정보시스템 보안

문 1. 해시함수 알고리즘에 해당하지 않는 것은?
① SHA1
② MD5
③ RMD160
④ IDEA

문 2. 사용자가 별도의 인프라를 구축하지 않고 인터넷을 통해 가상서버, 가상 PC 등의 컴퓨팅 자원을 이용하는 클라우드 서비스 유형은?
① PIMS
② IaaS
③ SaaS
④ ISMS

문 3. 리눅스 환경에서 사용되는 명령어에 대한 설명으로 옳지 않은 것은?
① touch – 파일 내의 특정 문자열을 검색할 때 사용한다.
② chown – 파일이나 디렉터리의 소유자를 변경할 때 사용한다.
③ mv – 파일을 다른 디렉터리로 이동하거나 파일명을 바꿀 때 사용한다.
④ df – 파일 시스템의 사용 중이거나 사용 가능한 디스크 공간에 대한 정보를 보여 준다.

문 4. 디지털 포렌식의 원칙 중에 “수집된 증거가 위·변조되지 않았음을 증명해야 한다”는 원칙은?
① 정당성의 원칙
② 신속성의 원칙
③ 무결성의 원칙
④ 연계 보관성의 원칙

문 5. 리버스 엔지니어링에 대한 설명으로 옳지 않은 것은?
① 안티 디버거는 안티 리버싱의 방법이다.
② 안티 리버싱은 리버스 엔지니어링을 쉽게 만드는 기술이다.
③ 리버스 엔지니어링에서 이용하는 도구는 OllyDbg와 IDA가 있다.
④ 완성된 소프트웨어를 역으로 분석하는 방법이다.

문 6. 스마트폰 이용자들에게 돌잔치, 결혼 청첩장, 교통법규 위반 통보 문자를 보내, 이를 클릭하는 순간 악성코드가 설치되고, 이를 통해 피해자의 개인정보를 탈취하는 기법은?
① 스미싱
② 루트킷
③ 스턱스넷
④ 키로깅

문 7. 백도어에 대한 설명으로 옳지 않은 것은?
① 백도어 공격 도구로는 NetBus, Back Orifice 등이 있다.
② 원격 백도어는 시스템 계정이 필요하고, 서버의 쉘을 얻어 내 관리자로 권한 상승할 때 사용하는 백도어이다.
③ 로컬 백도어는 시스템 내에서 동작하기 때문에 공격자는 해당 시스템에 접속할 수 있는 계정을 획득할 수 있어야 한다.
④ Schoolbus 공격도구는 기존의 트로이 목마처럼 서버 파일과 클라이언트 파일로 이루어져 있다.

문 8. 다음 설명에 해당하는 시스템 메모리 기본구조의 영역은?

> 프로그램이 실행될 때까지 알 수 없는 가변적인 양의 데이터를 저장하기 위해 프로그램의 프로세스가 사용할 수 있도록 예약되어 있는 메인 메모리의 영역으로, 프로그램들에 의해 할당되었다가 회수되는 작용이 되풀이된다. 프로그램들이 요구하는 블록의 크기나 요구/횟수 순서에 일정한 규칙이 없다.

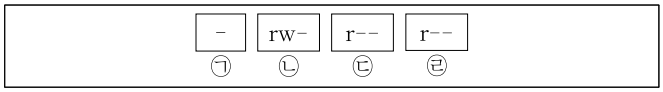
① 힙(Heap) 영역
② 스택(Stack) 영역
③ 텍스트(Text) 영역
④ 데이터(Data) 영역

문 9. 버퍼 오버플로우 공격에 대한 설명으로 옳지 않은 것은?
① 버퍼 오버플로우 공격의 종류 중에는 스택 기반 오버플로우와 힙 기반 오버플로우 공격이 있다.
② 버퍼 오버플로우 공격은 프로그램의 메모리 버퍼를 넘치게 해서 프로그램의 이상 동작을 유발하는 기법이다.
③ 버퍼 오버플로우 공격에 대응하기 위해서는 프로그램을 작성할 때 strcat(), strcpy(), getwd(), gets(), scanf() 등 입출력에 대한 사용자의 접근 가능성이 높은 함수를 사용한다.
④ 버퍼 오버플로우 공격의 대응 방법 중에는 Non-Executable Stack, Stack Guard, Stack Shield가 있다.

