2014년 서울시 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
④	⑤	⑤	③	②	①	⑤	②	④	③
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
④	⑤	④	정답 없음	②	③	①	②	①	①

1. 정보보호의 목적 중 '기밀성'을 보장하기 위한 방법만을 묶은 것은?

① 데이터 백업 및 암호화
② 데이터 백업 및 데이터 복원
③ 데이터 복원 및 바이러스 검사
④ 접근통제 및 암호화
⑤ 접근통제 및 바이러스 검사

답 ④

④ 기밀성(Confidentiality)은 허가 받지 않은 사용자가 메시지를 볼 수 없도록 숨기는 것이다. 이를 위해서 허가 받지 않은 사용자는 접근하지 못하도록 접근 통제를 하거나, 암호를 모르는 사용자는 내용을 볼 수 없도록 암호화를 해야 한다.

<오답 체크> ② 데이터 백업과 데이터 복원은 가용성을 보장하기 위한 방법

③ 바이러스 검사는 바이러스가 기본적으로 파일을 변형시킨다는 점에서 무결성에 해당하나, 바이러스가 끼치는 피해에 따라 기밀성이나 가용성이 될 수도 있다.

2. 다음 중 정보보호의 요소들에 대한 설명으로 옳은 것은?

① 부인방지(non-repudiation)란 정보가 비인가된 방식으로 변조되는 것을 방지하는 것을 의미한다.
② 무결성(integrity)이란 특정한 작업 또는 행위에 대해 책임소재를 확인 가능함을 의미한다.
③ 인증성(authenticity)이란 인가된 사용자가 필요 시 정보를 접근하고 변경하는 것이 가능함을 의미한다.
④ 가용성(availability)이란 정보나 해당 정보의 주체가 진짜임을 의미한다.
⑤ 기밀성(confidentiality)이란 정보의 비인가된 유출이 불가능함을 의미한다.

답 ⑤

<오답 체크> ① 무결성
② 책임추적성
③ 가용성
④ 인증성

3. 다음 중 가장 안전한 패스워드는 어떤 것인가?

① 75481235 ② abcd1234
③ korea2034 ④ honggildong
⑤ do@ssud23

답 ⑤

⑤ 영어 소문자, 숫자, 특수문자까지 3종류의 문자열을 사용한 ⑤번이 가장 보안성이 뛰어나다.

✠ **추가 사항**
『개인정보의 기술적·관리적 보호조치 기준』
제4조(접근통제) ⑧ 정보통신서비스 제공자 등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.
1. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

4. 다음 중 kerberos 인증 프로토콜에 대한 설명으로 옳지 않은 것은?

① Needham-Schroeder 프로토콜을 기반으로 만들어졌다.
② 대칭키 암호 알고리듬(Algorithm)을 이용한다.
③ 중앙 서버의 개입 없이 분산 형태로 인증을 수행한다.
④ 티켓 안에는 자원 활용을 위한 키와 정보가 포함되어 있다.
⑤ TGT를 이용해 자원 사용을 위한 티켓을 획득한다.

답 ③

③ 커버로스(Kerberos)는 중앙집중식 인증 시스템이다.
<오답 체크> ② 커버로스는 대칭키를 사용한다.
커버로스 버전4는 DES 알고리즘 사용
커버로스 버전5는 DES 이외의 다른 알고리즘도 사용
⑤ 자원 사용을 위한 티켓이란 서비스 티켓을 의미한다.
클라이언트는 TGS(Ticker Granting Server)에 TGT(티켓 승인 티켓)을 제시하여 서비스 티켓을 획득하고, 이 서비스 티켓을 서비스 서버에 제시함으로써 서버의 자원을 사용할 수 있다.

