

2017 년 서울시 9 급 정보보호론 풀이

by 호이호이꿀떡

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 시스템이다.

- ① MDM ② FDS
③ MDC ④ RPO

답 ②

- ② FDS(Fraud Detection System, 이상 거래 탐지 시스템)은 전자금융거래에 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심거래를 탐지하고 이상금융거래를 차단하는 시스템이다.

<오답 체크> ① MDM(Master Data Management, 마스터 데이터 관리)는 자주 변하지 않으면서 여러 업무 및 프로세스에 공통적으로 참조되고 활용되는 전사 관점의 기준정보를 의미한다.

MDM(Mobile Device Management, 모바일 기기 관리)란 스마트폰이나 태블릿, 휴대용 컴퓨터와 같은 모바일 기기를 보호, 관리, 감시, 지원하는 일련의 과정을 의미한다.

- ③ MDC(Modification Detection Code, 메시지 변경 감지 코드)는 메시지가 위·변조되지 않았다는 것을 보장하는 메시지 다이제스트.

- 수신한 메시지의 MDC 를 계산하고 송신측이 보내준 MDC 와 비교하여 동일한지 비교함.

- ④ RTO(Recovery Time Objective)는 서버에 장애가 발생하였을 때 장애 복구를 수행하고 서비스가 정상적으로 다시 복구될 때까지 걸리는 시간을 의미한다.

RPO(Recovery Point Objectives)는 시스템에 장애가 발생했을 때 시스템의 복원시점을 어디에 맞추는가에 대한 기준으로, 재해로 인해 데이터를 손실할 경우 어디까지 허용할 수 있는냐에 따라 결정된다.

정답 체크 ①②③④⑤

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

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.

답 ④

APT(Advanced Persistent Threats, 지능형 지속 공격)

개인이나 단체, 국가, 또는 사업체나 정치 단체를 표적으로 삼아, 목적을 달성하기 위해 오랜 시간 동안 정보를 수집하고 다각도로 연구하여 고급 기술을 동원해 공격하는 기법을 말한다.

- ④ APT 공격은 명확한 공격 대상을 정해놓고 철저한 준비를 통해 공격한다.

<오답 체크> ①③ APT 공격은 가능한 모든 수단을 동원한다. 제로 데이 공격, 악성코드 유포, 사회공학적 기법 등 가능한 모든 수단을 동원한다. 심지어 일부는 회사에 직접 침입하기도 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 MAC 는 가변 크기의 인증 태그를 생성한다.
- ④ 부인 방지를 제공하지 않는다.

답 ④

메시지 인증 코드(MAC: Message Authentication Code)는 대칭 키를 사용하는 해시값으로, 무결성과 출처 인증(송신자에 대한 인증)이 가능하다.

- ④ 출처 인증은 가능하지만, 부인 방지는 불가능하다.
송신자 인증(출처 인증)은 통신 당사자간 상대방의 신원을 확인할 수 있는 것을 의미한다. MAC 는 대칭키를 사용하기 때문에 네트워크 상의 상대방이 자신과 같은 비밀키를 가진 특정인이라는 걸 확인할 수 있다.
부인 방지는 누가 어떤 내용의 메시지를 보냈는지, 메시지의 전송 및 수신에 대한 사실 제 3 자에게 증명하는 것으로 MAC 는 대칭키를 사용하기 때문에 누가 보내고 누가 받은 것인지 제 3 자는 구별할 수 없다.

<오답 체크> ① 해시를 이용하며 무결성을 제공한다.

- ② 대칭키를 사용한다.
- ③ 해시와 동일하게 고정 크기의 출력값(인증 태그)을 생성한다.

4. 다음 중 데이터베이스 관리자(Database Administrator)가 부여할 수 있는 SQL 기반 접근 권한 관리 명령어로 옳지 않은 것은?

