정보시스템 보안

1. 유닉스 파일 시스템의 i-node 정보에 해당하지 않는 것은?

① 소유그룹 ② 파일 타입
③ 파일명 ④ 접근권한

2. PGP의 인증에 대한 설명으로 옳지 않은 것은?

① 송신자는 일방향 해시함수를 사용하여 송신 메시지의 해시 코드를 생성한다.
② 송신자가 생성한 해시 코드는 송신자의 개인키를 사용하여 암호화되며, 그 결괏값이 메시지에 포함된다.
③ 수신자는 수신한 메시지를 송신자의 공개키로 복호화하고 해시 코드를 알아낸다.
④ 디지털 서명을 생성하는 데 DSS를 사용하는 것은 허용하지 않는다.

3. 사용자 및 그룹 계정 정보에 대한 데이터베이스를 관리하는 윈도 인증 구성 요소는?

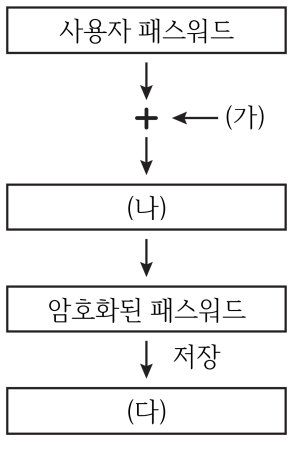
① LSA ② SAM
③ SRM ④ SID

4. 다음에서 설명하는 웹 취약점은?

> 웹 애플리케이션을 구동하는 웹 서버의 보안 설정이 취약하여 발생하는 보안 설정 오류 취약점이다. 정상적인 URL 경로 중 확인 대상 디렉터리까지만 직접 접근하여 이 취약점을 점검할 수 있다.

① SQL Injection ② 디렉터리 인덱싱
③ 운영체제 명령어 실행 ④ XSS(Cross Site Scripting)

5. 다음 리눅스 시스템 사용자 패스워드 저장 과정의 (가) ~ (다)에 들어갈 내용을 바르게 연결한 것은?



	(가)	(나)	(다)
①	Salt	RSA	/etc/passwd
②	Salt	SHA256	/etc/shadow
③	암호키	MD5	/etc/passwd
④	암호키	ARIA	/etc/shadow

6. x86 32bit 계열 CPU의 레지스터에 대한 설명으로 옳지 않은 것은?

① EDI는 목적지 주소 값을 저장한다.
② ECX는 반복적으로 실행되는 특정 명령에 사용된다.
③ CS는 프로그램에서 정의된 데이터, 상수, 작업 영역의 메모리 주소를 저장한다.
④ EFLAGS는 연산 결과 및 시스템의 상태와 관련된 여러 가지 플래그 값을 저장한다.

7. 다음에서 설명하는 공격에 대한 대응 방법으로 옳지 않은 것은?

> ○ 웹 서버를 기반으로 서버에 파일이 업로드되고 서버 측에서 실행되는 이러한 파일을 웹 셸(web shell)이라고 한다.
> ○ 공격자는 웹 서버에 업로드된 웹 셸 파일을 원격지에서 실행하여 웹 서버를 공격할 수 있다.

① 업로드 파일에 대한 실행 금지
② 업로드 파일에 대한 위치 격리
③ 업로드 가능한 파일 형식 제한
④ 업로드 파일명에 대한 필터링 설정

8. 참조 모니터(Reference Monitor)에 대한 설명으로 옳지 않은 것은?

① 모든 주체 간 상호 접근통제를 담당하는 추상적인 기계이다.
② 참조 모니터 데이터베이스를 참조하여 접근통제를 수행한다.
③ 모든 접근 시도에 대해 시행되어야 하고 회피하는 것이 불가능해야 한다.
④ 보안 매개변수 설정 등과 같은 다른 보안 메커니즘과 데이터를 교환하면서 상호 작용을 한다.

9. (가)에 들어갈 리눅스 메일 시스템의 구성 요소는?

> ○ 메일 클라이언트에서 [(가)]로 메일을 보낼 때와 [(가)]에서 [(가)]로 메일이 중계될 때 SMTP 프로토콜을 사용한다.
> ○ 불특정 다수의 메일 전송 및 중계를 허용하면 공격자는 스팸 메일을 보내는 도구로 [(가)]를 악용할 수 있다.

① MTA(Message Transfer Agent)
② MDA(Mail Delivery Agent)
③ MUA(Mail User Agent)
④ MRA(Mail Relay Agent)

10. 보안 취약점으로 인해 실제 발생한 취약점의 등급을 매기는 공개 프레임워크는?

