

정보시스템보안

1. 다음 중 암호를 찾기 위하여 가능한 모든 조합을 시도하는 공격기법으로 가장 옳은 것은?
① 무차별(Brute-force) 공격
② 사전(Dictionary) 공격
③ 스미싱(Smishing) 공격
④ 암호 추측>Password Guessing) 공격
2. 다음 중 웜(Worm)에 대한 설명으로 가장 옳지 않은 것은?
① 시스템의 취약점을 이용해 자신을 실행시킨다.
② 자신을 복제하여 네트워크 연결을 통해 복제본을 전송한다.
③ 다른 프로그램의 한 유형인 것처럼 가장하여 활동한다.
④ 네트워크 기반 웜 방어가 가능하다.
3. 다음 중 윈도우를 설치할 때 기본적으로 생성되는 그룹 설명으로 가장 옳지 않은 것은?
① Users: 개개인에 할당된 사용자 환경을 직접 만들 수 있지만 시스템 서비스의 시작 및 종료 권한이 없다.
② Replicator: 도메인에 있는 파일을 복제할 수 있는 권한을 가지는 그룹이다.
③ Administrators: 도메인 지원이나 로컬 컴퓨터에 대한 모든 권한이 있다.
④ Power Users: 공용 프로그램 그룹 생성 및 컴퓨터의 시계 설정 권한은 있으나 디렉터리나 네트워크 공유 설정 권한은 없다.
4. 다음 중 윈도우 NTFS 디스크 구조에서 볼륨 및 파일시스템에 존재하는 모든 파일과 디렉터리에 대한 정보를 담고 있는 테이블로 가장 옳은 것은?
① MFT(Master File Table)
② VBR(Volume Boot Record)
③ MBR(Master Boot Record)
④ FSINFO(File System Information)

5. 다음 중 사용자 및 그룹 계정에 대한 데이터베이스를 관리하며, 사용자의 로그인 입력 정보와 데이터베이스 정보를 비교하여 인증 여부를 결정하는 윈도우 인증 구성요소로 가장 옳은 것은?
① LSA(Local Security Authority)
② SAM(Security Account Manager)
③ SRM(Security Reference Monitor)
④ NTLM(NT LAN Manager)
6. 다음 중 윈도우 운영체제의 레지스트리에 대한 설명으로 가장 옳지 않은 것은?
① 레지스트리 편집기로 레지스트리 설정을 열람, 수정, 추가, 삭제할 수 있다.
② HKEY_CLASSES_ROOT(HKCR)에는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 애플리케이션에 대한 맵핑 정보를 저장하고 있다.
③ HKEY_CURRENT_CONFIG(HKCC)에는 소프트웨어 목록과 애플리케이션 이름, 경로, 라이선스 정보 등 환경 설정 정보가 저장되어 있다.
④ HKEY_USERS(HKU)에는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.
7. 다음 중 유닉스 디렉터리 설명으로 가장 옳은 것은?
① /dev: 프로그램 실행 및 설치 시 생성되는 임시 파일을 담고 있다.
② /home: 시스템 최상위 디렉터리이다.
③ /lib: 시스템 로그가 저장되는 디렉터리이다.
④ /etc: 시스템의 환경 설정 및 주요 설정 파일을 담고 있다.
8. 다음 중 생체인증의 오인식률과 오거부율에 대한 설명으로 가장 옳은 것은?
① 오인식률이 높으면 허가되어야 할 사람의 차단이 높아진다.
② 오거부율이 높으면 차단되어야 할 사람의 진입이 높아진다.
③ 오인식률과 오거부율간의 상관관계는 나타나지 않는다.
④ 보안 등급을 높여야 할 경우, 상대적으로 오거부율이 높아질 수 있다.

9. 다음 중 시스템 관리와 관련된 보안 기능에서 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대해 관리하는 것으로 가장 옳은 것은?

- ① 로그 관리 ② 세션 관리
③ 권한 관리 ④ 취약점 관리

10. 다음 중 버퍼오버플로우(Buffer Overflow) 공격에 가장 안전한 C언어 함수로 옳은 것은?

- ① sscanf() ② strcat()
③ snprintf() ④ vsprintf()

11. 다음 중 정보보호에서 무결성에 대한 설명으로 가장 옳은 것은?

- ① 정보의 내용이 임의적으로 생성, 변경, 삭제되지 않도록 보호된다.
- ② 정보에 대한 필요성이 요구될 때, 신속하게 액세스할 수 있다.
- ③ 정보에 대한 변형이 용이하여 추가 정보의 가공이 간편하다.
- ④ 인가된 사람만이 정보를 액세스할 수 있다.

12. 다음 중 디지털 콘텐츠의 보호에 관련된 설명으로 가장 옳지 않은 것은?

