

국가직 7급 공개채용시험

-2014년 7월 26일 시행

1. 2014년 7급

이미지 파일 또는 MP3 파일 등에 인지하지 못할 정도의 미세한 변화를 주어 정보를 숨기는 기술은? (난이도:2)

- ① 스테가노그래피(Steganography)
- ② 워터마킹(Watermarking)
- ③ 핑거프린팅(Fingerprinting)
- ④ 암호(Cryptography)



워터마킹이란 용어는 지폐의 제조과정에서 위조지폐를 가리기 위해 물에 젖은 상태에서 특정 그림을 인쇄하고 말린 후 불빛에 비추었을 때 그림이 보이도록 하는 기술에서 유래했다. 현재는 저작권 정보를 원본의 내용의 왜곡하지 않는 범위에서 혹은 사용자가 인식하지 못하도록 디지털 컨텐트에 삽입하는 기술을 말한다.

① 스테가노그래피(steganography)는 읽지 못하게 하는 것이 아니라 메시지의 존재 자체를 숨기는 기법이다. 일반적으로 사진파일에 인간이 인지하지 못할 정도의 미세한 부분에 변화를 주어 정보를 입력하는 방식이 많이 사용된다.

정답 ①

2. 2014년 7급

대표적인 공격 유형으로 방해(interrupt)와 가로채기(intercept), 위조(fabrication), 변조(modification) 공격이 있다. 이 중 가로채기 공격에서 송수신되는 데이터를 보호하기 위한 정보보호 요소는? (난이도:1)

- ① 기밀성(Confidentiality)
- ② 무결성(Integrity)
- ③ 인증(Authentication)

④ 부인방지(Non-Repudiation)



① 가로채기(interception)는 기밀성에 영향을 주고, 방해(interruption)은 기용성에 영향을 주며, 변조(modification)와 위조(fabrication)는 무결성에 영향을 준다.

정답 ①

3. 2014년 7급

다음은 공개키 암호 시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고, 이를 복호화하는 과정에 대한 설명이다. ① ~ ⑤에 들어갈 내용으로 옳은 것은? (난이도:3)

- 보기
- ㄱ. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
 - ㄴ. Bob은 (①)를 Alice에게 전송한다.
 - ㄷ. Alice는 (②)를 사용하여 메시지를 암호화한다.
 - ㄹ. Alice는 생성된 암호문을 Bob에게 전송한다.
 - ㅁ. Bob은 (⑤)를 사용하여 암호문을 복호화한다.

- | | | |
|------------|------------|------------|
| ① Bob의 공개키 | Alice의 공개키 | Alice의 개인키 |
| ② Bob의 개인키 | Bob의 공개키 | Bob의 개인키 |
| ③ Bob의 개인키 | Alice의 공개키 | Alice의 개인키 |
| ④ Bob의 공개키 | Bob의 공개키 | Bob의 개인키 |



- 오늘 피하기** ④ 앤리스가 밥에게 메시지를 보낸다고 가정할 때 통신의 흐름은 아래와 같다.
- 밥은 공개키/개인키로 이루어진 한 쌍의 키($K_{B(\text{pub})}/K_{B(\text{pri})}$)를 만든다.
 - 밥은 자신의 공개키($K_{B(\text{pub})}$)를 앤리스에게 보낸다.
 - 앤리스는 밥의 공개키를 써서 메시지(P)를 암호화($C = E(K_{B(\text{pub})}, P)$) 한다.
 - 앤리스는 암호문(C)을 밥에게 보낸다.
 - 밥은 자신의 개인키($K_{B(\text{pri})}$)로 암호문을 복호화($P = D(K_{B(\text{pri})}, C)$) 한다.

정답 ④

4. 2014년 7급

해시 함수(Hash Function)의 특징에 대한 설명으로 옳지 않은 것은? (난이도:2)

- ① 임의의 메시지를 입력받아, 고정된 길이의 해시 값으로 출력한다.
- ② 암호학적으로 안전한 해시 함수를 설계하기 위해서는 역상 저항성(preimage resistance) 및 충돌 저항성(collision resistance)의 기준을 충족해야 한다.
- ③ 일반적으로 데이터 암호화에 사용된다.
- ④ 종류에는 SHA-1, MD5, HAS-160 등이 있다.



