2017-서울시-정보보호론-A형-해설-곽후근

1. 다음의 지문은 무엇을 설명한 것인가?

ㄱ. 전자금융거래에서 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심 거래를 탐지하고 이상금융거래를 차단하는 시스템이다. ㄴ. 보안 프로그램에서 방지하지 못하는 전자금융사기에 대한 이상거래를 탐지하여 조치를 할 수 있도록 지원하는 시스템 이다.

① MDM
② FDS
③ MDC
④ RPO

정답 체크 :

(2) FDS(Fraud Detection System) : 전자금융거래에서 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심거래를 탐지하고 이상금융거래를 차단하는 시스템을 말한다.

오답 체크 :

(1) MDM(Mobile Device Management) : MDM은 통상 IT 부서가 기기를 완전히 제어할 수 있도록, 직원의 스마트패드와 스마트폰에 잠금·제어·암호화·보안 정책 실행을 할 수 있는 기능을 제공한다.

(3) MDC(Modification Detection Code) : 메시지의 무결성(메시지가 변하지 않았다는 것) 보장하는 메시지 다이제스트(해시값)이다. 이와 비슷한 개념인 MAC(Message Authentication Code)은 무결성과 인증을 보장한다. 즉, MDC는 인증을 보장하지는 않는다.

(4) RPO(Recovery Point Objective) : 목표 복구 시점을 의미한다. 조직에서 발생한 여러 가지 재난 상황으로 IT 시스템이 마비되었을 때 각 업무에 필요한 데이터를 여러 백업 수간을 활용하여 복구할 수 있는 기준점이다. 예를 들어, RPO가 3분이면 3분전의 시점으로 복구할 수 있다는 의미이다.

2. 다음 중 APT(Advanced Persistent Threat) 공격에 대한 설명 중 옳지 않은 것은?

① 사회 공학적 방법을 사용한다.
② 공격대상이 명확하다.
③ 가능한 방법을 총동원한다.
④ 불분명한 목적과 동기를 가진 해커 집단이 주로 사용한다.

정답 체크 :

(4) 단계1에서처럼 공격대상이 명확하면 이에 따라 분명한 목적과 동기를 가진다. (아래의 단계를 참고한다.)

오답 체크 :

(1) 단계3에서처럼 사회 공학적 방법을 사용한다.
(2) 단계1에서처럼 공격대상이 명확하다.
(3) 단계2에서처럼 가능한 방법을 총동원한다.

Tip! : APT 공격은 다음과 같은 단계를 가진다.

단계1-사전조사(Reconnaissance) : 공격자는 공격 목표에 대한 킬 체인(Kill Chain : 취약점들)을

구성하기 위해 공격 목표의 홈페이지, 외부 공개자료, 조직도, 주요 임직원 정보, 협력업체, 정보시스템 유형 및 버전, 어플리케이션의 종류 및 버전 등 공격목표에 대해 전방위적으로 정보를 수집하고 공격에 활용할 수 있는 취약점을 식별한다.
단계2-제로데이(Zero-Day) 공격 : 사전 조사된 정보를 바탕으로 정보시스템, 웹 어플리케이션 등의 알려지지 않은 취약점 및 보안시스템에서 탐지되지 않는 악성코드 등을 감염시키는 것이다.
단계3-사회공학(Social Engineering) : 공격목표의 중요 임직원 및 외부 유명인사 등을 가장하여 제로데이 취약점을 악용한 악성코드, 프로그램 등을 이메일, SNS, App 등을 통해 전송한다.
단계4-은닉(Convert) : 트로이목마 등 악성 프로그램을 설치하고 정상적인 이용자로 가장하여 시스템 접속정보 등에 대한 정보수집과 서비스 이용패턴, 방법 등에 대한 모니터링을 수행하는 것으로, 관리자 계정의 확보를 시도하여 관리자 권한으로 상승 후 수집 가능한 모든 정보를 수집한다.
단계5-적응(Adaption) : 권한상승을 통해 목표로 한 정보를 획득한 이후 공격대상의 내부 서버에 암호화하여 저장하거나 압축파일로 저장하여 비정기적으로 공격자의 단말기로 유출하는 등 공격이 탐지되지 않도록 하는 활동, 공격이 탐지 되었는지를 지속적으로 모니터링 하는 활동, 공격이 탐지된 경우 대응을 하는 활동 등을 포함한다.
단계6-지속(Persistent) : 공격자가 핵심정보를 지속적으로 유출시키기 위해 백도어 등의 프로그램을 설치하여 표적대상에 지속적으로 접근할 수 있도록 한다.

