2015년도 국가직 9급 정보보호론

문 1. 다음에서 설명하는 공격방법은? 2

정보보안에서 사람의 심리적인 취약점을 악용하여 비밀정보를 취득하거나 컴퓨터 접근권한 등을 얻으려고 하는 공격방법이다.

① 스푸핑 공격
② 사회공학적 공격
③ 세션 가로채기 공격
④ 사전 공격
[해설]
- 사회공학적 공격 : 시스템이나 네트워크의 취약점을 이용한 해킹기법이 아니라 사회적이고 심리적인 요인을 이용하여 해킹하는 것을 가리키는 말이다.

문 2. 능동적 보안 공격에 해당하는 것만을 모두 고른 것은? 4

ㄱ. 도청 ㄴ. 감시 ㄷ. 신분위장 ㄹ. 서비스 거부

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
[해설]
- 능동적 공격(적극적 공격)은 데이터에 대한 변조를 하거나 직접 패킷을 보내서 시스템의 무결성, 가용성, 기밀성을 공격하는 것으로 직접적인 피해를 입힌다.
- 수동적 공격(소극적 공격)은 데이터 도청, 수집된 데이터 분석 등이 있으며, 직접적인 피해를 입히지는 않는다..

문 3. 다음에서 설명하는 재해복구시스템의 복구 방식은? 1

재해복구센터에 주 센터와 동일한 수준의 시스템을 대기상태로 두어, 동기적 또는 비동기적 방식으로 실시간 복제를 통하여 최신의 데이터 상태를 유지하고 있다가, 재해 시 재해복구센터의 시스템을 활성화 상태로 전환하여 복구하는 방식이다.

① 핫 사이트(Hot Site)

② 미러 사이트(Mirror Site)
③ 웜 사이트(Warm Site)
④ 콜드 사이트(Cold Site)
[해설]
- 미러 사이트(Mirror Site) : 메인 센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하고, 메인 센터와 재해 복구 센터 모두 액티브 상태로 실시간 동시 서비스를 하는 방식이다. RTO(복구 소요 시간)은 이론적으로 0이다.
- 핫 사이트(Hot Site) : 메인 센터와 동일 한 수준의 정보 기술 자원을 대기 상태로 사이트에 보유하면서, 동기적 또는 비동기적 방식으로 실시간 미러링을 통하여 데이터를 최신 상태로 유지한다. RTO(복구 소요 시간)은 수 시간 이내이다.
- 웜 사이트(Warm Site) : 메이 센터와 동일한 수준의 정보 기술 자원을 보유하는 대신 중요성이 높은 기술 자원만 부분적으로 보유하는 방식이다. 실시간 미러링을 수행하지 않으며 데이터의 백업 주기가 수 시간 ~1일(RTO) 정도로 핫 사이트에 비해 다소 길다
- 콜드 사이트(Cold Site) : 데이터만 원격지에 보관하고 서비스를 위한 정보 자원은 확보하지 않거나 최소한으로만 확보하는 유형이다. 메인 센터의 데이터는 주기적 수 일~ 수 주(RTO)으로 원격지에 백업한다.

문 4. 정보보안의 기본 개념에 대한 설명으로 옳지 않은 것은? 3
① Kerckhoff의 원리에 따라 암호 알고리즘은 비공개로 할 필요가 없다.
② 보안의 세 가지 주요 목표에는 기밀성, 무결성, 가용성이 있다.
③ 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유하지 않아도 된다.
④ 가용성은 인가된 사용자에게 서비스가 잘 제공되도록 보장하는 것이다.
[해설]
- 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유하여야 한다. 이는 대칭키 암호 알고리즘의 단점이기도 하다.
- Kerckhoff의 원리 : Kerckhoff에 따르면 암호문의 안전성은 비밀키의 비밀성에만 기반을 두라고 권장한다. 키를 알아내는 것이 매우 여러워서 암/복호화 알고리즘을 비밀로 한 필요가 없어야 한다는 것이다.

