Web 보안 평가문제 이름 :

1. 유닉스 계열의 시스템에서 일반 계정의 비밀번호를 저장할 때 암호화하여 저장한다. 일반적으로 어떤 알고리즘을 이용하여 저장하는가?
① DES
② SHA
③ MD5
④ RSA

2. 다음에서 설명하는 공격용 소프트웨어는 무엇인가?

· 안티바이러스 프로그램에 의해 탐지된다.
· 특정 문자열을 타이핑한 후 파일의 내용에서 타이핑한 문자열이 검색된다.
· 지정된 시간에 로그파일을 설정된 공격자 메일로 자동 전송기능을 포함한다.
소프트웨어로 winhawk가 있다.

① Root Kit
② Key Logger software
③ Port Scanning
④ Nessassin

3. 다음 중에서 시스템의 취약성 점검을 위하여 사용할 수 있는 도구가 아닌 것은?
① ping
② SATAN
③ SAINT
④ NESSUS

4. 라우터(Router)를 이용한 네트워크 보안 설정 방법 중에서 내부 네트워크로 유입되는 패킷의 소스 IP나 목적지 포트 등을 체크하여 적용하거나 거부하도록 필터링 과정을 수행하는 것은?
① Ingress Filtering
② Egress Filtering
③ Unicast RFP
④ Packet Sniffing

5. 한 개의 ICMP(Internet Control Message Protocol) 패킷으로 많은 부하를 일으켜 정상적인 서비스를 방해하는 공격 기법은?
① Ping of Death
② Land Attack
③ IP Spoofing
④ Hash DDoS

6. 다음 중에서 원격지 운영체제(OS)를 탐지해 내는 방법으로 옳지 않은 것은?
① telnet, IP port, ftp 등을 이용한다.
② nmap -oX 옵션을 이용한다.
③ TCP의 시퀀스를 확인한다.
④ HTTP GET과 서버의 포워드를 grep한다.

7. 메일 서버 서비스에 대해서 할 수 있는 서버 공격 기법은?
① Active Contents
② UDP Bomb
③ Syn Flooding
④ Mail Bomb

8. 다음은 웹 보안공격 방지에 대한 설명을 나열한 것이다. 어떤 웹 보안 공격을 방지하기 위한 설명인가?

· 세션 관리 모든 정보를 서버 측에서 저장 관리
· SMS 인증과 같은 2차 인증
· 쿠키 정보는 불완전하므로 암호화하여 변조를 방지
소프트웨어로 winhawk가 있다.

① SQL Injection
② XSS
③ 쿠키/세션 위조 공격 방지 방법
④ 좀비 쿠키 위조 공격방지 방법

9. 다음에서 설명하고 있는 웹 서비스 공격 유형은 무엇인가?

· 이 공격은 게시판의 글에 원본과 함께 악성코드를 삽입하여 웹 어플리케이션에 순수하게 제공되는 동작 외에 부정적으로 일어나는 액션
· 다른 기법과 차이점은 공격 대상이 서버가 아닌 클라이언트

① SQL Injection
② XSS(Cross Site Scripting)
③ 업로드 취약점
④ CSRF(Cross Site Request Forgery)

10. 웹과 데이터베이스를 연동한 애플리케이션에서 SQL Injection 공격을 방어하기 위한 방지법이 아닌 것은?
① 로그인 창에 특수기호를 넣지 못하도록 한다.
② 인증 시에 2채널 인증을 한다.
③ 원시 ODBC 에러를 사용자가 볼 수 있도록 코딩한다.
④ 스니핑을 통해서 모니터링을 하고 취약점을 개선한다.

11. 컴퓨터시스템에 대한 공격 방법 중에서 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀 주소(return address)를 조작, 궁극적으로 공격자가 원하는 코드를 실행하도록 하는 공격은?
① 버퍼 오버플로우 공격
② Race Condition
③ Active Contents
④ Memory 경합

12. 데이터베이스 내의 자료 값들을 잘못된 갱신이나 불법조작으로부터 보호함으로써, 정확성을 유지하고자 하는 것은 아래의 DB보안 요구사항 중 어느 것인가?
① 데이터 일관성
② 데이터 무결성
③ 데이터 보안
④ 데이터 접근제어

13. 오라클 데이터베이스의 보안설정 및 운영으로 옳지 않은 것은?
① 데이터베이스 설치 이후 디폴트로 설정된 패스워드는 모두 변경되어야 한다.
② svrmgr 제공하는 버전의 경우에는 Connect Internal 에 암호가 설정되도록 change_password 명령을 사용한다.
③ MySQL의 경우 호스트 명령을 실행하는 프로시저는 삭제한다.
④ UTL_File에 대한 실행 권한을 제한한다.

14. 다음 중에서 블록 알고리즘 종류와 특징을 옳게 설명한 것은?
① IDEA는 유럽에서 1990년 개발되었으며 PGP를 채택하고 8라운드의 알고리즘이다.
② AES는 미국 연방표준 알고리즘으로 DES를 대신할 64비트 암호 알고리즘이다.
③ SEED는 128비트 암호 알고리즘으로 NIST에서 개발한 대칭키 암호 알고리즘 표준이다.
④ DES의 취약점을 보완하기 위하여 1997년 3-DES가 개발되었고 이것은 AES를 대신할 기술이다.

15. 커버로스(Kerberos) 인증에 대한 설명으로 옳지 않은 것은?
① 커버로스 인증은 MIT에서 개발한 중앙 집중적 인증 시스템이다.
② 커버로스 인증은 티켓 서버와 인증 서버가 존재하고 티켓을 발급받아 이중시스템으로 인증한다.
③ 커버로스는 대칭키 기반 인증시스템을 사용한다.
④ 커버로스의 인증과정 중에서 인증 서버는 사용자의 비대칭키로 메시지를 암호화해서 전송한다.

16. 다음 중 TLS의 보안 서비스에 해당되지 않는 것은?
① SSL을 대신하기 위한 차세대 안정 통신 규약이다.
② 암호화에는 3개의 다른 데이터 암호화 표준(DES)키를 사용한 3DES 기술을 사용한다.
③ 관용키 기반 암호화시스템이다.
④ 네트워크나 순차 패킷교환, 애플토크(Appletalk) 등의 통신망 통신 규약에도 대응된다.

17. 다음 중에서 전자 서명의 조건이 아닌 것은?
① 서명자 이외의 타인이 서명을 위조하기 어려워야 함
② 서명한 문서의 내용은 변경 불가능
③ 누구든지 검증할 수는 없다.
④ 다른 전자문서의 서명으로 재사용 불가능

18. 개인정보를 취급할 때에는 개인정보의 분실, 도난, 누출, 변조 또는 훼손을 방지하기 위해서 기술적, 관리적 보호조치를 취해야 하는 사항이 아닌 것은 무엇인가?
① 정보의 주체가 언제든지 쉽게 확인할 수 있는 조치
② 개인정보처리에 대한 감독
③ 업무범위를 초과하여 개인정보를 이용하면 안됨
④ 개인정보 동의를 안전하게 받을 수 있는 보호조치

19. Lamport의 일회용 패스워드의 안정성은 무엇에 근거하는가?
① 공개키 암호화
② 키 분배
③ 해쉬 함수의 일방향성
④ 대칭키 암호화

20. 무선플랫폼에서 보안 기술을 제공하기 위해 제시된 기술 중에서 WAP 기반 클라이언트/서버간의 인증을 제공하며 적합한 인증서를 발급, 운영 관리하는 등 무선망에서의 공개키 기반 구조를 의미하는 것은?
① PKI
② VPN
③ WPKI
④ SSL