3. 다음 중 메시지 인증 코드(MAC : Message Authentication Code)에 대한 설명 중 옳은 것은?
① 메시지 무결성을 제공하지는 못한다.
② 비대칭키를 이용한다.
③ MAC는 가변 크기의 인증 태그를 생성한다.
④ 부인 방지를 제공하지 않는다.
정답 체크 :
(4) MAC은 인증과 무결성만을 제공한다. 부인방지는 전자서명이 제공한다.
오답 체크 :
(1) 메시지 무결성을 제공한다. 만약, MAC으로 HMAC(해시+대칭키=MAC)을 사용하게 되면 해시값 자체는 무결성을 제공하는데 사용한다.
(2) 대칭키를 이용한다. 대칭키를 이용해서 인증을 제공한다(통신 당사자들만 가지고 있는 것이기 때문). 비대칭키를 이용할 수도 있지만(자주 사용하는 방법이 아님) 공무원 시험 특성상 가장 틀린 답은 (4)가 된다.
(3) 고정 크기의 인증 태그를 생성한다. 고정된 인증 태그를 통해 인증과 무결성을 제공한다.

4. 다음 중 데이터베이스 관리자(Database Administrator)가 부여할 수 있는 SQL기반 접근권한 관리 명령어로 옳지 않은 것은?
① REVOKE
② GRANT
③ DENY
④ DROP
정답 체크 :
(4) DROP : DDL(데이터 구조를 정의하는 질의문)로써 데이터베이스 객체를 삭제한다.

오답 체크 :

(1) REVOKE : DCL(권한 관리를 위한 질의문)로써 이미 부여된 데이터베이스 객체의 권한을 취소한다.

(2) GRANT : DCL(권한 관리를 위한 질의문)로써 데이터베이스 객체에 권한을 부여한다.

(3) DENY : DCL(권한 관리를 위한 질의문)로써 사용자에게 해당 권한을 금지한다.

Tip! : DDL에는 CREATE(객체 생성)과 ALTER(객체 변경)이 있고, DML(데이터베이스의 운영과 사용을 위한 질의문)은 SELECT(테이블이나 뷰의 내용을 읽고 선택), INSERT(데이터 입력), UPDATE(데이터 수정), DELETE(데이터 삭제)가 있다. 이를 테이블로 정리하면 다음과 같다. 시험에 자주 출제되므로 무조건 숙지하여야 한다.

DDL(정의어)	CREATE, ALTER, DROP, RENAME, TRUNCATE
DML(조작어)	SELECT, INSERT, UPDATE, DELETE
DCL(제어어)	GRANT, DENY, REVOKE, COMMIT, ROLLBACK

5. 스위칭 환경에서 스니핑(Sniffing)을 수행하기 위한 공격으로 옳지 않은 것은?

① ARP 스푸핑(Spoofing)

② ICMP 리다이렉트(Redirect)

③ 메일 봄(Mail Bomb)

④ 스위치 재밍(Switch Jamming)

정답 체크 :

(3) Mail Bomb : 흔히 폭탄 메일이라고 하고 스팸 메일도 여기에 해당한다. 메일 서버는 각 사용자에게 일정한 양의 디스크 공간을 할당하는데, 메일이 폭주하여 디스크 공간을 가득 채우면 정작 받아야 하는 메일을 받을 수 없다. 즉 스팸 메일도 서비스 거부 공격이 될 수 있다. DoS 공격이지 스니핑(sniffing)과는 무관한다.

오답 체크 :

(1) ARP Spoofing : 거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법(sniffing)이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다.

(2) ICMP Redirect : 3계층에서 스니핑(sniffing) 시스템을 ICMP Redirect 메시지를 통해 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.

(4) Switch Jamming : 스위치의 주소 테이블의 기능을 마비시키는 공격. MACOF(MAC Flooding) 공격이라고도 한다. 스위치에 랜덤한 형태로 생성한 MAC을 가진 패킷을 무한대로 보내면, 스위치의 MAC 테이블은 자연스레 저장 용량을 넘게 되고, 스위치의 원래 기능을 잃고 더미 허브(브로드캐스팅)처럼 작동하게 된다. 공격자가 자연스럽게 브로드캐스팅된 패킷을 스니핑(sniffing)할 수 있다.