문 5. 공개키 기반 구조(PKI : Public Key Infrastructure)의 인증서에 대한 설명으로 옳은 것만을 모두 고른 것은? 1

ㄱ. 인증기관은 인증서 및 인증서 취소목록 등을 관리한다. ㄴ. 인증기관이 발행한 인증서는 공개키와 공개키의 소유자를 공식적으로 연결해 준다. ㄷ. 인증서에는 소유자 정보, 공개키, 개인키, 발행일, 유효기간 등의 정보가 담겨 있다. ㄹ. 공인인증서는 인증기관의 전자서명 없이 사용자의 전자서명만으로 공개키를 공증한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
[해설]
- 인증서의 구조 : 버전(Version), 일련번호(Serial Number), 알고리즘 식별자(Algorithm Identifier), 발행자(Issuer), 유효기간(Period of validity), 주체(Subject), 공개키 정보(Public-key information), 서명(Signature)
-인증서에는 인증 기관(CA : Certificate Authority)의 서명문을 포함한다.

문 6. 위험 분석에 대한 설명으로 옳지 않은 것은? 4
① 자산의 식별된 위험을 처리하는 방안으로는 위험 수용, 위험 회피, 위험 전가 등이 있다.
② 자산의 가치 평가를 위해 자산구입비용, 자산유지보수비용 등을 고려할 수 있다.
③ 자산의 적절한 보호를 위해 소유자와 책임소재를 지정함으로써 자산의 책임추적성을 보장받을 수 있다.
④ 자산의 가치 평가 범위에 데이터베이스, 계약서, 시스템 유지 보수 인력 등은 제외된다.
[해설]
- 자산의 가치 평가 범위에는 서버시스템, 네트워크, 정보시스템, 보안시스템, 데이터베이스, 문서, 소프트웨어, 물리적환경 등이 포함된다.

문 7. 메시지 인증 코드(MAC : Message Authentication Code)를 이용한 메시지 인증 방법에 대한 설명으로 옳지 않은 것은? 4
① 메시지의 출처를 확신할 수 있다.
② 메시지와 비밀키를 입력받아 메시지 인증 코드를 생성한다.
③ 메시지의 무결성을 증명할 수 있다.
④ 메시지의 복제 여부를 판별할 수 있다.
[해설]
- MAC 값은 검증자(비밀 키를 소유한 사람)의 허가에 의해서 메시지의 데이터 인증과 더불어 무결성을 보호한다.

문 8. 유닉스(Unix)의 로그 파일과 기록되는 내용을 바르게 연결한 것은? 1

ㄱ. history - 명령창에 실행했던 명령 내역 ㄴ. sulog - su 명령어 사용 내역 ㄷ. xferlog - 실패한 로그인 시도 내역 ㄹ. loginlog - FTP 파일 전송 내역

① ㄱ, ㄴ

② ㄱ, ㄷ

③ ㄴ, ㄷ

④ ㄷ, ㄹ

[해설]

- xferlog : FTP 서버의 데이터 전송관련 로그
- loginlog : 5번이상 로그인에 실패한 정보 기록

문 9. 전송계층 보안 프로토콜인 TLS(Transport Layer Security)가 제공하는 보안 서비스에 해당하지 않는 것은? 1

① 메시지 부인 방지

② 클라이언트와 서버 간의 상호 인증

③ 메시지 무결성

④ 메시지 기밀성

[해설]

- 상호 인증 : 클라이언트와 서버간의 상호 인증(RSA, DSS, X.509)
- 기밀성 : 대칭키 암호화 알고리즘을 통한 데이터의 암호화(DES, 3DES, RC4 등)
- 데이터 무결성 : MAC 기법을 이용해 데이터 변조 여부 확인(HMAC-md5, HMAC-SHA-1)

문 10. 다음에서 설명하는 스니퍼 탐지 방법에 이용되는 것은? 3

○스니핑 공격을 하는 공격자의 주요 목적은 사용자 ID와 패스워드의 획득에 있다. ○보안 관리자는 이 점을 이용하 가짜 ID와 패스워드를 네트워크에 계속 보내고, 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지한다.

