

정보보호론

1. 다음은 ARP 스푸핑에 대한 설명이다. (가)에 들어갈 용어는?

공격자가 스위치 내의 다른 단말기에 가짜 ARP 응답을 보내어 왜곡하는 공격으로, 공격자의 (가)를 속여서 패킷을 가로채는 공격이다. 이를 통해 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 로컬 네트워크의 통신 흐름을 왜곡한다.

- ① MAC 주소
- ② IP 주소
- ③ Port 주소
- ④ email 주소

2. 다음에서 설명하는 알고리즘은?

- 이산대수 문제를 기반으로 암호·복호화를 지원하고 전자서명에 활용될 수 있는 방식이다.
- 디피헬만(Diffie-Hellman)의 공용키 분배법의 확장형으로 암호문 길이가 평문 길이의 2배가 되는 단점이 있다.

- ① RSA
- ② ElGamal
- ③ LEA
- ④ KCDSA

3. 정보보호 컴플라이언스에 대한 설명으로 옳지 않은 것은?

- ① 정보보호 관련 법률과 규정을 준수하는 활동이다.
- ② 조직의 비즈니스 연속성과 투명성을 높이기 위한 활동의 일환이다.
- ③ 기술적 조치를 중심으로 구성되며, 인적·제도적 요소는 포함하지 않는다.
- ④ 외부 규제뿐만 아니라 내부 통제 기능을 대상으로 한다.

4. 「개인정보 보호법」상 고정형 영상정보처리기기의 설치·운영 제한에 대한 설명으로 옳지 않은 것은?

- ① 교통단속을 위하여 정당한 권한을 가진 경우 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있다.
- ② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실, 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 고정형 영상정보처리기기를 설치·운영 하여서는 아니 된다. 다만 대통령령으로 정하는 시설에 대하여는 그러지 아니하다.
- ③ 고정형영상정보처리기기운영자는 고정형 영상정보처리기기의 설치 목적과 다른 목적으로 고정형 영상정보처리기기를 임의로 조작 하거나 다른 곳을 비춰서는 아니 되나, 녹음기능은 사용할 수 있다.
- ④ 고정형영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 고정형 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 다만 「개인정보 보호법」에 따라 개인정보 처리방침을 정할 때 고정형 영상정보처리기기 운영·관리에 관한 사항을 포함시킨 경우에는 고정형 영상정보처리기기 운영·관리 방침을 마련하지 아니할 수 있다.

5. 해시(Hash) 함수에 대한 설명으로 옳은 것은?

- ① 해시 함수는 결과값(해시값)으로부터 원래 입력을 쉽게 복원할 수 있다.
- ② 같은 입력에 대해서는 같은 해시값이 생성된다.
- ③ 네트워크로 메시지와 메시지의 해시값을 전송하면 메시지의 무결성이 보호된다.
- ④ 해시 함수는 임의 길이의 입력을 받아 입력마다 서로 다른 길이의 결과값을 만든다.

6. 다음에서 설명하는 보안 시스템은?

조직의 IT 인프라 전체에서 발생하는 로그와 이벤트 데이터를 실시간으로 수집·분석하여 보안 위협을 탐지하는 통합 보안 솔루션이다.

- ① NAC
- ② DLP
- ③ VPN
- ④ SIEM

7. 악성코드(Malware)의 종류로만 옳게 짝지어진 것은?

- ① Worm, Trojan Horse
- ② IDS, APT
- ③ SET, IPsec
- ④ DDoS, IP 스푸핑

8. 리눅스 운영체제에서 허가권을 변경하는 명령어 사용 형식이 옳지 않은 것은?

- ① 그룹에 쓰기 권한 부여: `chmod g+w`
- ② 사용자의 실행 권한 제거: `chmod o-x`
- ③ 사용자, 그룹, 타인의 실행 권한 제거: `chmod a-x`
- ④ 타인에게 읽기, 쓰기 권한만 부여: `chmod o+rw`

9. 다음은 정보보호의 요구사항에 대한 설명이다. (가)에 들어갈 용어는?

(가)은 비인가된 자에 의한 정보의 변경, 삭제, 생성 등으로부터 보호되어 정보의 정확성, 완전성이 보장되어야 한다는 원칙이다.

- ① 기밀성
- ② 인증성
- ③ 무결성
- ④ 가용성

10. 책임 추적성(Accountability)을 보장하기 위한 주요 수단은?

- ① 암호화
- ② 백업 및 복구
- ③ 감사 로그
- ④ 침입 방지 시스템

11. SSL(Secure Socket Layer)에 대한 설명으로 옳지 않은 것은?

- ① TCP/IP 4계층 모델의 네트워크 계층에서 동작하는 프로토콜이다.
- ② 암호화된 웹 서핑을 가능하게 한다.
- ③ 서버 인증, 클라이언트 인증, 암호화 세션 기능을 제공한다.
- ④ SSL을 지원하는 웹 사이트 URL은 'https://'로 시작한다.

12. 웹 취약점과 대응 방안에 대한 설명으로 옳지 않은 것은?

- ① 업로드 취약점 공격: 파일 고유의 데이터인 시그니처를 분석하여 특정 파일에 대한 접근제어를 수행한다.
- ② 인젝션 공격: 파일 확장자를 검증한다.
- ③ XSS 공격: 웹 브라우저를 업데이트하여 악성 스크립트 실행을 차단하거나 사용자의 입력에 대한 유효성을 검사한다.
- ④ CSRF 공격: 위조 방지 토큰(요청 검증 토큰)을 추가한다.