✠ **커버로스**(Kerberos) 작동 순서
1. 클라이언트는 사용자의 ID와 원하는 TGS ID를 인증서버(AS)에 전송
2. AS는, TGS에 보내기 위한 티켓 승인 티켓을(TGT)를 사용자의 패스워드로부터 얻은 키로 암호화한 후 클라이언트로 보낸다.
(티켓에는 재사용 방지를 위해 유효기간(lifetime)이 포함되어 있다. 티켓 승인 티켓은 클라이언트가 볼 수 없도록 인증서버와 TGS의 대칭키로 암호화되어 있다.)
3. 클라이언트는 사용자의 패스워드를 이용해 복호화를 하여 티켓 승인 티켓을 획득한다.
4. 사용자 ID, 요구하는 서비스 ID, 티켓 승인 티켓을 TGS에 전송한다.
5. TGS는 전송받은 메시지를 복호화하여 ID, 유효기간, IP와 네트워크 점검 등을 확인한 후 서비스 승인 티켓(Ticketv)를 클라이언트로 전송한다.
6. 클라이언트는 사용자 ID와 서비스 승인 티켓을 서비스 서버(응용서버)로 보낸다.
(서비스 승인 티켓은 클라이언트가 볼 수 없도록 TGS와 서비스 서버의 대칭키로 암호화되어 있다.)
7. 서비스 서버는 ID와 티켓의 내용을 확인한 후 인증을 완료한다.

5. 다음 중 공개키 암호(public key cryptosystem)에 대한 설명으로 옳은 것은?

① 대표적인 암호로 AES, DES 등이 있다.
② 대표적인 암호로 RSA가 있다.
③ 일반적으로 같은 양의 데이터를 암호화하기 위한 연산이 대칭키 암호(symmetric key cryptosystem)보다 현저히 빠르다.
④ 대칭키 암호(symmetric key cryptosystem)보다 수백 년 앞서 고안된 개념이다.
⑤ 일반적으로 같은 양의 데이터를 암호화한 암호문(ciphertext)이 대칭키 암호(symmetric key cryptosystem) 보다 현저히 짧다.

답 ②

② RSA는 소인수분해 계산의 어려움에 기반한 공개키 암호 알고리즘이다.
<오답 체크> ① AES는 SPN 구조의 대칭키 알고리즘, DES는 페이스텔(Fiestel) 구조의 대칭키 알고리즘이다.
③⑤ 공개키는 동일한 보안 수준에서 암호화·복호화 속도도 느리고, 키의 길이와 암호문의 길이도 길다.
④ 공개키 암호보다 대칭키 암호가 먼저 고안되었다.

✠ **대칭키** 암호 알고리즘
DES, 3-DES, IDEA, AES, RC5, Skipjack, Blowfish
(**국산**) SEED, HIGHT, ARIA, LEA, LSH

✠ **비대칭키** 암호(공개키 암호) 알고리즘
RSA : **소인수분해**
Rabin : **소인수분해**
ElGamal : **이산대수**
ECC : **타원곡선 상의 이산대수**
Schnorr : **이산대수, ElGamal에 기반, 짧은 키 길이**
DSA : **이산대수, Schnorr의 응용**
DSS : **이산대수, 전자서명 전용**
ECDSA : **내부적으로 타원곡선**
Knapsack : **부분집합의 합을 구하는 문제**
(NP-complete 문제)
KCDSA : **국산, 국내표준**
ECKDSA : **국산, 내부적으로 타원곡선, 소규모, 무선**

6. 다음에서 설명하고 있는 기술은?

> "이것은 디지털 컨텐츠의 저작권을 보호하기 위한 기술로 DVD와 다운로드된 음원, 유료 소프트웨어 등에 적용된다. 이는 주로 컨텐츠의 불법적인 복제나 허가받지 않은 기기에 서의 컨텐츠 소비를 방지한다."