- ① REVOKE ② GRANT
③ DENY ④ DROP

답 ④

- ④ DROP 명령어는 테이블이나 뷰, 계정 등을 삭제하는 명령어로, 접근 권한을 조정할 때는 사용하지 않는다.

<오답 체크> ① REVOKE: 사용자에게 부여했던 권한을 취소

- ② GRANT: 사용자에게 허용 권한을 부여
- ③ DENY: 사용자에게 접근 금지를 설정

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

- ① ARP 스푸핑(Spoofing)
- ② ICMP 리다이렉트(Redirect)
- ③ 메일 폭탄(Mail Bomb)
- ④ 스위치 재밍(Switch Jamming)

답 ③

- ③ 메일폭탄(Mail Bomb)은 엄청난 양의 전자우편을 보내 서버에 할당되어 있는 수신자의 디스크 용량을 단순히 채워버려 중요 메일을 받지 못하게 하고, 다량의 메일을 처리하느라 서버의 자원이 고갈되어 서버의 작동을 멈추게 할 수도 있는 DoS 공격 중 하나이다.

<오답 체크> ① ARP 스푸핑은 공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격으로, 공격 대상으로 보내지는 패킷을 가로채 스니핑을 하는 것이 목적이다.

- ② ICMP 리다이렉트(또는 ICMP 스푸핑)
공격자는 공격 대상에게 ICMP 리다이렉트 메시지를 보내, 자신이 공격 대상의 게이트웨이 역할을 하게 만든다. 그러면 공격 대상이 보내는 메시지는 게이트웨이인 공격자를 통하게 되므로 스니핑이 가능해진다.

- ④ 스위치 재밍(Switch Jamming)은 위조된 MAC 주소를 지속적으로 보내 스위치가 관리하는 매핑 테이블을 넘치게 만드는 스니핑 기법이다.
스위치는 매핑 테이블이 가득 차게 되면, 스위치는 브로드캐스팅(broadcasting) 모드로 전환하게 되어 스니핑이 가능해진다.

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)

답 ①

- ① 제시된 지문은 소프트웨어 개발 보안 또는 시큐어 코딩(Secure Coding)에 대한 위키백과의 설명이다.

<오답 체크> ② 스캐빈징(Scavenging)은 컴퓨터실에서 작업하면서 휴지통에 버린 프로그램 리스트, 데이터 리스트, 복사된 자료 등을 통해 중요 정보를 얻는 해킹 방법이다. 의외로 중요한 정보를 획득할 수 있는 경우도 있다.

- ③ 데이터 웨어하우스(Data Warehouse, DW)는 기업의 대단위 데이터를 사용자 관점에서 주제별로 통합하여 축적하여 별도의 장소에 저장해 놓은 것이다. 단순한 데이터의 저장고가 아니라, 데이터를 다차원으로 분석하여 의사결정에 도움을 준다.

- ④ 살라미(Salami) 기술은 많은 사람들로 부터 눈치채지 못할 만큼의 금액을 빼내어 가는 사기 수법이다. 예를 들면, 은행의 금리 계산 과정에서 1의 자리의 단수를 버리지 않고 자신의 계좌로 보내 착복하는 것이다.

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

- 각 계정별 로그인 가능하며 그룹 ID 에 따라 통제가 가능한 시스템이다.
- 보안감사가 가능하며 특정 사용자의 접근을 거부할 수 있다.
- 윈도우 NT 4.0 과 현재 사용되는 대부분의 유닉스 시스템이 이에 해당한다.