① CVE
② CVSS
③ CWE
④ NVD

11. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

> ○ (가)는 컴파일러가 프로그램의 함수를 호출할 때 ret 앞에 canary 값을 주입하고, 종료할 때 canary 값을 변조했는지 확인하여 공격을 탐지한다.
> ○ (나) 공격은 데이터의 형태와 길이에 대한 불명확한 정의로 인한 문제점 중 데이터 형태에 대한 불명확한 정의로 인한 것이다.

	(가)	(나)
①	스택 실드	버퍼 오버플로
②	스택 실드	포맷 스트링
③	스택 가드	버퍼 오버플로
④	스택 가드	포맷 스트링

12. 다음에서 설명하는 인증 방법은?

> 사용자가 많이 가입한 웹 사이트(네이버, 구글, 페이스북 등)의 사용자 가입 정보를 이용해서 다른 웹 사이트에 별도의 가입 과정 없이 단순하게 사용자 신원을 검증하는 토큰을 제공하여 제삼자 인증 서비스를 이용할 수 있게 해 준다.

① Kerberos
② OAuth
③ SSO
④ DIAMETER

13. 클라우드 서비스 및 보안에 대한 설명으로 옳지 않은 것은?

① 클라우드 환경에서의 서비스 모델은 IaaS, PaaS, SaaS로 구분할 수 있다.
② 한국인터넷진흥원(KISA)에서는 클라우드 서비스의 보안성 강화를 위해 '클라우드 서비스 보안인증'을 시행하고 있다.
③ 대부분의 취약점은 전통적인 IT 환경의 보안 취약점과 유사하여 기존의 보안시스템을 최대한 활용하여 방어하는 것만으로도 충분하다.
④ CSA(Cloud Security Alliance)에서는 심각한 클라우드 보안 위협에 대해 공유하고 있다.

14. 신뢰 플랫폼 모듈(Trusted Platform Module)의 구성 요소로 옳지 않은 것은?

① 난수 발생기
② 암복호화 엔진
③ RSA 키 발생기
④ MD5 해시값 생성기

15. syslogd 데몬에서 사용하는 다음 메시지 중 우선순위가 가장 높은 것은?

① alert ② crit
③ err ④ debug

16. 웹 취약점에 대한 설명으로 옳지 않은 것은?

① 입력 값에 대한 특수문자 검증을 통해 XSS 공격에 대응할 수 있다.
② 리버스 텔넷은 방화벽의 아웃바운드 정책에서 별다른 필터링을 수행하지 않는 허점을 이용한다.
③ 취약점이 있는 컴포넌트, 라이브러리, 프레임워크 및 다른 소프트웨어 모듈이 악용되는 경우 데이터에 손실을 발생시킬 수 있다.
④ CSRF는 사용자의 브라우저로 전달되는 데이터에 악성코드가 포함되어 브라우저에서 실행되면서 공격하는 기법이다.

17. 리눅스 bash shell의 환경 변수에 대한 설명으로 옳은 것은?

① TERM은 접속 호스트 이름을 나타낸다.
② SHELL은 서브 셸을 사용할 때 서브 셸을 의미한다.
③ PATH는 명령을 탐색할 경로를 의미한다.
④ PWD는 현재 사용 중인 패스워드의 위치를 나타낸다.

18. 다음에서 설명하는 공격을 수행할 수 있는 도구로 옳지 않은 것은?

> 관리자 인증 등 정상적인 절차를 거치지 않고 시스템에 접근하기 위해 제작된 프로그램으로, 원격지에서 공격자가 몰래 정보를 수집하거나 시스템의 특정 명령을 수행하고 재구성할 수 있도록 통제한다.

① Netbus ② Schoolbus
③ Nessus ④ Back Orifice

19. 윈도 운영체제의 감사 정책에 대한 설명으로 옳지 않은 것은?

① 권한 사용은 관리자 권한이 필요한 작업을 수행할 때 감사한다.
② 계정 로그온 이벤트는 로컬 계정에 접근할 때 생성되는 이벤트를 감사한다.
③ 개체 액세스는 파일, 디렉터리, 레지스트리 키, 프린터와 같은 개체에 접근 시도나 속성 변경 등을 감사한다.
④ 계정 관리는 신규 사용자 및 그룹 추가, 기존 사용자 그룹 변경, 사용자 활성화 및 비활성화, 계정 패스워드 변경 등을 감사한다.

20. 안티 리버싱 기법으로 프로그램의 실행 코드나 데이터를 압축 및 암호화하여 저장하는 기술은?

① 패킹
② 디컴파일
③ 시큐어 코딩
④ 안티 디버깅