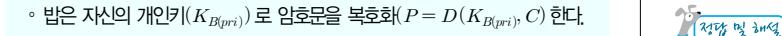
- 오늘 피하기** ③ 해시 알고리즘의 주요 응용분야는 전자서명, 중요 정보의 무결성 확인 등이다. 데이터 암호화에 주로 사용되는 것은 대칭키 암호이다.

정답 ③

5. 2014년 7급

RSA 암호화 알고리즘에 대한 설명으로 옳지 않은 것은? (난이도:3)

- ① 비대칭키를 이용한 부인방지 기능을 포함한다.
- ② AES 암호화 알고리즘보다 수행 속도가 빠르다.
- ③ 키 분배 및 관리가 용이하다.
- ④ 전자서명 등 응용 범위가 매우 넓다.



- 오늘 피하기** ② AES와 같은 대칭키 암호화 알고리즘은 RSA와 같은 비대칭키 암호화 알고리즘보다 수행속도가 빠르다.

정답 ②

6. 2014년 7급

개인정보보호관리체계(PIMS)에 대한 설명으로 옳지 않은 것은? (난이도:3)

- ① 내부 정보 유출을 방지하기 위해, 인증 과정에 외부 전문가는 포함되지 않는다.
- ② PIMS 인증 취득 기업이 사고 발생 시 과징금, 과태료가 경감된다.
- ③ 인증 심사 기준은 개인정보관리과정과 개인정보보호대책, 개인정보생명주기 등이 있다.
- ④ PIMS는 기업이 자율적으로 심사를 신청하는 자율 제도로 운영한다.



- PIMS(Personal Information Management System) 인증제도는 기업이 전사차원에서 개인정보보호 활동을 체계적·지속적으로 수행하기 위해 필요한 일련의 보호조치체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도이다.
- PIMS 인증 취득 기업이 개인정보보호 법규 위반 시 과징금/과태료 감경 혜택을 부여한다.

① 인증심사원은 각 분야별 외부전문가로 구성된다.

①

7. 2014년 7급

영국, 독일, 네덜란드, 프랑스 등 유럽 국가에서 평가 제품의 상호 인정 및 정보보호 평가 기준의 상이함에서 오는 시간과 인력 낭비를 줄이기 위해 제정한 유럽형 보안 기준은? (난이도:2)

- ① CC(Common Criteria)
- ② ITSEC(Information Technology Security Evaluation Criteria)
- ③ TCSEC(Trusted Computer System Evaluation Criteria)
- ④ ISO/IEC JTC 1



② ITSEC은 독일, 프랑스, 네덜란드, 영국 등 유럽 4개국이 평가제품의 상호인정 및 평가기준이 상이함에 따른 불합리함을 보완하기 위하여 작성한 유럽형 보안기준이다.

②

8. 2014년 7급

보안 사고에 대한 설명으로 옳지 않은 것은? (난이도:3)

- ① 파밍(pharming)은 신종 인터넷 사기 수법으로 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.
- ② 스파이웨어(spyware)는 사용자의 동의 없이 시스템에 설치되어, 금융 정보 및 마케팅용 정보를 수집하거나 중요한 개인 정보를 빼내가는 악의적 프로그램을 말한다.
- ③ 피싱(phishing)은 금융기관 등의 웹 사이트에서 보낸 이메일(email)로 위장하여, 링크를 유도해 타인의 인증 번호나 신용 카드 번호, 계좌 정보 등을 빼내는 공격 기법이다.
- ④ 스니핑(sniffing)은 백 도어(backdoor) 등의 프로그램을 사용하여, 원격에서 남의 패킷 정보를 도청하는 해킹 유형의 하나로 적극적 공격에 해당한다.



④ 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미하며, 소극적 공격에 해당한다.