① ARP

② DNS

③ Decoy

④ ARP watch

[해설]

- 유인(Decoy)을 이용한 스니퍼 탐지 : 스니핑 공격을 하는 공격자의 주요 목적은 ID와 패스워드의 획득에 있다. 가짜 ID와 패스워드를 네트워크에 계속 뿌려 공격자가 이 ID와 패스워드를 이용하여 접속을

시도할 때 공격자를 탐지할 수 있다.

문 11. 다음에 제시된 <보기 1>의 사용자 인증방법과 <보기 2>의 사용자 인증도구를 바르게 연결한 것은? 3

<보기 1>

ㄱ. 지식기반 인증 ㄴ. 소지 기반 인증 ㄷ. 생체 기반인증

<보기 2>

A. OPT 토큰 B. 패스워드 C. 홍채

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	A	C
④	B	C	A

[해설]

- 지식 기반 인증 : 패스워드
- 소유(소지) 기반 인증 :스마트카드, OPT 토큰
- 존재(생체) 인증 기반 : 지문, 홍채, 망막
- 행위 기반 인증 : 서명, 움직임

문 12. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 용어의 정의에 대한 설명으로 옳지 않은 것은? 3

① 정보통신서비스 : 「전기통신사업법」 제2조제6호에 따른 전기 통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것

② 정보통신망 : 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제

③ 통신과금서비스이용자 : 정보보호제품을 개발·생산 또는 유통하는 사람이나 정보보호에 관한 컨설팅 등과 관련된 사람

④ 침해사고 : 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태

[해설]

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조(정의)

- 통신과금서비스이용자 : 통신과금 서비스제공자로부터 통신과금서비스 이용하여 재화등을 구입 · 이용하는 자를 말한다.

문 13. 안드로이드 보안에 대한 설명으로 옳지 않은 것은? 4

① 리눅스 운영체제와 유사한 보안 취약점을 갖는다.

② 개방형 운영체제로서의 보안정책을 적용한다.

③ 응용프로그램에 대한 서명은 개발자가 한다.

④ 응용프로그램 간 데이터 통신을 엄격하게 통제한다.

[해설]

- 안드로이드 환경은 앱의 파일 복제가 자유롭고 마켓의 검증 과정이 철저하지 않으며, 개발과 배포가 자유로운 오픈 소스 플랫폼과 오픈 마켓의 특성으로 인한 보안에 대한 본질적인 문제는 극복하기가 쉽지 않다.

문 14. 개인정보 보호 인증(PIPL) 제도에 대한 설명으로 옳은 것은? 2

① 물리적 안전성 확보조치 심사영역에는 악성 소프트웨어 통제 심사항목이 있다.

② 인증절차는 인증심사 준비단계, 심사단계, 인증단계로 구성되며, 인증유지관리를 위한 유지관리 단계가 있다.

③ 개인정보 보호를 위해 관리계획 수립과 조직구축은 정보주체권리보장 심사영역에 속한다.

④ 인증을 신청할 수 있는 기관은 공공기관에 한정한다.

[해설]

- 개인정보 보호 인증(PIPL)의 적용대상은 업무를 목적으로 개인정보를 처리하는 공공기관, 민간기업, 법인, 단체 및 개인 등 모든 공공 기관 및 민간 개인정보처리자를 대상으로 한다.

문 15. 해킹에 대한 설명으로 않은 것은? 2

① SYN Flooding은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.

② Zero Day 공격은 시그니처(signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.

③ APT는 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.

④ Buffer Overflow는 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

[해설]

- 침입탐지시스템에서 시그니처(signature) 기반은 오용탐지에 해당되며, 오용탐지는 Zero Day 공격을 탐지할 수 없다. 비정상 행위탐지가 Zero Day 공격을 탐지할 수는 있다.

문 16. 다음에서 설명하는 웹 서비스 공격은? 4

공격자가 사용자의 명령어나 질의어에 특정한 코드를 삽입하여 DB 인증을 우회하거나 데이터를 조작한다.

① 직접 객체 참조

② Cross Site Request Forgery

③ Cross Site Scripting
④ SQL Injection
[해설]
- SQL Injection : 응용프로그램 보안 상의 허점을 의도적으로 이용해, 개발자가 생각지 못한 SQL문을 실행되게 함으로써 데이터베이스를 비정상적으로 조작하는 공격 방법이다.