6. 다음의 지문은 무엇을 설명한 것인가?

안전한 소프트웨어 개발을 위해 소스코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 보안 활동이다.

① 시큐어코딩(Secure Coding)

② 스캐빈징(Scavenging)

③ 웨어하우스(Warehouse)
④ 살라미(Salami)
정답 체크 :
(1) 시큐어코딩 : 안전한 소프트웨어 개발을 위해 소스 코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동을 의미한다.
오답 체크 :
(2) 스캐빈징 : 컴퓨터 시스템에서 휴지통에 버린 데이터, 프로그램 리스트, 데이터 리스트, 복사하고 버린 데이터 등을 뒤져 필요한 정보를 얻는 해킹방법을 말한다.
(3) 웨어하우스 : 사용자의 의사 결정에 도움을 주기 위하여, 기간시스템의 데이터베이스에 축적된 데이터를 공통의 형식으로 변환해서 관리하는 데이터베이스를 말한다.
(4) 살라미 : 많은 사람들로부터 눈치 채지 못할 정도의 적은 금액을 빼내는 컴퓨터 사기수법의 하나이다. 이탈리아 음식 살라미소시지를 조금씩 얇게 썰어 먹는 모습을 연상시킨다고 해서 붙은 이름이다.

7. 다음은 TCSEC 보안등급 중 하나를 설명한 것이다. 이에 해당하는 것은?

• 각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다. • 보안감사가 가능하며 특정 사용자의 접근을 거부할 수 있다. • 윈도우 NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 이에 해당한다.

① C1
② C2
③ B1
④ B2
정답 체크 :
(2) C2 : 각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다. 보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있다. 윈도우 NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 C2 등급에 해당된다.
오답 체크 :
(1) C1 : 일반적인 로그인 과정이 존재하는 시스템이다. 사용자 간 침범이 차단되어 있고 모든 사용자가 자신이 생성한 파일에 대해 권한을 설정할 수 있다. 특정 파일에 대해서만 접근이 가능하다. 초기의 유닉스 시스템이 C1 등급에 해당된다.
(3) B1 : 시스템 내의 보안 정책을 적용할 수 있고 각 데이터에 대해 보안 레벨 설정이 가능하다. 시스템 파일이나 시스템에 대한 권한을 설정할 수 있다.
(4) B2 : 시스템에 정형화된 보안 정책이 존재하며 B1 등급의 기능을 모두 포함한다. 일부 유닉스 시스템이 B2 인증에 성공했다.
Tip! : TCSEC를 하나의 테이블로 정리하면 다음과 같다. 시험에 자주 출제되므로 무조건 숙지하여야 한다.

D	보안 설정이 이루어지지 않은 단계이다. (Minimal Protection)
C1	일반적인 로그인 과정이 존재하는 시스템이다. 사용자 간 침범이 차단되어 있고 모든 사용자가 자신이 생성한 파일에 대해 권한을 설정할 수 있다. 특정 파일에 대해서만 접근이 가

	능하다. 초기의 유닉스 시스템이 C1 등급에 해당된다. (Discretionary Security Protection)
C2	각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다. 보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있다. 윈도우 NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 C2 등급에 해당된다. (Controlled Access Protection)
B1	시스템 내의 보안 정책을 적용할 수 있고 각 데이터에 대해 보안 레벨 설정이 가능하다. 시스템 파일이나 시스템에 대한 권한을 설정할 수 있다. (Labeled Security)
B2	시스템에 정형화된 보안 정책이 존재하며 B1 등급의 기능을 모두 포함한다. 일부 유닉스 시스템이 B2 인증에 성공했다. (Structured Protection)
B3	운영체제에서 보안에 불필요한 부분을 모두 제거하고, 모듈에 따른 분석 및 테스트가 가능하다. 시스템 파일 및 디렉터리에 대한 접근 방식을 지정하고, 위험 동작을 하는 사용자의 활동에 대해서는 백업까지 자동으로 이루어진다. 현재까지 B3 등급을 받은 시스템은 극히 일부이다. (Security Domains)
A	수학적으로 완벽한 시스템이다. 현재까지 A1 등급을 받은 시스템은 없으므로 사실상 이상적인 시스템이다. (Verified Design)

8. 다음 중 백도어(BackDoor) 공격으로 옳지 않은 것은?