① DRM ② IPS
③ GPL ④ VPN
⑤ DOM

답 ①

① **DRM**(Digital right management, 디지털 저작권 관리)는 각종 미디어의 출판자 또는 저작권자가 배포한 디지털 자료나 하드웨어의 사용을 제어하고 불법적인 유통을 방지하도록 사용되는 기술들을 의미한다.
<오답 체크> ② **IPS**(Instrusion Prevention System, 침입 방지 시스템)
시스템 및 네트워크 자원에 대한 다양한 형태의 침입 행위를 실시간 탐지, 분석 후 비정상으로 판단된 패킷을 차단하는 시스템이다.
IDS는 공격자의 침입을 탐지하는 반면, IPS는 탐지뿐 아니라 직접 차단 작업을 수행하는 시스템이다.
③ **GPL**(GNU General Public License, GNU 일반 공중 사용 허가서)
자유 소프트웨어에 대한 수정과 공유의 자유를 모든 사용자들에게 보장하기 위한 저작권으로, GNU 일반 공중 사용 허가서는 누구에게나 다음의 네 가지의 자유를 저작권의 한 부분으로서 보장합니다.
○ 컴퓨터 프로그램을 어떤 목적으로든지 사용할 수 있다.
○ 컴퓨터 프로그램의 복사를 언제나 프로그램의 코드와 함께 판매 또는 무료로 배포할 수 있다.
○ 컴퓨터 프로그램의 코드를 용도에 따라 변경할 수 있다.
○ 변경된 컴퓨터 프로그램 역시 프로그램의 코드와 함께 자유로이 배포할 수 있다.
④ **VPN**(Virtual Private Network, 가상사설망)
공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 데이터 암호화, 무결성, 접근 제어, 터널링, 인증 등의 보안 서비스를 제공한다.
⑤ **DOM**(Document Object Model, 문서 객체 모델)
HTML 및 XML 문서 등 구조화된 문서를 표현하는 W3C 공식 표준 API이다. 문서의 구조적 형태를 제공하므로 자바스크립트(JavaScript)와 같은 스크립트 언어를 사용하여 문서 내용과 시각적 표현을 수정할 수 있습니다.

7. 다음 중 공격자가 통신 프로토콜에 직접 개입하지 않고 감청(eavesdropping) 또는 감시(monitoring)만을 수행하는 수동적 공격(passive attack)으로 분류될 수 있는 것은?

① 가장(masquerade)
② 재사용(replay)
③ 서비스 거부(denial of service)
④ 메시지 변조(modification of message)
⑤ 트래픽 분석(traffic analysis)

답 ⑤

<오답 체크> ①②③④ 가장(신분 위장), 재사용, 서비스 거부(DoS), 메시지 변조는 모두 능동적(적극적) 공격에 해당한다.

✠ **소극적 공격**(수동적 공격)
도청(가로채기, interception)
트래픽 분석(traffic analysis)
메시지 내용 공개(release of message contents) 등

◈ **적극적 공격**(능동적 공격)
차단(interruption)
변조(modification)
위조(fabrication)
신분 위장(masquerade)
서비스 거부 공격(Dos)
재전송 공격(replay attack) 등

8. 다음의 블록 암호 모드 중 각 평문 블록을 이전 암호문 블록과 XOR한 후 암호화되어 안전성을 높이는 모드는?

① ECB 모드 ② CBC 모드
③ CTR 모드 ④ OFB 모드
⑤ CFB 모드

답 ②

② **CBC**(cipher-block chaining, 암호 블록 체인) 모드
평문 블록을 이전 단계의 암호문 블록과 XOR 한 후 암호화한다. 첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.

◈ **ECB**(electronic codebook, 전자 코드북) 모드
가장 간단한 구조로, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.

◈ **CBC**(cipher-block chaining, 암호 블록 체인) 모드
평문 블록을 이전 단계의 암호문 블록과 XOR 한 후 암호화한다. 첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.
초기화 벡터가 같은 경우 출력 결과가 같기 때문에, 매 암호화마다 다른 초기화 벡터를 사용해야 한다.

◈ **CFB**(cipher feedback, 암호 피드백) 모드
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.

◈ **OFB**(output feedback, 출력 피드백) 모드
초기화 벡터(IV)를 매 단계마다 암호화해가며 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

◈ **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

9. PKI에 관한 다음의 설명 중 옳지 않은 것은?

① PKI란 public key infrastructure의 약어로 공개키 암호 알고리듬(Algorithm)을 적용하고 인증서를 관리하기 위한 기반시스템이다.
② 주로 X.509인증서를 사용하고 있다.
③ 인증서를 발급하는 역할을 하는 기관을 CA라 한다.
④ 인증서는 대상과 공개키를 묶어주는 역할을 하며 변조를 막기 위해 대상의 서명이 추가된다.
⑤ 인증서의 폐기 여부를 확인하기 위해 사용되는 프로토콜은 OCSP이다.