- ① C1 ② C2
③ B1 ④ B2

답 ②

< TCSEC 보안 등급 >

- **A1 Verified Design**(검증된 보호)
수학적으로 완벽한 시스템
- **B3 Security Domains**(보안 영역)
운영체제에서 보안에 불필요한 부분을 모두 제거
모듈에 따른 분석 및 테스트가 가능
시스템 파일 및 디렉터리에 대한 접근 방식을 지정하고
위험 동작을 하는 사용자의 활동에 대해서는 백업까지 자동
으로 이루어짐
- **B2 Structured Protection**(계층 구조화된 정보보호)
시스템에 정형화된 보안 정책이 존재
일부 유닉스 시스템이 B2 인증에 성공
- **B1 Labeled Security**(레이블된 정보보호)
시스템 내의 보안 정책을 적용할 수 있으며 각 데이터에
대해 보안 레벨 설정이 가능
시스템 파일이나 시스템에 대한 권한을 설정
- **C2 Controlled Access Protection**(통제된 접근보호)
각 계정별 로그인 가능하며 그룹 ID 에 따라 통제가 가
능한 시스템
보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있
음
윈도우 NT 4.0 과 현재 사용되는 대부분의 유닉스 시스템이
이 등급에 해당
상용 프로그램을 위한 최소한의 요구 등급
- **C1 Discretionary Security Protection**(임의적 접근보호)
일반적인 로그인 과정이 존재하는 시스템.
사용자간 침범이 차단되어 있고 모든 사용자가 자신이 생
성한 파일에 대해 권한을 설정할 수 있으며, 특정 파일에
대해서만 접근이 가능
초기의 유닉스 시스템이 C1 등급
- **D Minimal Protection**(최소한의 보호)
보안 설정이 이루어지지 않은 단계

8. 다음 중 백도어(BackDoor) 공격으로 옳지 않은 것은?

- ① 넷버스(Netbus)
② 백오리피스(Back Orifice)
③ 무차별(Brute Force) 공격
④ 루트킷(RootKit)

답 ③

백도어(Backdoor)는 인증 과정을 거치지 않고, 접근할 수 있도
록 만든 비밀 통로이다. = 트랩도어(Trapdoor)

③ 무차별 공격(Brute Force Attack)은 특정 패턴을 사용하지
않고, 패스워드로 사용 가능한 모든 문자열, 숫자열을 대입
해가는 공격 방법이다.

백도어와는 상관이 없다.

<오답 체크> ① 넷버스(Netbus)는 원격으로 다른 사람의 컴
퓨터를 조작할 수 있는 크래킹 도구이다.

② 백오리피스(Back Orifice)는 원격 관리를 위하여 고안된 컴
퓨터 프로그램으로, 사용자가 원격지로부터 실행중인 마이
크로소프트 윈도 운영 체제를 조작 가능하게 한다.

④ 루트킷(RootKit)은 해커들이 컴퓨터나 또는 네트워크에 침입
한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득
하는데 사용하는 도구의 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)

답 ④

- ④ 스크린드 서브넷 게이트웨이(Screened Subnet Gateway)
외부 네트워크와 내부 네트워크 사이에 서브넷(Subnet)이라는 완충지대를 두며, 서브넷에는 주로 DMZ 와 방화벽이 위치한다.
내부 네트워크와 서브넷 사이에 스크리닝 라우터 1 개, 외부 네트워크와 서브넷 사이에도 스크리닝 라우터 1 개, 총 2 개의 스크리닝 라우터가 들어간다.
- <오답 체크> ① 베스천 호스트(Bastion host)는 내부 네트워크와 외부 네트워크 사이에 위치하는 게이트웨이이다. 내부 네트워크와 외부 네트워크를 분리하여, 외부에서 내부로의 직접 연결을 차단하여 보안성을 높인다.
- ② 듀얼 홈드 게이트웨이(Dual homed gateway)는 두개의 네트워크 인터페이스를 가진 베스천 호스트를 말하며, 하나의 네트워크 인터페이스는 인터넷 등 외부 네트워크에 연결되고, 다른 하나의 네트워크 인터페이스는 내부 네트워크에 연결된다. 양 네트워크 간의 라우팅은 존재하기 때문에 양 네트워크 간의 직접적인 접근은 허용되지 않는다.
- ③ 패킷 필터링 방화벽(Packet filtering Firewall)은 OSI 7 계층 중 네트워크 계층과 전송 계층 사이에서 작동하며, 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등의 규칙을 설정하여 접속제어를 수행한다.