① 넷버스(Netbus)

② 백오리피스(Back Orifice)

③ 무차별(Brute Force) 공격

④ 루트킷(RootKit)

정답 체크 :

(3) 무차별 공격 : 특정한 암호(암호화키 혹은 패스워드)를 풀기 위해 가능한 모든 값을 대입하는 것을 의미한다. 대부분의 암호화 방식은 이론적으로 무차별 대입 공격에 대해 안전하지 못하며, 충분한 시간이 존재한다면 암호화된 정보를 해독할 수 있다.

오답 체크 :

백도어는 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로이다.

(1) 넷버스 : 네트워크를 통해 Microsoft Windows 컴퓨터 시스템을 원격으로 제어하기위한 소프트웨어 프로그램 이다. 1998년에 만들어졌으며 백도어로 사용될 가능성에 대해 매우 논란의 대상이 되었다(실제 백도어로 사용됨). 1998년 3월에 출시되었다.

(2) 백오리피스 : 원격 관리를 위하여 고안된 논의의 여지가 있는 컴퓨터 프로그램이다(백도어로 사용됨). 프로그램은 사용자가 원격지로부터 실행중인 마이크로소프트 윈도 운영 체제를 조절 가능하게 한다. 1998년 8월에 출시되었다.

(4) 루트킷 : 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입을 위한 백도어, 트로이목마 설치, 원격 접근, 내부 사용 흔적 삭제, 관리자 권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램의 모음이다.

9. 다음 지문에서 설명하는 방화벽으로 옳은 것은?

ㄱ. 다단계 보안을 제공하기 때문에 강력한 보안을 제공한다. ㄴ. DMZ(DeMilitarization Zone)라는 완충 지역 개념을 이용한다.

ㄷ. 설치와 관리가 어렵고 서비스 속도가 느리다는 단점이 있다.

① 베스천 호스트(Bastion host)

② 듀얼 홈드 게이트웨이(Dual homed gateway)

③ 패킷 필터링(Packet filtering)

④ 스크린드 서브넷 게이트웨이(Screened subnet gateway)

정답 체크 :

(4) 스크린드 서브넷 게이트웨이 : 스크린 호스트 게이트웨이와 듀얼 홈 게이트웨이의 변형으로, 두 개 이상의 스크린 라우터의 조합을 이용하며 베스천 호스트(Screened Host)는 격리된 네트워크인 스크린 서브넷(DMZ) 상에 위치하게 된다. 비록 베스천 호스트를 통과하여 스크린 서브넷에 접근하였다 할지라도, 내부의 스크린 라우터를 통과하여야 하므로 내부 네트워크는 매우 안정적이다.

오답 체크 :

(1) 베스천 호스트 : 네트워크에 접근하거나 떠나려고 하는 모든 실재들(entities)에 의해 접근되는 시스템 구조를 가진다. 오고 가는 트래픽에, 사전에 보안 관리자에 의해 구성된 IP 패킷에 대한 필터링(filtering) 규칙을 적용할 수 있다. 베스천 호스트는 그 자체보다는, 좀 더 정교한 네트워크 보안을 구현하기 위한 하나의 기본적인 모듈로써 이용한다.

(2) 듀얼 홈드 게이트웨어 : 두 개의 NIC를 가진 베스천 호스트(Bastion Host)를 말하며, 하나의 NIC는 외부 네트워크에 연결되고 다른 하나의 NIC는 보호하고자 하는 내부 네트워크에 연결된다. 네트워크 간의 직접적인 접근은 허용되지 않는다. 라우팅 기능이 활성화되어 있을 때, 문제가 되는 방화벽 유형이다.

(3) 패킷 필터링 : 나머지 지문은 방화벽 구축 형태(전체적인 구조)이고, 패킷 필터링은 방화벽 구성 방식(방화벽이 어떤 기능을 수행하는가?)이다. 특정한 프로토콜이나 IP 주소, 포트 번호 등을 이용하여 접근을 통제하도록 구성된 형태이다(4계층에서 동작한다).

Tip! : 방화벽의 구축 형태를 테이블의 형태로 정리하면 다음과 같다.