답 ④

④ 공개키에는 인증기관(CA)의 서명이 추가된다.
공인된 인증기관의 공개키를 이용해 공개키 인증서의 서명을 검증함으로써 인증서가 변조되지 않았다는 것을 확인할 수 있다.

<오답 체크> ③ **CA**(Certification Authority, 인증 기관)
공개키 인증서와 인증서 폐기목록을 생성하고 발급한다.
공개키에 대한 공신력있는 인증기관

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

⑤ **OCSP**(Online Certificate Status Protocol, 온라인 인증서 상태 프로토콜)은 공개키 인증서의 폐지나 효력 정지 상태를 **실시간으로 검증**할 수 있는 프로토콜

10. DES에 대한 다음의 설명 중 옳지 않은 것은?

① 1970년대에 표준화된 블록 암호 알고리듬(Algorithm)이다.
② 한 블록의 크기는 64비트이다.
③ 한번의 암호화를 위해 10라운드를 거친다.
④ 내부적으로는 56비트의 키를 사용한다.
⑤ Feistel 암호 방식을 따른다.

답 ③

③ 페이스텔(Feistel) 구조 16라운드를 거친다.

◈ **DES**(Data Encryption Standard)
페이스텔(Feistel) **구조 16라운드**
블록 64비트
키 길이 56비트 + 패리티 8비트 = 64비트

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

11. 방화벽(Firewall)에 대한 설명으로 옳지 않은 것은?

① 허가되지 않은 외부의 공격에 대비해 시스템을 보호하기 위한 하드웨어와 소프트웨어를 말한다.
② IP 필터링을 통하여 내부 네트워크로 들어오는 IP를 차단할 수 있다.
③ 방화벽을 구축해도 내부에서 일어나는 정보유출은 막을 수 없다.
④ 방화벽을 구축하면 침입자의 모든 공격을 완벽하게 대처할 수 있다.
⑤ 방화벽은 일반적으로 라우터 또는 컴퓨터가 된다.

답 ④

④ 물리적으로 네트워크 선의 연결을 끊거나 전원을 끄지 않는 이상, 모든 공격을 완벽하게 방어할 수 있는 보안 시스템은 어디에도 없다.

<오답 체크> ③ 방화벽은 외부에서 내부로 침입하는 공격을 예방할 뿐, 방화벽 내부에서 일어나는 불법적인 정보 유출은 막을 수 없다.

12. 다음은 무엇에 대한 설명인가?

> "이것은 네트워크 상의 트랜잭션에 대한 상태 정보를 포함하는 일종의 토큰으로 주로 웹서버가 웹브라우저로 전송하여 클라이언트 쪽에 저장하고 나서 사용자가 해당 사이트를 재방문할 경우 웹브라우저가 웹서버에 재전송하는 형태로 많이 이용된다. 그러나 이는 원하지 않는 보안 상의 취약점을 야기할 수 있으므로 사용자가 이것을 주기적으로 삭제해 주는 것이 바람직하다."

① 애플릿(applet)
② URL(Uniform Resource Locator)
③ 공개키 인증서(public key certificate)
④ DOI(Digital Object Identifier)
⑤ 쿠키(Cookie)

답 ⑤

⑤ 쿠키에 대한 설명이다.
쿠키(Cookie)는 사용자가 방문하는 웹 사이트에 대한 설정 정보와 인증 정보를 사용자의 PC에 저장해두는 것이다.

▷ **Persistent Cookie**는 사용자가 웹 사이트 방문했을 때 설정한 정보(팝업창 표시 등)와 인증 정보(ID, Password 등)을 기억해두었다가, 나중에 재방문 시에 빠른 서비스를 제공하기 위한 것으로, 사용자의 하드 디스크에 저장해둔다.

▷ **Session Cookie**(세션 쿠키)는 브라우저 프로세스가 실행되고 있을 때까지만 유효한 쿠키로, 현재 연결중인 웹 사이트의 인증 정보를 유지하기 위한 것이다. 메모리 공간에 상주해있다가, 사용자가 브라우저를 종료하면 세션 쿠키는 삭제된다.