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

답 ③

< 포렌식의 원칙 >

- 재현의 원칙: 증거를 복구하는 과정에서 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함
- 정당성의 원칙: 모든 증거는 적법한 절차를 거쳐서 획득하여야 함
- 신속성의 원칙: 시스템 안의 디스크 또는 메모리 정보가 휘발되기 전에 빠르게 획득하여야 함
- 연계보관성의 원칙: 증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 함
- 무결성의 원칙: 증거가 위조/변조되어서는 안 됨

11. 다음 <보기>가 설명하는 접근제어방식은?

< 보 기 >

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

답 ②

- ② Discretionary Access Control(**DAC**, 임의적 접근 제어)
정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.
보기의 '신원에 근거하여 객체에 대한 접근 제한', '보안관리자의 개입 없이 자율적 판단에 따라'의 문장을 통해 임의적 접근 제어임을 알 수 있다.

<오답 체크> ① Role Based Access Control(**RBAC**, 역할 기반 접근 제어)

정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

- ③ 강제적 접근 제어(**MAC**, Mandatory Access Control)
조직 관리자만이 객체와 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.

- ④ 레이블 기반 접근 제어(**LBAC**, Label Based Access Control)
레이블에 근거해 액세스의 접근을 결정

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

답 ④

IPSec(IP Security)은 IP 패킷을 암호화하고 인증하는 안전한 인터넷 프로토콜(IP) 통신을 위한 프로토콜이다.

- ④ 신규 알고리즘 적용이 가능하다.

<오답 체크> ① IPSec은 DES-CBC, RC5, Blowfish 등 대칭키를 이용해 암호화를 한다.

- ③ IPSec(IP Security)은 용어 그대로 IP 네트워크 사이에서의 통신을 보호하기 위한 보안 서비스이다.

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

ㄱ. 두 개의 큰 소수, p 와 q 를 생성한다. ($p \neq q$)
 ㄴ. 두 소수를 곱하여, $n = p \cdot q$ 를 계산한다.
 다. (㉔)을 계산한다.
 ㄹ. $1 < A < \phi(n)$ 이면서 $A, \phi(n)$ 이 서로소가 되는 A 를 선택한다. $A \cdot B$ 를 $\phi(n)$ 으로 나눈 나머지가 1임을 만족하는 B 를 계산한다.
 ㅁ. 공개키로 (㉓), 개인키로 (㉔)를 각각 이용한다.

- | ㉓ | ㉔ | ㉕ |
|--------------------------|----------|----------|
| ① $\phi(n) = (p-1)(q-1)$ | (n, A) | (n, B) |
| ② $\phi(n) = (p+1)(q+1)$ | (n, B) | (n, A) |
| ③ $\phi(n) = (p-1)(q-1)$ | (n, B) | (n, A) |
| ④ $\phi(n) = (p+1)(q+1)$ | (n, A) | (n, B) |

답 ①

- ① 먼저 구한 A 를 암호화키로 이용하고, 나중에 구한 B 를 복호화키로 이용한다.

14. 스파이웨어 주요 증상으로 옳지 않은 것은?

- ① 웹브라우저의 홈페이지 설정이나 검색 설정을 변경, 또는 시스템 설정을 변경한다.
- ② 컴퓨터 키보드 입력내용이나 화면표시내용을 수집, 전송한다.
- ③ 운영체제나 다른 프로그램의 보안설정을 높게 변경한다.
- ④ 원치 않는 프로그램을 다운로드하여 설치하게 한다.

답 ③

- 스파이웨어(Spyware)는 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어로, 신용카드와 같은 금융 정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집하는 기능을 한다.
- ③ 공격자가 사용자의 컴퓨터 정보를 빼내기 수월하기 위해서는 보안 설정을 낮게 변경해야 한다.