베스천 호스트	네트워크에 접근하거나 떠나려고 하는 모든 실재들(entities)에 의해 접근되는 시스템 구조를 가진다. 오고 가는 트래픽에, 사전에 보안 관리자에 의해 구성된 IP 패킷에 대한 필터링(filtering) 규칙을 적용할 수 있다. 베스천 호스트는 그 자체보다는, 좀 더 정교한 네트워크 보안을 구현하기 위한 하나의 기본적인 모듈로써 이용한다.
스크리닝 라우터	3계층과 4계층에서 실행되며 IP 주소와 포트에 대한 접근통제가 가능하다. 네트워크 수준의 IP 데이터그램에서는 출발지 주소 및 목적지 주소에 의한 스크린 기능. TCP/UDP 수준의 패킷에서는 포트 번호에 의한 스크린, 프로토콜별 스크린 기능을 가진다.
듀얼 홈드 게이트웨이	두 개의 NIC를 가진 베스천 호스트를 말하며, 하나의 NIC는 외부 네트워크에 연결되고 다른 하나의 NIC는 보호하고자 하는 내부 네트워크에 연결된다. 네트워크 간의 직접적인 접근은 허용되지 않는다. 라우팅 기능이 활성화되어 있을 때, 문제가 되는 방화벽 유형이다. 한 개의 NIC을 가지면 싱글 홈드 게이트웨이가 된다.
스크린드 호스트 게이트웨이	베스천 호스트와 스크린 라우터를 혼합하여 사용한 방화벽이다. 외부 네트워크와 내부 네트워크 사이에 스크린 라우터를 설치하고, 스크린 라우터와 내부 네트워크 사이에 베스천 호스트를 설치한다
스크린드 서브넷	스크린 호스트 게이트웨이와 듀얼 홈 게이트웨이의 변형으로, 두 개 이상의 스크린 라우터의 조합을 이용하며 베스천 호스트(Screened Host)는 격리된 네트워크인

게이트웨이	스크린 서브넷(DMZ) 상에 위치하게 된다. 비록 베스천 호스트를 통과하여 스크린 서브넷에 접근하였다 할지라도, 내부의 스크린 라우터를 통과하여야 하므로 내부 네트워크는 매우 안정적이다.

10. 포렌식의 기본 원칙 중 증거는 획득되고, 이송/분석/보관/법정 제출의 과정이 명확해야 함을 말하는 원칙은?

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

정답 체크 :

(3) 연계 보관성의 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) 재현의 원칙 : 법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 한다. 수행할 때마다 다른 결과가 나온다면 증거로 제시할 수 없다.

(4) 신속성의 원칙 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.

Tip! : 포렌식의 기본 원칙을 테이블로 정리하면 다음과 같다. 시험에 자주 출제되므로 무조건 숙지하여야 한다. 원칙(단어)과 설명이 맞아 떨어지므로 자연스럽게 숙지하면 된다.

정당성	모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
재현	법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 한다. 수행할 때마다 다른 결과가 나온다면 증거로 제시할 수 없다.
신속성	컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
연계 보관성	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.
무결성	수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 함을 의미한다.

11. 다음 〈보기〉가 설명하는 접근제어방식은?

〈보기〉 주체나 그것이 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 자원의 소유자 혹은 관리자가 보안관리자의 개입 없이 자율적 판단에 따라 접근 권한을 다른 사용자에게 부여하는 기법이다.

① RBAC

② DAC
③ MAC
④ LBAC
정답 체크 :
(2) DAC : 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
오답 체크 :
(1) RBAC : 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
(3) MAC : 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(4) LBAC : 객체들(자원, 컴퓨터, 어플리케이션)과 주체들(개인, 그룹, 조직) 사이의 상호작용에 기반을 둔 복잡한 접근 제어 모델이다.
Tip! : 접근 제어 방식을 테이블로 정리하면 다음과 같다. 접근 제어 방식은 자주 출제되므로 무조건 숙지하여야 한다.

ACL(리스트)	주체의 관점에서 객체들에 대한 권한을 다루거나 객체의 관점에서 주체들의 권한을 다룬다.
ACM(매트릭스)	주체와 객체 쌍에 대해 어떤 권한이 부여되었는지를 나타낸다.
MAC(강제)	주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
DAC(임의)	객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
RBAC(역할)	기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
RBAC(규칙)	규칙에 기반한 접근 제어이다. 여기서 규칙이란 “어떤 데이터는 3:00부터 6:00까지만 접근이 허용된다“와 같은 것을 의미한다.
ABAC(행위)	행위에 기반한 접근 제어이다. 하려고 하는 행위에 따라 접근 권한이 달라진다.
LBAC(격자)	객체들(자원, 컴퓨터, 어플리케이션)과 주체들(개인, 그룹, 조직) 사이의 상호작용에 기반을 둔 복잡한 접근 제어 모델이다.
Capability List(목록)	주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산 시스템 환경에서 많이 사용한다. ACL과 다른 점은 권한 위임이 가능하다(transferable).