<오답 체크> ① **애플릿**(applet)이란 작은 응용프로그램을 의미하며, 웹 브라우저나 제어판과 같은 다른 프로그램에서 실행되는 소프트웨어 구성 요소를 말한다. 애플릿은 컴퓨터 프로그램과 달리 독립적으로 사용되지 않으며 작은 기능을 수행하고 제한된 보안 권한만 가지고 있다.

② **URL**(Uniform Resource Locator, 유일 자원 지시기)은 네트워크상에서 자원이 어디 있는지를 나타내는 주소 또는 규약이다. 흔히 웹 사이트 주소로 알고 있지만, URL은 웹 사이트 주소뿐만 아니라 컴퓨터 네트워크상의 자원을 모두 나타낼 수 있다.

③ **공개키 인증서**(public key certificate)는 공개키와 그에 관한 정보를 포함하는 전자 증명서이다.

④ **DOI**(Digital Object Identifier, 디지털 객체 식별자)는 ISO 표준으로, 인터넷 상의 파일이나 문서에 붙은 고유한 영구 식별자이다. 인터넷 주소가 바뀌어도 사용자는 영구 식별자를 통해 파일이나 문서의 새 주소를 찾아갈 수 있다.

13. 다음은 어떤 공격에 대한 설명인가?

> "웹사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로 사용자로 위장한 공격자가 웹사이트에 프로그램 코드를 삽입하여 나중에 이 사이트를 방문하는 다른 사용자의 웹 브라우저에서 해당 코드가 실행되도록 한다."

① HTTP 세션 탈취(session hijacking)
② 피싱(phishing)
③ 클릭 탈취(click jacking)
④ 사이트 간 스크립팅(Cross-site scripting : XSS)
⑤ 파밍(pharming)

답 ④

④ XSS에 대한 설명이다.
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.
<오답 체크> ① HTTP 세션 탈취(session hijacking) 또는 **세션 하이재킹**(Session Hijacking) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채는 공격이다.
② **피싱**(phishing)
인터넷 사용자에게 가짜 도메인을 알려주어, 가짜 사이트로 접속을 유도하는 공격이다.
③ **클릭 재킹**(click jacking)
공격자가 사용자로 하여금 알아차리지 못하게 하고 다른 것을 클릭하도록 속이는 공격이다. iframe 태그를 이용한 눈속임으로, 사용자는 어떤 웹 페이지 혹은 버튼을 클릭하지만 실제로는 다른 페이지의 콘텐츠를 클릭하게 되는 것이다.
예를 들어 사용자가 웹 페이지의 동영상 재생 버튼을 클릭하는데, 실제로는 인터넷 쇼핑 상품 구매 화면으로 연결이 되는 것이다.
⑤ **파밍**(pharming)
사용자가 자신의 웹 브라우저에서 올바른 도메인을 입력해도 가짜 웹 페이지에 접속하게 하여 개인정보를 훔치는 것이다.

14. 다음 중 IPsec에 대한 설명으로 옳지 않은 것은?

① IPsec은 network layer에서 동작한다.
② Tunnel mode에서는 기존 패킷 앞에 IPsec 헤더 정보가 추가된다.
③ IKE 프로토콜은 SA를 협의하기 위해 사용된다.
④ AH 프로토콜은 메시지에 대한 인증과 무결성을 제공하기 위해 사용된다.
⑤ ESP 헤더는 메시지의 기밀성을 제공하기 위해 사용된다.