④

9. 2014년 7급

공공 기관에서 「개인정보 보호법」에 의거하여 영상정보처리기기를 설치 및 운용하려고 할 때, 안내판에 기재해야 할 내용으로 옳지 않은 것은? (난이도:4)

- ① 설치 장소
- ② 영상정보 저장 방식
- ③ 촬영 시간
- ④ 관리 책임자의 이름



- 안내판에 기재하여야 할 사항
 1. 설치 목적 및 장소
 2. 촬영 범위 및 시간
 3. 관리책임자의 성명(직책) 및 연락처
 4. (영상정보처리기기 설치운영을 위탁한 경우) 위탁받는자의 명칭 및 연락처

오늘 피하기 ② 영상정보 저장 방식은 안내판 기재사항이 아니다.

정답 ②

10. 2014년 7급

생일 역설(Birthday Paradox)에 대한 설명으로 옳지 않은 것은? (난이도:3)

- ① 해시 함수(hash function)는 충돌 메시지 쌍을 찾아내는 데 사용된다.
- ② 특정 장소에서 23명 이상이 있으면, 그중에서 2명 이상의 사람이 생일이 같은 확률은 0.5보다 크다.
- ③ 블록 암호 알고리즘의 안전성을 분석하는 데 이용된다.
- ④ 0부터 N-1까지의 균일 분포를 갖는 수 중에서 임의로 한 개의 수를 선택한다면, (N)1/2번의 시도 후에 동일한 수가 반복해서 선택될 확률은 0.5를 넘는다는 이론과 부합한다.



- 생일 패러독스(birthday paradox)는 랜덤으로 선택한 N명 중 적어도 2명의 생일이 일치할 확률이 「2분의1」 이상이 되도록 하기 위해서는 N은 최저 23명이라는 것이다.

오늘 피하기 ③ 생일 공격(birthday attack)은 일방향 해시함수의 「강한 충돌 내성」을 깨고자 하는 공격이다.

정답 ③

11. 2014년 7급

자산의 위협과 취약성을 분석하여, 보안 위험의 내용과 정도를 결정하는 과정은? (난이도:2)

- ① 위험 분석
- ② 보안 관리
- ③ 위험 관리
- ④ 보안 분석

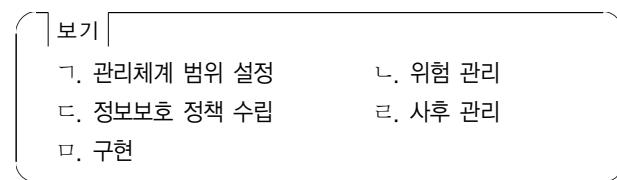


오늘 피하기 ① 위험분석의 목적은 보호되어야 할 대상 정보시스템과 조직의 위험을 측정하고 이 측정된 위험이 허용 가능한 수준인지 아닌지 판단할 수 있는 근거를 제공하는 것이다.

정답 ①

12. 2014년 7급

정보보호관리체계(ISMS) 인증과 관련하여 정보보호 관리과정 수행 절차를 순서대로 올바르게 나열한 것은? (난이도:3)



- ① ㄱ → ㄴ → ㄷ → ㄹ → ㅁ
- ② ㄱ → ㄷ → ㄴ → ㄹ → ㅁ
- ③ ㄷ → ㄴ → ㅁ → ㄱ → ㄹ
- ④ ㄷ → ㄱ → ㄴ → ㅁ → ㄹ



오늘 피하기 ④ ISMS 정보보호 관리과정 수행 절차는 정보보호정책수립 및 범위설정, 경영진 책임 및 조직구성, 위험관리, 정보보호대책 구현, 사후관리이다.

정답 ④

13. 2014년 7급

다음은 개인정보의 수집 이용에 대한 사항이다. 동의를 받아야 할 항목만을 모두 고른 것은? (난이도:3)

보기

- ㄱ. 개인정보의 수집·이용 목적
- ㄴ. 수집하는 개인정보의 항목
- ㄷ. 개인정보의 보유 및 이용 기간
- ㄹ. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

- ① ㄱ, ㄴ
- ② ㄴ, ㄷ, ㄹ
- ③ ㄱ, ㄷ, ㄹ
- ④ ㄱ, ㄴ, ㄷ, ㄹ



◦ 제15조(개인정보의 수집·이용) ② 개인정보처리자는 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