15. 다음 설명에 해당하는 취약점 점검도구는?

어느 한 시점에서 시스템에 존재하는 특정경로 혹은 모든 파일에 관한 정보를 DB 화해서 저장한 후 차후 삭제, 수정 혹은 생성된 파일에 관한 정보를 알려주는 툴이다. 이 툴은 MD5, SHA 등의 다양한 해시 함수를 제공하고 파일들에 대한 DB 를 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)

답 ①

- ① Tripwire(트립와이어)는 시스템의 특정한 파일의 변화를 모니터링하고 알람을 해주는 유용한 보안 그리고 무결성 도구이다.

관리자에 의해 파일 시스템을 스캔하고, 스캔된 파일들의 정보를 각각 데이터베이스에 저장한다. 이후 같은 파일을 스캔해서 데이터베이스에 저장된 결과와 비교한다.

암호화 해시 함수들이 파일의 변화를 탐지하는데 사용되므로 파일의 전체 내용을 데이터에 저장할 필요가 없다.

<오답 체크> ② COPS(Computer Oracle and Password System)은 시스템 보안 감시활동을 자동화해주는 프로그램의 집합이다.

- ③ Nipper 는 네트워크 장비의 취약점을 점검해주는 도구로, 오픈 소스 프로그램이다.

- ④ MBSA(Microsoft Baseline Security Analyzer)는 마이크로소프트의 윈도우즈 기반 컴퓨터를 검사하여 일반적으로 잘못된 보안 구성을 찾아내고 검사하는 각 컴퓨터에 대해 개별 보안 보고서를 생성하는 도구이다.

16. 정부는 사이버테러를 없애기 위하여 2012 년 8 월 정보통신망법 시행령 개정으로 100 만 명 이상 이용자의 개인정보를 보유했거나 전년도 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 망분리를 도입할 것을 법으로 의무화했다. 다음 중 망 분리 기술로 옳지 않은 것은?

- ① DMZ
- ② OS 커널분리
- ③ VDI
- ④ 가상화기술

답 ①

망분리는 내부 네트워크망과 외부 네트워크망을 분리하여 외부로의 침입을 막고 내부 정보의 유출을 막기 위한 기술을 말한다.

물리적 망분리는 말 그대로 물리적으로 네트워크망을 분리한 것이다. 외부의 네트워크와 내부의 네트워크를 별도로 구성하여 물리적으로 분리가 되어 있기 때문에, 가시성이 확보되어 분리된 상태를 눈으로 직접 확인할 수 있고 시스템적으로 완전하다는 것이다.

논리적 망분리는 하나의 단말기에 가상화 기술을 적용하여 각 업무 영역별로 분리하여 사용하는 것이다. 하나의 PC로 업무를 처리할 수 있어 물리적 망분리보다 편리하다.

- ① DMZ(demilitarized zone, 비무장지대)

내부 방화벽과 외부 방화벽 사이에 위치한 서브넷으로, DMZ 내의 컴퓨터는 오직 외부 네트워크에만 연결되어 있고, 내부 네트워크로 연결할 수 없다.

(DMZ 기술도는 망분리 기술로 분류되지는 않지만, 네트워크망을 내부와 외부로 나누어 운영한다는 점에서 망분리와 유사한 개념이긴 하다.)

<오답 체크> ② OS 커널분리는 논리적 망분리로, 하나의 PC에 두 개의 운영체제를 설치하여 독립적으로 실행하는 기술이다.

- ③ VDI(Virtual Desktop Infrastructure, 가상 데스크탑 인프라)는 논리적 망분리 기술로, 데스크탑을 가상화하고 이를 중앙에서 사용자 환경으로 제공하는 것을 말한다.

OS, 사용자 정보 및 데이터가 사용자의 노트북이나 데스크탑에 직접 저장되는 것이 아니라, 모든 데스크탑 데이터는 IT 관리자가 중앙에서 관리하는 서버에서 실행되는 방식이다.