문 17. 사용자와 인증 서버 간 대칭키 암호를 이용한 시도 - 응답(Challenge-Response) 인증방식에 대한 설명으로 옳지 않은 것은? 3
① 재전송 공격으로부터 안전하게 사용자를 인증하는 기법이다.
② 인증 서버는 사용자 인증을 위해 사용자의 비밀키를 가지고 있다.
③ 사용자 시간과 인증 서버의 시간이 반드시 동기화되어야 한다.
④ Response값은 사용자의 비밀키를 사용하여 인증 서버에서 전달받은 Challenge값을 암호화한 값이다.
[해설]
- OTP(One Time Password)의 구현에 이용되는 방식은 비동기화 방식과 동기화 방식이 있다. 비동기화 방식은 미리 설정되어 있는 동기화 기준 정보가 없어 난수값을 이용하며, 대표적인 예가 시도 - 응답(Challenge-Response) 인증방식이다.

문 18. 국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은? 2
① 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.
② 보호 프로파일(Protection Profiles)은 특정 제품이나 시스템에만 종속되어 적용하는 보안기능 수단과 보증수단을 기술한 문서이다.
③ 평가 보증 등급(EAL : Evaluation Assurance Level)에서 가장 엄격한 보증(formally verified) 등급은 EAL7이다.
④ 보안 요구조건을 명세화하고 평가기준을 정의하기 위한 ISO/IEC 15408 표준이다.
[해설]
- 보안목표명세서가 특정 TOE(평가대상물)을 서술하는 반면, 보호프로파일은 TOE 유형을 서술한다. 따라서 동일한 보호프로파일이 여러 평가에 사용될 다양한 보안목표명세서들에 대한 기본모델(Template)로써 사용된다

문 19. 「개인정보 보호법」상 주민등록번호 처리에 대한 설명으로 옳지 않은 것은? 1
① 주민등록번호를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, 개인인 개인정보처리자는 개인정보 보호위원회의 심의·의결을 거쳐 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

② 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 유출된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 주민등록번호가 유출되지 아니하도록 개인정보처리자가 「개인정보 보호법」에 다른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.
③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.
④ 개인정보처리자는 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

[해설]

- 보기1번은 주민등록번호가 아니라, 개인정보이다. 주민등록번호는 개인정보보호법 제24조의2에서 명시하는 경우를 제외하고는 처리/수집/제공 할 수 없다.

- 제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

- 제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

문 20. 다음에서 설명하는 윈도우 인증 구성요소는? 2

○사용자의 계정과 패스워드가 일치하는 사용자에게 고유의 SID(Security Identifier)를 부여한다. ○SID에 기반을 두어 파일이나 디렉터리에 대한 접근의 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① LSA(Local Security Authority)
② SRM(Security Reference Monitor)
③ SAM(Security Account Manager)
④ IPSec(IP Security)

[해설]

- SRM (Security Reference Monitor) : SAM이 사용자의 계정과 패스워드가 일치하는지를 확인하여 SRM (Security Refenrnce Monitor)에게 알려주면, SRM은 사용자에게 고유의 SID(Security Identifier)를 부여한다. SRM은 SID에 기반하여 파일이나 디렉토리에 접근(access)제어를 하게 되고,

이에 대한 감사 메시지를 생성한다.(실질적으로 SAM에서 인증을 거치고 나서 권한을 부여하는 모듈이라고 생각하면 된다)

- LSA (Local security Authority) : 모든 계정의 로그인에 대한 검증, 시스템 자원 및 파일 등에 대한 접근 권한을 검사한다. SRM이 생성한 감사 로그를 기록하는 역할을 한다.(즉, NT 보안의 중심 요소, 보안 서브 시스템(Security subsystem)이라고 부르기도 한다.)

- SAM (Security Account Manager) : 사용자/그룹 계정 정보에 대한 데이터베이스를 관리한다. 사용자의 로그인 입력 정보와 SAM 데이터베이스 정보를 비교하여 인증 여부를 결정하도록 해주는 것이다.