12. 다음은 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명이다. 이들 중 옳지 않은 것은?
① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원

② 방화벽이나 게이트웨이 등에 구현
③ IP 기반의 네트워크에서만 동작
④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능함
정답 체크 :
(4) IKE(Internet Key Exchange)를 통해 신규 알고리즘을 적용할 수 있다.
오답 체크 :
(1) 메시지 암호화에 DES-CBC, 3DES, CAST-128, IDEA, RC5, Blowfish 등을 사용할 수 있다.
(2) 방화벽, 게이트웨이, 라우터 등에 구현할 수 있다.
(3) IP 기반의 네트워크에서만 동작하기 때문에 IPSec(IP Security)이다.

13. 다음의 지문은 RSA 알고리즘의 키생성 적용 순서를 설명한 것이다. ( )를 바르게 채운 것은?

ㄱ. 두 개의 큰 소수, p와 q를 생성한다. (p ≠ q)
ㄴ. 두 소수를 곱하여, n = p · q 를 계산한다.
ㄷ. (㉮)을 계산한다.
ㄹ. 1 〈 A 〈 ϕ(n)이면서 A, ϕ(n)이 서로소가 되는 A를 선택한다. A · B를 ϕ(n)으로 나눈 나머지가 1임을 만족하는 B를 계산한다.
ㅁ. 공개키로 (㉯), 개인키로 (㉰)를 각각 이용한다.

	㉮	㉯	㉰
①	ϕ(n)=(p-1)(q-1)	(n, A)	(n, B)
②	ϕ(n)=(p+1)(q+1)	(n, B)	(n, A)
③	ϕ(n)=(p-1)(q-1)	(n, B)	(n, A)
④	ϕ(n)=(p+1)(q+1)	(n, A)	(n, B)

정답 체크 :
(1)
RSA 알고리즘의 키 생성 순서는 다음과 같다.
단계-1 : N을 구한다(공개키와 개인키에 사용). N = p x q (p, q는 큰 소수)
단계-2 : L을 구한다(키쌍을 생성할 때만 사용). 초기 버전(L = (p-1) x (p-1)), 최신 버전(L = 최소공배수(p-1, q-1))
단계-3 : E를 구한다(암호화키=공개키). 1 〈 E 〈 L의 조건과 최대공약수(E, L) = 1의 조건을 만족해야 한다.
단계-4 : D를 구한다(복호화키=개인키). 1 〈 D 〈 L의 조건과 E x D mod L = 1의 조건을 만족해야 한다.

14. 스파이웨어 주요 증상으로 옳지 않은 것은?
① 웹브라우저의 홈페이지 설정이나 검색 설정을 변경, 또는 시스템 설정을 변경한다.
② 컴퓨터 키보드 입력내용이나 화면표시내용을 수집, 전송 한다.
③ 운영체제나 다른 프로그램의 보안설정을 높게 변경한다.
④ 원치 않는 프로그램을 다운로드하여 설치하게 한다.
정답 체크 :
(3) 운영체제나 다른 프로그램의 보안설정을 낮게 변경한다.

오답 체크 :
(1) 브라우저의 기본 설정이나 검색 또는 시스템 설정을 변경한다.
(2) 광고나 마케팅용 정보를 수집하거나 중요한 개인 정보를 빼낸다.
(4) 다른 프로그램을 다운로드하여 설치한다.
Tip! : 보안설정을 높게 설정하는 것은 시스템 입장에서 좋은 것이므로 스파이웨어의 주요 증상을 몰랐다고 하더라도 맞출 수 있는 문제이다. 시험장에서 문제당 시간 분배가 관건이므로 모르는 문제는 과감하게 찍고, 애매한 문제는 나중에 풀도록 한다.

15. 다음 설명에 해당하는 취약점 점검도구는?