답 **정답없음**

처음에 가답안으로는 ②번이 답이라고 발표되었으나 ②번은 맞는 내용이며, 결국 최종적으로 정답이 없는 것으로 인정되었다.
<오답 체크> ① **IPSec**(IP Security)은 용어 그대로 IP 네트워크 사이에서의 통신을 보호하기 위한 보안 서비스이다. IP는 네트워크 계층에서 작동하며, IPSec 역시 네트워크 계층에서 작동한다.
② 터널 모드에서는 내부 IP 패킷 전체(헤더+페이로드)를 인증암호화하며 앞에 새로운 IPSec 헤더가 추가된다.
전송 모드에서는 IP 페이로드와 IP 헤더 일부를 인증·암호화하며, 기존의 IP 헤더는 그대로 유지된다.
③ **IKE**(Internet Key Exchange, 인터넷 키 교환)
RSA와 디피 헬만 등의 공개키 기술을 기반으로, 암호화에 사용할 세션키를 관리하고 SA(Security Association, 보안 연계)를 협의하기 위한 프로토콜
④ **AH**(Authentication Header, 인증 헤더)
메시지 인증과 무결성 제공
⑤ **ESP**(Encapsulating Security Payload, 캡슐화 보안 페이로드)
대칭키 암호화를 통해, 기밀성과 무결성과 선택적 인증 제공

15. DDoS(Distributed Denial of Service)에 대한 설명으로 옳지 않은 것은?

① 좀비PC 가 되지 않기 위해서는 신뢰할 수 없는 기관의 프로그램은 설치하지 않는 것이 좋다.
② DDoS공격은 특정 서버에 침입하여 자료를 훔쳐가거나 위조시키기 위한 것이다.
③ 좀비PC 가 되면 자신도 모르게 특정사이트를 공격하는 수단으로 이용될 수 있다.
④ 공격을 당하는 서버에는 서비스가 중지될 수 있는 큰 문제가 발생한다.
⑤ 좀비PC 는 악성코드의 흔적을 지우기 위해 스스로 하드디스크를 손상시킬 수도 있다.

답 ②

② DDoS 공격은 시스템의 시스템을 마비시켜 이용하지 못하도록 가용성을 떨어뜨리는 공격으로, 자료를 훔쳐가거나 위조시키지는 않는다.
자료를 훔쳐가거나 위조하는 공격은 악성코드나 바이러스 등 각종 악성 소프트웨어에 해당한다.

<오답 체크> ⑤ DDoS 공격 자체는 하드디스크를 손상시키는 공격은 아니다. 하지만 좀비PC를 만들기 위해 악성코드를 심어두고, DDoS 공격이 끝난 뒤 추적을 피하기 위해 좀비PC의 기록을 지우거나 시스템을 손상시킨다.

▶ 목표 시스템이 정상적으로 처리할 수 있는 것보다 많은 양의 자원을 보내, 시스템 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격을 DoS 공격(Denial of Service, 서비스 거부 공격)이라고 하는데, **DDoS 공격**(Distributed DoS, 분산 서비스 거부 공격)은 다수의 시스템을 이용해 DoS 공격을 하는 것이다.
DDoS 공격에서 공격자는 악성코드를 통해 다수의 시스템을 감염시켜 좀비PC로 만든 뒤, 그 다수의 좀비PC를 이용해 공격을 감행한다. 공격 대상 시스템은 여러 곳으로부터 공격을 받기 때문에, 공격의 근원지를 찾기 매우 어려워진다.
DoS의 또 다른 변형 공격으로 DRDoS 공격이 있다.
DRDoS 공격(Distributed Reflect DoS, 분산 반사 서비스 거부 공격)는 패킷의 출발지 IP 주소를 공격 대상의 IP주소로 스푸핑한 TCP-SYN 패킷을 브로드캐스트로 다수의 시스템에 전송한다. 패킷을 받은 각 단말들은 이에 응답 패킷을 보내게 되는데, TCP-SYN 패킷의 출발지 IP 주소가 공격 대상의 IP 주소로 위조된 상태이기 때문에 응답 패킷은 공격 대상으로 향하게 된다. 결국 각 단말들이 보내는 응답 패킷들이 공격 대상으로 몰리게 만들어 시스템 자원을 고갈시켜 서비스를 마비시키게 된다.

16. 다음의 접근 제어 모델 중 대상 기반의 접근 제어가 아니라 특정한 역할들을 정의하고 각 역할에 따라 접근 권한을 지정하고 제어하는 방식은?