정답 ④

14. 2014년 7급

패스워드>Password)에 사용될 수 있는 문자열의 범위를 정하고, 그 범위 내에서 생성 가능한 패스워드를 활용하는 공격은? (난이도:2)

- ① 레인보 테이블(Rainbow Table)을 이용한 공격
- ② 사전 공격(Dictionary Attack)
- ③ 무작위 대입 공격(Brute-Force Attack)
- ④ 차분 공격(Differential Attack)



- 사전공격(Dictionary Attack)은 패스워드 사전 파일을 이용하여 접속 계정을 알아내는 해킹 방법이다. 일반적으로 패스워드에 사용하기 위해 선택되는 수백 혹은 수천 개의 단어를 포함하는 소프트웨어를 가지고 수행된다.
- 레인보 테이블(영어: rainbow table)은 해시 함수를 사용하여 변환 가능한 모든 해시 값을 저장시켜 놓은 표이다. 보통 해시 함수를 이용하여 저장된 비밀번호로 부터 원래의 비밀번호를 추출하는데 사용된다.

오늘 피하기 ③ 무차별 공격(Brute-force Attack)은 성공할 때까지 가능한 모든 조합의 경우의 수를 시도해 원하는 공격을 시도하는 해킹 방법이다. 이 경우 정확한 패스워드가 드러날 때까지 모든 가능한 문자의 나열을 시도하는 툴이 사용된다.

정답 ③

15. 2014년 7급

다음의 공격 유형과 그 대응 조치를 올바르게 연결한 것은? (난이도:4)

보기

〈공격유형〉

1. Sendmail Daemon에 대해 알려진 패턴의 원격 버퍼 오버플로(Buffer Overflow) 공격
 2. 계정 도용(Account Theft)
 3. 해커가 임의로 파일을 삭제
 4. XSS(Cross Site Scripting)
- 〈대응조치〉
- ㄱ. WAF(Web Application Firewall)
 - ㄴ. OTP(One Time Password)
 - ㄷ. IPS(Intrusion Prevention System)
 - ㄹ. 디스크 포렌식(Disk Forensics)에 의한 자료 복원

① 1 – ㄱ, 2 – ㄴ, 3 – ㄹ, 4 – ㄷ

② 1 – ㄷ, 2 – ㄴ, 3 – ㄹ, 4 – ㄱ

③ 1 – ㄴ, 2 – ㄱ, 3 – ㄹ, 4 – ㄷ

④ 1 – ㄷ, 2 – ㄱ, 3 – ㄴ, 4 – ㄹ



- sendmail은 인터넷 전자 메일의 표준규약인 SMTP(Simple Mail Transfer Protocol) 프로토콜을 통해서 메일 서비스 기능을 한다. 즉, sendmail은 메일 서버 간에 메일을 주고받는 역할을 한다.
- 웹 방화벽 (Web firewall)은 웹 해킹을 방어하기 위한 웹 서버에 특화된 방화벽. 일반 방화벽에서는 탐지하지 못하는 웹 관련 공격 경로를 감시하고 공격이 웹 서버에 도달하기 전에 차단해 주는 보안 솔루션이다.

호^로피^피아^아기 ② Sendmail Daemon에 대해 알려진 패턴의 원격 버퍼 오버플로(Buffer Overflow) 공격은 침입방지시스템으로 효율적으로 방어가 가능하고, 계정 도용(Account Theft)은 일회용 패스워드로 패스워드를 매번 변경함으로써 방어가 가능하고, 해커가 임의로 파일을 삭제는 디스크 포렌식으로 자료 복원이 가능하며, XSS는 웹 공격법으로 웹 방화벽이 효율적인 방어수단이다.

정답 ②

16. 2014년 7급

다음 설명에 해당하는 접근제어 정책은? (난이도:3)

보기

한 개체(entity)가 자신의 의지로 다른 개체의 자원에 접근할 수 있는 권한을 승인받을 수 있다.