어느 한 시점에서 시스템에 존재하는 특정경로 혹은 모든 파일에 관한 정보를 DB화해서 저장한 후 차후 삭제, 수정 혹은 생성된 파일에 관한 정보를 알려주는 툴이다. 이 툴은 MD5, SHA 등의 다양한 해시 함수를 제공하고 파일들에 대한 DB를 만들어 이를 통해 해커들에 의한 파일들의 변조여부를 판별 하므로 관리자들이 유용하게 사용할 수 있다.

① Tripwire
② COPS(Computer Oracle and Password System)
③ Nipper
④ MBSA(Microsoft Baseline Security Analyzer)
정답 체크 :
(1) Tripwire : 먼저 시스템에 존재하는 파일에 대해 DB를 만들어 저장한 후, 생성된 DB와 비교하여 추가, 삭제되거나 변조된 파일이 있는지 점검하고 관리자에게 레포팅 해 주는 무결성 검사 도구이다.
오답 체크 :
(2) COPS : 시스템 보안 감시 활동을 자동화해 주는 프로그램의 집합이다. 자신의 유닉스,리눅스 시스템에 대한 보안 감시 활동을 위한 프로그램으로써 COPS는 시스템에 침투한 외부 크래커나, 악의적인 내부 사용자들이 시스템 관리자 몰래 시스템을 변경하더라도 이 COPS 프로그램을 실행함으로써 초기에 시스템 관리자가 설정한 것과 다르게 변경된 모든 것을 보여주므로, 어느 부분이 변경되어서 시스템이 보안에 취약해졌는가를 알 수 있게 되는 것이다.
(3) Nipper : 다양한 네트워크 장비의 환경 설정에서 보안 설정 상태를 점검하는 도구이며, 주어진 각각의 장비에서 보안 문제점을 발견해서 취약점에 대한 대략적인 위험도와 함께 리포트 한다. 또한 발견된 문제점 내용에 대해 자세히 소개하고, 이를 fix 할 수 있는 방법을 알려준다.
(4) MBSA : 주로 Windows 기반 컴퓨터를 대상으로 일반적으로 잘못된 보안 구성을 찾아내고 검사하며, 관련 결과에 대한 보안 보고서를 생성한다. MBSA가 실행될 수 있는 환경은 Windows Server 2003, Windows Server 2000 및 Windows XP 등이 있다.

16. 정부는 사이버테러를 없애기 위하여 2012년 8월 정보 통신망법 시행령 개정으로 100만 명 이상 이용자의 개인 정보를 보유했거나 전년도 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 망분리를 도입할 것을 법으로 의무화했다. 다음 중 망분리 기술로 옳지 않은 것은?
① DMZ
② OS 커널분리
③ VDI

④ 가상화기술

정답 체크 :

(1) DMZ : 기업의 내부 네트워크와 외부 네트워크 사이에 일종의 중립 지역이 설치되는 호스트 또는 네트워크이다. 외부 사용자가 기업의 정보를 담고 있는 내부 서버에 직접 접근하는 것을 방지하며, 외부 사용자가 DMZ 호스트의 보안을 뚫고 들어오더라도 기업 내부의 정보는 유출되지 않는다.

오답 체크 :

(2) OS 커널분리 : VDI 방식과는 다르게 운영체제를 이중화시켜 논리적으로 망을 분리하는 OS 커널 분리 솔루션도 많이 이용되고 있다. OS 커널 분리 솔루션의 경우 VDI를 구축하는 것보다 가격이 훨씬 저렴하다. 특히 VDI는 시스템 장애 시 전체 이용자가 피해를 보지만, OS 커널 분리 방식은 하나의 PC만 장애가 발생하기 때문에 위험 관리 측면에서 우수하다.

(3) VDI : 데스크톱 가상화(VDI, Virtual Desktop Infrastructure)란 물리적으로 존재하진 않지만 실제 작동하는 컴퓨터 안에서 작동하는 또 하나의 컴퓨터를 만들 수 있는 기술이다. 한마디로 컴퓨터 속에 또 다른 가상 컴퓨터를 만들 수 있게 돕는 기술이다.

(4) 가상화기술 : 물리적인 컴퓨터 리소스의 특징을 다른 시스템, 응용 프로그램, 최종 사용자들이 리소스와 상호 작용하는 방식으로부터 감추는 기술이다. 간단하게 말하면 가상화를 적용하면 하나의 컴퓨터에서 동시에 1개 이상의 운영체제를 가동시킬 수 있다.