① ACL ② DAC
③ RBAC ④ MAC
⑤ Capability

답 ③

③ **역할 기반 접근 제어**(RBAC, Role Based Access Control)
정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

<오답 체크>

①⑤ **ACL**(Access Control List, 접근통제 목록)은 한 객체에 대한 주체들의 접근 권한을 명시한 리스트이며,
CL(Capability List, 접근가능 목록)은 한 주체의 객체들에 대한 접근 권한을 명시한 리스트이다.
예를 들어, '2급 기밀'이라는 객체에 대해 '김씨', '이씨', '정씨'라는 주체들에게는 허용한다고 작성한 것은 ACL에 해당하며,
주체 '김씨'가 접근 가능한 권한은 '2급 기밀', '3급 기밀', '서버 관리'라고 작성한 것은 CL에 해당한다.
ACM(Access Control Matrix, 접근통제 매트릭스)은 ACL과 CL의 결합하여, 주체들과 객체들의 접근 권한을 행렬(매트릭스) 형태로 작성한 표이다.

② 임의적 접근 제어(**DAC**, Discretionary Access Control)는 정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

④ **MAC**(Mandatory Access Control, 강제적 접근 제어)
오직 관리자만이 객체과 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안레벨에 기반한다.
관리자가 규칙을 작성하기 때문에 **규칙 기반 접근 제어**(Rule Based Access Control)이라고도 한다.

17. IDS에 관한 다음의 설명 중 옳지 않은 것은?

① IDS를 이용하면 공격 시도를 사전에 차단할 수 있다.
② 기존 공격의 패턴을 이용해 공격을 감지하기 위해 signature 기반 감지 방식을 사용한다.
③ 알려지지 않았지만 비정상적인 공격 행위를 감지해서 경고하기 위해 anomaly 기반 감지 방식을 사용한다.
④ DoS 공격, 패킷 조작 등의 공격을 감지하기 위해서는 network IDS를 사용한다.
⑤ IDS는 방화벽과 상호보완적으로 사용될 수 있다.

답 ①

① IDS(Intrusion Detection System, 침입 탐지 시스템)는 침입을 탐지만 할 뿐, 차단 작업은 수행하지 않는다.
침입을 차단하는 건 IPS(Intrusion Preventing System, 침입 방지 시스템)이나 방화벽(Firewall)이다.

<오답 체크> ② **오용 탐지**(Misuse Detection)
= 시그니처 기반(Signature Base)
= 지식 기반(Knowledge Base)
이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지

③ **이상 탐지**(Anomaly Detection IDS)
= 행위 기반(Behavior)
= 통계적 탐지(Statistical Detection)
정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지
알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능

④ **NIDS**(Network IDS, 네트워크 침입 탐지 시스템)
네트워크 트래픽을 감시하여 서비스 거부 공격(DoS 공격), 포트 스캔, 컴퓨터를 크랙하려는 시도 등과 같은 악의적인 동작들을 탐지하는 IDS 시스템

▶ **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

18. 다음 중 사용자 인증(user authentication)에 대한 설명으로 옳은 것은?

① 인터넷 뱅킹에 활용되는 OTP 단말(One Time Password Token)은 지식 기반 인증(authentication by what the entity knows)의 일종이다.
② 패스워드에 대한 사전 공격(dictionary attack)을 막기 위해 전통적으로 salt가 사용되어 왔다.
③ 통장 비밀번호로 흔히 사용되는 4자리 PIN(Personal Identification Number)은 소유 기반 인증(authentication by what the entity has)의 일종이다.
④ 지식 기반 인증(authentication by what the entity knows)의 가장 큰 문제는 오인식(False Acceptance), 오거부(False Rejection)가 존재한다는 것이다.
⑤ 건물 출입시 사용되는 ID 카드는 사람의 신체 또는 행위 특성을 활용하는 바이오 인식(biometric verification)의 일종이다.

답 ②

② 보통 사람들이 생각해내는 패스워드에는 일정한 패턴이 존재하는데, 이러한 특성을 이용해 미리 사용될 만한 패스워드 리스트를 사전으로 만들어 놓은 뒤 하나씩 대입해가면서 공격을 사전 공격(Dictionary Attack)이라고 한다.
사람이 정해놓은 일정한 패턴의 패스워드에, 패턴이 없는 무작위 문자열인 솔트(salt)를 붙이면, 패턴이 제거되는 효과가 생겨 사전 공격에 대한 내성을 높일 수 있다.