- ④ 가상화 기술은 논리적 망분리 기술로, 컴퓨터 안의 다른 가상의 컴퓨터를 생성하여 프로그램을 사용하는 것이다. 서버 기반 컴퓨팅(SBC, Server Based Computing)과 클라이언트 기반 컴퓨팅(CBC, Client Based Computing)이 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

답 ①

- ① ARIA
128 비트 블록
키 길이 128/192/256 비트
Involutional SPN 구조 12/14/16 라운드
KS 국가 표준, 효율성에 맞게 최적화, 다양한 환경에 적합
Academy(학계), Research Institute(연구소), Agency(정부 기관)의 약자이다.

<오답 체크>

- ② CAST-128: 128 비트 키와 64 비트 블록
CAST-256: 256 비트 키와 128 비트 블록
③ IDEA: 키 길이 128 비트, 64 비트 블록, 8 라운드
④ LOKI97
128, 192, 256 비트 길이의 키

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.

답 ②

- ② 백로그 큐(BackLog Queue)는 동시에 서버에 연결을 시도할 수 있는 클라이언트의 최대 수를 의미한다.
SYN 공격은 다량의 SYN 패킷을 이용해 목표 대상 서버가 수용할 수 있는 트래픽을 모두 점유하여 다른 정상적인 이용자가 서버에 접속하지 못하게 하는 것이다.
따라서 SYN 공격을 예방하기 위해서는 백로그 큐를 늘려, 동시에 연결을 시도할 수 있는 이용자 수를 늘려줘야 한다.

<오답 체크> ① ping 명령어는 해당 호스트가 접속 가능한지를 테스트하는 명령어인데, ping 명령어에 쓰이는 ICMP 패킷을 이용한 서비스 거부 공격(DoS, DDoS)가 자주 발생하기 때문에 ping 패킷을 무시하도록 설정하는 경우도 많다.

- ④ 클라이언트와 서버가 FIN 패킷을 보냈다고 바로 연결을 종료하는 게 아니다. 일련의 FIN_WAIT 와 TIME_WAIT 등의 상태를 거쳐 연결이 종료되는 것이다.
연결 종료 시간은 FIN 패킷을 보내 연결 종료 요청을 하고 실제 연결이 종료되기까지의 시간인데, 이 동안에도 연결은 유지된 상태이기 때문에 서버의 이용 가능한 자원을 점유하고 있는 상태인 것이다.
따라서 불필요한 서버의 자원을 낭비하지 위해 연결 종료 시간을 줄여야 한다.

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

답 ②

크로스 사이트 스크립팅(XSS, Cross-site Scripting)는 웹 사이트에 악성 스크립트를 삽입한 뒤, 다른 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.

기본적으로는 쿠키 정보를 획득하여 개인정보를 유출하는 것인데, 이 쿠키를 조작하여 세션 하이재킹, 요청 위변조, 공격자가 지정한 사이트로 강제 연결 등에 악용할 수 있다. 또한 XSS 공격을 받은 클라이언트는 좀비 PC가 되어 분산 서비스 거부 공격(DDoS)에 이용될 수 있다.

- ② XSS 공격은 사용자 컴퓨터의 파일을 삭제하거나 변조하는 직접적인 피해는 주지 못한다.

20. “「전자서명법」 제 15 조(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 경우에 관한 사항

답 ③

- ③ ‘공인인증서의 재발급 고유번호’가 아니고, ‘공인인증서의 고유번호’이다.

「전자서명법」

제 15 조(공인인증서의 발급)

- ① 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다. 이 경우 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하여야 한다.
- ② 공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다.
 1. 가입자의 이름(법인의 경우에는 명칭을 말한다)
 2. 가입자의 전자서명검증정보 (<- 공개키를 의미한다.)
 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 제 3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항
 9. 공인인증서임을 나타내는 표시