17. 다음 지문에서 설명하는 것은?

• 국내의 학계, 연구소, 정부 기관이 공동으로 개발한 블록 암호이다. • 경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다.

① ARIA

② CAST

③ IDEA

④ LOKI

정답 체크 :

(1) ARIA : 량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다. 블록 크기가 128비트이고, 키 크기가 128/192/256비트이다. 키 크기에 따라 라운드수가 12/14/16으로 결정된다.

오답 체크 :

(2) CAST : Carlisle Adams와 Stafford Tavares가 개발한 대칭 암호화 알고리즘이다. 128비트와 256비트 등 대형 키를 사용하여 암호화하고, 단일 키를 사용하며, 키는 암호화한 측에서 보존되고 상대방에게 전달되어 데이터를 해독한다.

(3) IDEA : 1990년에 ETH(스위스)의 라이(Lai)와 매시(Massey)가 개발한 알고리즘이다. 128비트의 키를 사용해 64비트의 평문을 8라운드에 거쳐 64비트의 암호문으로 만든다. 모든 연산이 16비트 단위로 이루어지도록 하여 16비트 프로세서에서 구현이 용이하며 주로 키 교환에 쓰인다.

(4) LOKI : DES를 대체하기 위해 만든 대칭키이다. DES와 비슷한 구조를 가지며, LOKI89, LOKI91이 존재한다.

18. 리눅스 커널 보안 설정 방법으로 옳지 않은 것은?

① 핑(ping) 요청을 응답하지 않게 설정한다.

② 싱크 어택(SYNC Attack) 공격을 막기 위해 백로그 큐를 줄인다.
③ IP 스푸핑된 패킷을 로그에 기록한다.
④ 연결 종료 시간을 줄인다.
정답 체크 :
(2) 싱크 어택(sync attack) 혹은 syn flooding 공격을 막기 위해 백로그 큐를 늘려준다. 일시적인 해결책으로, 계속된 공격을 막기 위해서는 syn cookie를 사용한다.
오답 체크 :
(1) 핑(ping) 처리도 부하이므로 요청에 응답하지 않게 설정한다.
(3) 스푸핑된 패킷이나 소스 라우팅, Redirect 패킷에 대해 로그 파일에 정보를 남긴다.
(4) TCP 연결 종료 시간을 줄인다.

19. 다음 중 XSS(Cross-Site Scripting) 공격에서 불가능한 공격은?
① 서버에 대한 서비스 거부(Denial of Service) 공격
② 쿠키를 이용한 사용자 컴퓨터 파일 삭제
③ 공격대상에 대한 쿠키 정보 획득
④ 공격대상에 대한 피싱 공격
정답 체크 :
(2) 공격 대상의 쿠키를 획득할 수는 있지만, 공격 대상의 쿠키를 이용해서 사용자 컴퓨터 파일을 삭제할 수 없다(쿠키는 실행 파일이 아니라 텍스트 파일이다).
오답 체크 :
(1) 공격 대상(서버)가 XSS가 포함된 파일을 실행하면 과부하를 일으켜 서버를 다운시킨다.
(3) 공격 대상이 XSS가 포함된 이메일을 읽으면 공격 대상의 쿠키가 공격자에게 전송된다.
(4) HTML과 javascript 등을 삽입하여 가짜 로그인 폼(username과 password)을 만든다. 그리고 사용자가 입력한 username과 password를 특정 주소로 전송되도록 하면 XSS를 이용해서 피싱 공격을 수행할 수 있다.

20. 「전자서명법」 제15조(공인인증서발급) 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급 한다. 라는 조문에서 공인인증서에 포함되지 않는 것은?
① 가입자의 전자서명검증정보
② 가입자와 공인인증기관이 이용하는 전자서명 방식
③ 공인인증서의 재발급 고유번호
④ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
정답 체크 :
(3)
“전자서명법” 제15조(공인인증서의 발급) 상 공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다. 1. 가입자의 이름(법인의 경우에는 명칭을 말한다), 2. 가입자의 전자서명검증정보, 3. 가입자와 공인인증기관이 이용하는 전자서명 방식, 4. 공인인증서의 일련번호, 5. 공인인증서의 유효기간, 6. 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보, 7. 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항, 8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격등의 표시를 요청한 경우 이에 관한 사항, 9. 공인인증서임을 나타내는 표시