<오답 체크> ① OTP 단말기(OTP 토큰)은 소지 기반 인증이다.
③ 비밀번호, PIN은 지식 기반 인증이다.
④ 오인식과 오거부가 존재하는 것은 생체 기반 인증이다.
▶ FRR(False Rejection Rate, 오거부율): 정당한 권한이 있는 사용자가 인증에 실패할 확률
▶ FAR(False Acceptance Rate, 오인식률): 권한이 없는 사용자가 인증에 성공할 확률
⑤ ID 카드는 소지 기반 인증이다.

✠ 사용자 인증 방법
▷ 지식 기반 인증: 패스워드(password), 아이핀(i-pin), 주민등록번호, 패스프레이즈(passphrase) 등
▷ 소지 기반 인증: 열쇠, 주민등록증, OTP 토큰(보안 토큰), 스마트 카드 등
▷ 생체 기반 인증: 지문, 홍채, 얼굴, 망막, 정맥 등
▷ 행동 기반 인증: 음성, 서명 동작, 키보드 동작 등
(행동 기반 인증을 생체 기반 인증에 포함하기도 하고, 별개로 나누기도 한다.)

19. 다음에서 설명하고 있는 공격은?

> "이 공격은 할당된 메모리 경계에 대한 검사를 하지 않는 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어쓰는 방식이다. 만약 실행 코드가 덮어써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다."

① Buffer overflow 공격
② SQL injection 공격
③ IP spoofing 공격
④ Format String 공격
⑤ Privilege escalation 공격

답 ①

① 버퍼 오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.
버퍼 오버플로우 공격에 대한 대응책으로, 오버플로우 공격에 취약한 표준 라이브러리 함수를 사용하지 않고, 버퍼 경계 검사를 수행하는 방법 등이 있다.

<오답 체크> ② **SQL 삽입**(SQL 인젝션, SQL injection) 공격
클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격이다.

③ **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 가능해진다.

④ **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

⑤ **Privilege escalation**(권한 확대) 공격
운영체제나 소프트웨어의 버그나 설계결함, 취약점 등을 이용해, 애플리케이션이나 시스템의 보호되는 자원에 대한 접근 권한을 얻는 행동을 말한다. 공격자는 애플리케이션 개발자나 시스템 관리자가 의도한 것보다 높은 수준의 권한을 얻어서 개발자나 관리자가 예상치 못한 악의적인 행동을 할 수 있게 된다.

20. 다음 중 개인정보 보호법에 대한 설명으로 맞는 것은?

① 개인정보 보호위원회의 위원은 대통령이 임명한다.
② 정보주체란 개인정보를 생성 및 처리하는 자를 의미한다.
③ 개인정보는 어떠한 경우에도 제3자에게 제공되거나 공유되어서는 안된다.
④ 개인정보의 처리 목적이 달성된 이후에는 개인정보를 1년간 보관하여야 한다.
⑤ 보호 대상이 되는 개인정보는 주민등록번호 등을 포함하여 생존 및 사망한 개인을 식별할 수 있는 정보를 의미한다.

답 ①

① **「개인정보 보호법」 제7조(개인정보 보호위원회)** 4항
위원은 다음 각 호의 어느 하나에 해당하는 사람을 대통령이 임명하거나 위촉한다. 이 경우 위원 중 5명은 국회가 선출하는 자를, 5명은 대법원장이 지명하는 자를 각각 임명하거나 위촉한다.
1. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
2. 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람
3. 그 밖에 개인정보에 관한 학식과 경험이 풍부한 사람

<오답 체크> ② 개인정보처리자에 대한 정의이다.
정보주체란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

③ 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

④ 제21조(개인정보의 파기)
개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 **그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기**하여야 한다.

⑤ 제2조(정의)
1. "개인정보"란 **살아 있는 개인에 관한 정보**로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.