결 관리를 악용한다. 블루투스 기기는 한 번 연결되면 이후에는 다시 연결해주지 않아도 서로 연결된다. 이 인증 취약점을 이용하여 공격이다.
(4) 블루재킹 : 무선이나 첨부파일 등의 형태로 휴대폰에 침입하여 프로그램이나 데이터를 파괴하는 악성 프로그램인 휴대폰바이러스의 일종이다. 전파 경로는 휴대폰에 메시지가 뜨면서 근처에 있는 다른 블루투스가 장착된 휴대폰에 이메일처럼 그 메시지를 보내 감염시킨다.

17. 데이터베이스 보안 요구사항 중 비기밀 데이터에서 기밀 데이터를 얻어내는 것을 방지하는 요구사항은?

① 암호화
② 추론 방지
③ 무결성 보장
④ 접근통제

정답 체크 :
(2) 추론 방지 : 추론(inference)은 보통의 일반적인 데이터로부터 기밀 정보를 획득할 수 있는 가능성을 의미한다. 추론 문제는 사용자가 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하여야 하는 통계 DB에 많은 영향을 미친다.

오답 체크 :
(1) 암호화 : 중요 데이터에 대한 기밀성을 보호(암호화)하고 인가된 사용자에 대해서만 접근을 허용해야 한다.
(3) 무결성 보장 : 데이터의 내용을 수정할 수 있는 인가되지 않은 접근, 저장 데이터를 손상시킬 수 있는 시스템의 오류, 고장 등으로부터 DB를 보호하여야 한다. 이러한 유형의 보호는 적절한 시스템 통제, 다양한 백업 및 복구 절차, 임시적인 보안 절차 등을 통하여 DBMS가 수행한다. 특히 시스템 고장 시, DB는 더 이상 일관성을 유지하지 못할 수도 있다.
(4) 접근 통제 : 부적절한 접근으로부터 DB를 보호하기 위해서는 승인된 사용자에게만 접근 권한을 부여하고, 사용자 혹은 응용 시스템의 접근 요청은 DBMS에 의하여 관리되어야 한다. 정당하게 권한을 부여 받은 사용자에게만 DB 접근을 허용한다.

18. 가상사설망의 터널링 기능을 제공하는 프로토콜에 대한 설명으로 옳은 것은?
① IPSec은 OSI 3계층에서 동작하는 터널링 기술이다.
② PPTP는 OSI 1계층에서 동작하는 터널링 기술이다.
③ L2F는 OSI 3계층에서 동작하는 터널링 기술이다.
④ L2TP는 OSI 1계층에서 동작하는 터널링 기술이다.
정답 체크 :
(1) IPSec : IP 망에서 안전하게 정보를 전송하는 표준화된 OSI 3계층 프로토콜이다.
오답 체크 :
(2) PPTP : Microsoft사에서 제안한 프로토콜로 OSI 2계층에서 동작한다. 처음에는 1:1 연결을 지원하고 현재는 1:N 연결을 지원한다.
(3) L2F : Cisco사에서 제안한 프로토콜로 OSI 2계층에서 동작한다. 1:N 연결을 지원한다.
(4) L2TP : PPTP와 L2F의 장점을 통합하여 제안되었고 OSI 2계층에서 동작한다.

19. 미국의 NIST와 캐나다의 CSE가 공동으로 개발한 평가체계로 암호 모듈의 안전성을 검증하는 것은?
① CMVP
② COBIT
③ CMM
④ ITIL
정답 체크 :
(1) CMVP : 미국(NIST)와 캐나다(CSE)에 의해 만들어진 암호 모듈(암호화 알고리즘, 키의 길이 등) 검증 프로그램이다. (한국에는 KCMVP가 있다.)
오답 체크 :
(2) COBIT : 정보 기술의 보안 및 통제 지침에 관한 표준 프레임워크를 제공하는 실무 지침이다.
(3) CMM : 소프트웨어 개발 능력 측정 기준과 소프트웨어 프로세스 평가 기준을 제공함으로써 정보 및 전산 조직의 성숙수준을 평가할 수 있는 모델이다.
(4) ITIL : 영국에서 태동한 정보 기술(IT) 서비스를 지원, 구축, 관리하는 프레임워크이다.

20. MS Windows 운영체제 및 Internet Explorer의 보안 기능에 대한 설명으로 옳은 것은?
① Windows 7의 각 파일과 폴더는 사용자에 따라 권한이 부여되는데, 파일과 폴더에 공통적으로 부여할 수 있는 사용 권한은 모든 권한·수정·읽기·쓰기의 총 4가지이며, 폴더에는 폴더 내용 보기라는 권한을 더 추가할 수 있다.
② Bit Locker 기능은 디스크 볼륨 전체를 암호화하여 데이터를 안전하게 보호하는 기능으로 Windows XP부터 탑재되었다.
③ Internet Explorer 10의 인터넷 옵션에서 개인정보 수준을 '낮음'으로 설정하는 것은 모든 쿠키를 허용함을 의미한다.
④ Windows 7 운영체제의 고급 보안이 포함된 Windows 방화벽은 인바운드 규칙과 아웃바운드 규칙을 모두 설정할 수 있다.
정답 체크 :
(4) 방화벽 : 인바운드(외부에서 컴퓨터로 들어오는 패킷)와 아웃바운드(컴퓨터에서 외부로 나

가는 패킷)에 대한 규칙을 설정할 수 있다.

오답 체크 :

(1) 권한 : 파일은 모든 권한, 수정, 읽기 및 실행, 읽기, 쓰기, 특정 권한을 가진다. 폴더는 모든 권한, 수정, 읽기 및 실행, 폴더 내용 보기, 읽기, 쓰기, 특정 권한을 가진다. 공통적으로 부여할 수 있는 권한은 6가지다.

(2) BitLocker : 마이크로소프트 윈도우 비스타, 윈도우 서버 2008, 윈도우 7, 윈도우 8, 윈도우 8.1, 윈도우 10 운영 체제에 포함된 완전한 디스크 암호화 기능이다. 즉, 윈도우 비스타부터 탑재되었다.

(3) Internet Explorer 10 : '낮음'으로 설정하면 압축된 개인 정보 취급 방침이 없는 타사의 쿠키를 차단하고 사용자의 암시적 동의 없이 사용자에게 연락하는데 사용할 수 있는 정보를 저장하는 타사의 쿠키를 제한한다.