- ① MAC(Mandatory Access Control)
- ② DAC(Discretionary Access Control)
- ③ ACL(Access Control List)
- ④ RBAC(Role Based Access Control)



호^로피^피아^아기 ② DAC은 중앙 집중화된 환경에서 제어되는 것이 아니며 MAC에서의 보다 정적인 역할에 비해 사용자에게 동적으로 정보에 접근할 수 있도록 해준다.(분산형 보안관리)

정답 ②

17. 2014년 7급

침입 탐지 시스템(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은? (난이도:3)

- ① 호스트 기반과 네트워크 기반으로 나눌 수 있다.
- ② 침입 탐지 기법은 크게 오용 탐지(misuse detection) 기법과 이상 탐지(anomaly detection) 기법으로 나눌 수 있다.
- ③ 데이터의 효과적인 필터링(filtering)과 축약(reduction)을 수행해야 한다.
- ④ 오용 탐지 기법에는 정량적인 분석과 통계적인 분석 등이 포함된다.



오늘 피하기 ④ Anomaly detection은 사용자의 행동양식을 분석한 후 정상적인 행동과 비교해 이상한 행동, 급격한 변화가 발견되면 불법침입으로 탐지하는 방법으로 정통적인 분석, 통계적 분석을 사용한다.

정답 ④

이도:3)

- ① TCP SYN 스캐닝
- ② UDP 스캐닝
- ③ NULL 스캐닝
- ④ X-MAS tree 스캐닝

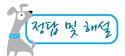
18. 2014년 7급

다음 설명에 해당하는 것은? (난이도:2)

보기

- 송신자 측에서는 전송할 이메일(email)에 대한 전자서명 생성에 사용되며, 수신자 측에서는 이메일에 포함된 전자서명의 확인 작업에 사용된다.
- 비대칭 암호 기술을 사용한다.
- 이메일 어플리케이션에 플러그인(plug-in) 방식으로 확장이 가능하다.
- 최초 개발자는 ‘필 짐머만(Phil Zimmermann)’이다.

- ① PGP(Pretty Good Privacy)
- ② PKI(Public-Key Infrastructure)
- ③ MIME(Multipurpose Internet Mail Extensions)
- ④ IKE(Internet Key Exchange)



오늘 피하기 ① PGP는 필립 짐머만(Philip Zimmermann)이 1991년에 독자적으로 개발하고 무료로 공개한 기밀성, 인증, 무결성, 송신부인 방지를 지원하는 이메일 보안 기술이다.

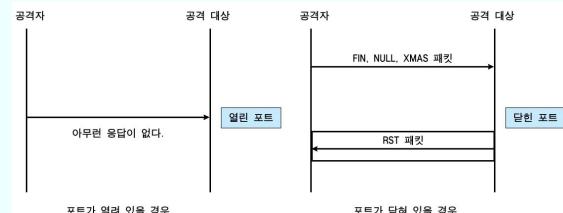
정답 ①

19. 2014년 7급

네트워크 스캐닝 기법 중 TCP 패킷에 FIN, PSH, URG 플래그를 설정해서 패킷을 전송하는 것은? (난



오늘 피하기 ④ NULL, XMAS 스캔 : NULL과 XMAS 패킷을 보내도 같은 결과를 얻을 수 있다. NULL은 플래그(flag) 값을 설정하지 않고 보낸 패킷이고, XMAS는 ACK, FIN, RST, SYN, URG 플래그 모두를 설정하여 보낸 패킷이다.



정답 ④

20. 2014년 7급

서비스 거부 공격(DoS: Denial of Service)에 대한 설명으로 옳지 않은 것은? (난이도:2)

- ① Smurf 공격은 공격 대상의 IP 주소를 근원지로 대량의 ICMP 응답 패킷을 전송하여, 서비스 거부를 유발시키는 공격이다.
- ② Syn Flooding 공격은 TCP 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약성을 이용한 공격이다.
- ③ Land 공격은 출발지와 목적지의 IP 주소를 상이하게 설정하여, IP 프로토콜 스택에 장애를 유발하는 공격이다.
- ④ Ping of Death 공격은 비정상적인 ICMP 패킷을 전송하여, 시스템의 성능을 저하시키는 공격이다.



③ Land Attack은 공격자가 임의로 자신의 IP 어드레스와 포트를 대상 서버의 IP 어드레스 및 포트와 동일하게 하여 서버에 접속하는 공격방식이다.

③