- ① 스테가노그래피(Steganography)는 공개된 콘텐츠에 기밀 메시지를 은폐, 전달하기 위한 방법이다.
- ② 디지털 워터마킹은 디지털 콘텐츠에 저작권 데이터를 부가, 콘텐츠 권리에 대한 행사를 위한 방법이다.
- ③ 핑거프린팅은 콘텐츠의 배포 경로에 따른 구매자를 추적하기 위한 목적으로, 콘텐츠에 따라 구분되는 정보가 부가된 방법이다.
- ④ DRM은 콘텐츠에 대한 구매자의 익명성을 보장, 구매자에 대한 역추적을 막으려는 방법이다.

13. 다음 중 유닉스 시스템의 로그 파일에서 FTP 파일을 전송한 날짜와 시간, 접근 시스템의 IP를 확인할 수 있는 것으로 가장 옳은 것은?

- ① xferlog ② utmp
③ wtmp ④ pacct

14. 다음 중 암호화 알고리즘에서 키의 공개 또는 비공개 형태가 동일하게 짝지어진 것으로 가장 옳은 것은?

- ① AES, RSA ② RSA, ECC
③ DES, RSA ④ AES, ECC

15. 다음 중 암호 분석가가 취득한 정보를 이용한 암호 분석으로 가장 옳지 않은 것은? (단, 사용된 키는 변하지 않는다고 가정한다.)

- ① 암호 알고리즘, 해독할 암호문을 취득하였다면, 암호문 단독(Ciphertext Only) 방법으로 공격한다.
- ② 암호 알고리즘, 해독할 암호문, 임의의 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문을 알고 있다면, 기지 평문(Known Plaintext) 방법으로 공격한다.
- ③ 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문을 얻을 수 있다면, 선택 평문(Chosen Plaintext) 방법으로 공격한다.
- ④ 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 수정된 평문, 암호문에 사용된 키로 생성한 각각의 암호문을 알고 있다면, 선택 암호문(Chosen Ciphertext) 방법으로 공격한다.

16. 다음 중 생체인증 기술의 평가 요건으로 가장 옳지 않은 것은?

- ① 보편성은 일반적인 사람이 가지고 있는 보편적인 특성을 의미한다.
- ② 지속성은 시간의 흐름에 따라 변하지 않는 특성을 지속함을 의미한다.
- ③ 획득성은 악의적인 방법으로 복제하기 어려운 성질인가를 의미한다.
- ④ 수용성은 사용자의 거부감이 없는 성질인가를 의미한다.

17. 다음 중 해시함수의 성질에 관련된 것으로 가장 옳지 않은 것은?

- ① 데이터에 대해 해시함수를 적용한 결과는 원 데이터에 나타나는 단어 빈도에 따라 불균일한 분포로 나타난다.
- ② 역상 저항성이란 해시함수를 적용한 결과로 원 데이터를 계산상 찾아내기 어려운 것이다.
- ③ 약한 충돌 저항성은 해시함수를 적용한 결과로 동일한 해시 결과값을 갖는 데이터를 계산상 찾아내기 어려운 것이다.
- ④ 강한 충돌 저항성은 해시함수를 적용한 결과가 같은 값이 되는 원 데이터쌍을 찾는 것이 계산상 찾아내기 어려운 것이다.

18. 다음 중 공개키 기반 구조(PKI)에 관한 내용으로 가장 옳지 않은 것은?
- ① 정책승인기관(PAA)은 PKI의 전반적인 정책과 절차를 생성하고 루트 CA역할을 수행한다.

② 정책인증기관(PCA)은 인증기관과 먼 사용자를 위하여 인증기관 대신 인증서 신청의 신분과 소속을 확인한다.

③ 저장소는 인증서와 사용자 관련정보, 인증서, 인증서 취소 목록을 저장, 검색하는 장소이다.

④ 인증기관(CA)은 공개키 인증서를 발급, 취소하며, 인증서/인증서 취소 목록을 관리한다.
19. 다음 중 난수에 관련된 것으로 가장 옳게 설명한 것은?
- ① 무작위성, 예측 불가능성, 재현 불가능성, 복제 유지성이 난수의 성질이다.

② 생성된 난수는 가능한 범위 전체 중 중앙값에 높은 빈도로 나타난다.

③ 의사난수에서 종자(Seed)값이 유출될 경우 예측 가능해진다.

④ 어떤 순간에 생성한 난수값에 의하여 다음 생성될 난수 값이 결정된다.
20. 다음 중 Diffie-Hellman 키 교환 알고리즘에 관련된 내용으로 가장 옳지 않은 것은?
- ① 공개키 암호화 방식에 대한 알고리즘이다.

② 중간자 공격 방법에 대해 강하다.

③ 유한체상의 이산대수 문제 해결의 어려움에 기반한다.

④ 공개키는 평문을 암호화하기 위해 사용되는 키로써 배포 가능하다.