13. 포트 스캔(Port Scan)에 대한 설명으로 옳지 않은 것은?

- ① 공격 대상 시스템의 운영체제 확인이 가능하다.
- ② 특정 패킷을 보내서 공격 대상 시스템의 어떤 서비스 포트가 열려 있고 닫혀 있는지 확인할 수 있다.
- ③ 스캐닝 공격 기법 종류에는 TCP Scan, UDP Scan, Fin Scan, XMAS Scan 등이 있다.
- ④ UDP Scanning은 3-Way Handshaking의 특징을 악용하는 방법이다.

14. OECD의 '개인정보보호 원칙'이 아닌 것은?

- ① 책임의 원칙(Accountability Principle)
- ② 이용 제한의 원칙(Use Limitation Principle)
- ③ 정보 정확성의 원칙(Data Quality Principle)
- ④ 비공개의 원칙(Closeness Principle)

15. 다음 설명의 (가), (나), (다)에 들어갈 용어를 바르게 연결한 것은?

- (가) 은/는 단말기가 회사의 내부 네트워크에 접속을 시도할 때 이를 제어하고 통제한다.
- (나) 은/는 외부 네트워크에서 내부 네트워크로 유입되는 침입을 막는다.
- (다) 은/는 시스템이나 네트워크에 대한 다양한 불법 침입행위를 실시간 탐지, 분석하여 비정상적인 패킷일 때 자동으로 차단한다.

(가)	(나)	(다)
① NAC	방화벽	IPS
② IPS	DRM	방화벽
③ NAC	IPS	IDS
④ DRM	IDS	NAC

16. 다음에서 설명하는 네트워크 공격은?

출발지와 목적지의 IP 주소를 동일하게 공격 대상의 IP 주소로 변조하여 전송한다. 출발지 IP 주소가 자신의 IP 주소이므로 스스로 응답하고, 이 과정을 반복하여 과부하를 유발한다.

- ① Teardrop 공격
- ② Smurf 공격
- ③ Ping of Death 공격
- ④ Land 공격

17. 암호에 대한 설명으로 옳지 않은 것은?

- ① 공개키 암호 알고리즘은 트랩도어 단방향 함수에 기반을 둔다.
- ② 대칭키 암호 알고리즘은 공개키 암호 시스템에 비해서 암호화 및 복호화 속도가 빠르다.
- ③ 공개키 암호 알고리즘의 대표적인 알고리즘은 DES이다.
- ④ 공개키 암호는 전자서명에 사용된다.

18. 「정보보호산업의 진흥에 관한 법률 시행령」에 따른 정보보호 공시에 대한 설명으로 옳지 않은 것은?

① 정보기술부문 투자 현황 대비 정보보호부문 투자 현황은 정보보호 공시 내용에 포함된다.

② 공공기관은 정보보호공시의무자에서 제외된다.

③ 공시 주체의 정보보호 최고책임자가 주관하여 공시하여야 한다.

④ 「전자금융거래법」에 따른 금융회사는 정보보호공시의무자에 포함된다.

19. 다음에서 설명하는 접근제어 과정은?

○ 자신의 신분 또는 위변조를 증명하는 과정

○ 지문, 홍채, 정맥을 이용한 확인 과정

① Identification

② Authorization

③ Authentication

④ One-Time Password

20. 암호 알고리즘에 대한 설명으로 옳은 것은?

① AES는 다에먼(Daemen)과 레이먼(Rijmen)이 제안한 Rijndael을 기반으로 제정된 미국 표준 알고리즘이다.

② SEED는 미국 NIST가 표준으로 선정한 대칭키 알고리즘이다.

③ ARIA는 스트림 암호 방식으로 동작하는 알고리즘이다.

④ IDEA는 리베스트(Rivest)가 개발한 알고리즘으로 블록, 키, 라운드 크기가 모두 가변적이다.

21. 국가정보원장이 중앙행정기관의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등을 평가하는 제도는?

① 개인정보 보호수준 평가

② 보안적합성 검증

③ 사이버보안 실태평가

④ 개인정보 침해요인 평가

22. CC 인증은 시스템에 대한 보안을 평가하기 위하여 EAL(Evaluation Assurance Level)의 1 ~ 7단계를 두어 평가한다. ‘정형화된 설계 검증 및 시험’ 단계에 해당하는 것은?

① EAL4

② EAL5

③ EAL6

④ EAL7

23. 기업망을 보호하기 위해 네트워크 경계를 신뢰 판단의 전제로 삼지 않고, 위치와 관계없이 모든 접근을 지속적으로 검증하고, 최소 권한만 부여하는 보안 방식은?

① 다중 인증(Multi-factor Authentication)

② 챌린지 핸드셰이크 인증 프로토콜(Challenge Handshake Authentication Protocol)

③ 제로 트러스트 보안 모델(Zero Trust Security Model)

④ 임의적 접근 통제 모델(Discretionary Access Control Model)

24. 검증필 암호모듈(KCMVP)의 검증대상 암호알고리즘이 아닌 것은?

① ARIA

② RC5

③ AES

④ LEA

25. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」에 따른 클라우드컴퓨팅서비스의 보안인증 절차 등에 대한 설명으로 옳지 않은 것은?

① 한국인터넷진흥원은 클라우드컴퓨팅서비스에 대한 보안인증 기관의 하나이다.

② 국가기관 등이 이용하는 클라우드컴퓨팅서비스의 보안인증 기준은 국가정보원장이 정한다.

③ 보안인증의 유효기간은 5년이다.

④ 보안인증의 유효기간은 연장할 수 있다.