문 10. 파일 시스템에 대한 설명으로 옳지 않은 것은?
① 파일 시스템은 파일을 체계적으로 기록하는 방식으로 파일이 어디에 저장되어 있는지 조직화하고 구조적으로 정의한다.
② EXT(Extended File System) 파일 시스템은 리눅스 고유의 파일 시스템으로 계속 업그레이드가 되어지고 있다.
③ 슈퍼 블록은 파일 시스템을 관리하는 데 필요한 블록의 총수, 사용 중인 블록 및 이용 가능한 블록 정보를 포함하여 좀 더 빠르고 효과적인 파일 시스템 관리를 가능하게 한다.
④ FAT(File Allocation Table) 파일 시스템은 연결리스트를 사용하기 때문에 검색 시간이 짧으며 단편화 현상이 없도록 NTFS(New Technology File System)의 많은 제약 사항을 개선한 파일 시스템이다.

문 11. 인증, 무결성, 부인봉쇄, 기밀성 등의 기능을 지원하는 이메일 보안 기술은?
① TFTP
② S/MIME
③ WEP
④ WPA

문 12. 유닉스/리눅스 시스템에서 다음의 권한 설정에 대한 설명으로 옳지 않은 것은?



① ㉠은 파일 및 디렉터리의 종류로서 ‘-’는 디렉터리를 나타낸다.
② ㉡은 파일 및 디렉터리 소유자의 권한이다.
③ ㉢은 파일 및 디렉터리 그룹의 권한이다.
④ ㉣은 해당 파일 및 디렉터리의 소유자도 그룹도 아닌 제3자의 사용자에 대한 권한이다.

문 13. Cookie에 대한 설명으로 옳지 않은 것은?

① 쿠키는 클라이언트의 컴퓨터에 생성된다.
② 사용자와 웹사이트를 연결해 주는 정보가 저장되어 있다.
③ 직접 바이러스를 옮기거나 악성코드를 설치할 수 없다.
④ 사용자들의 로그인, 로그아웃, 시스템 재부팅 정보를 저장한다.

문 14. 다음에서 설명하고 있는 알고리즘은?

○ 순수 국내 기술로 개발된 128비트 크기의 블록 암호 알고리즘 ○ Feistel 구조로 128비트 알고리즘이 있음 ○ 1999년 국내 표준으로 제정, 2005년에는 국제 표준 제정 ○ IETF RFC 4269

① RSA
② Triple DES
③ AES
④ SEED

문 15. CSRF(Cross Site Request Forgery)의 특징에 대한 설명으로 옳지 않은 것은?

① 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 방법이다.
② 사이트에 방문하는 사용자가 정상적인 요청이 아닌 임의의 요청을 하도록 위조하는 방법이다.
③ 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 사용하여 연결된 세션에 혼란을 줌으로써 공격자가 서버와의 연결을 획득하는 방법이다.
④ 특정 웹사이트가 사용자의 웹브라우저를 신용하는 상태를 악용하는 방법이다.

문 16. 다음에서 설명하고 있는 공격에 해당하는 것은?

○ 파일의 소유자가 root이어야 함 ○ SetUID 비트를 가져야 함 ○ 바로 생성되는 임시 파일의 이름을 알고 있어야 함

① 버퍼 오버플로우
② 포맷 스트링
③ 패스워드 크래킹
④ 레이스 컨디션

문 17. SQL 인젝션에 대한 설명으로 옳지 않은 것은?

① 공격자가 입력값을 조작하여 원하는 SQL 구문을 실행한다.
② 전송되는 패킷을 가로채어 자신이 송신자인 것처럼 패킷을 변경하여 다시 보내는 기법이다.
③ 대응 방법 중에는 사용자의 입력에 특수문자가 포함되어 있는지 검증하는 방법이 있다.
④ OWASP에서 선정한 10대 웹 어플리케이션 보안 위험으로 SQL 인젝션의 취약점이 2004년, 2007년, 2010년, 2013년, 2017년에 포함되어 있다.

문 18. 와이파이(WiFi) 무선 네트워크에서 공격자가 가짜 AP(Access Point)를 구축하고 강한 신호를 보내어 사용자가 가짜 AP에 접속하게 함으로써 사용자 정보를 중간에서 가로채는 기법은?

① Zero Day
② DDoS
③ Evil Twin
④ DRDoS

문 19. HTTP에 대한 설명으로 옳지 않은 것은?

① 상태 코드 404는 클라이언트의 PUT요청이 성공적이라는 것을 의미한다.
② HTTP 1.0 프로토콜은 RFC 1945이고, HTTP 1.1 프로토콜은 RFC 2616에 기술되어 있다.
③ HTTPS는 SSL을 이용하여 클라이언트와 서버 사이에 주고받는 정보를 보호하는 데 사용된다.
④ Request는 웹서버에 데이터를 요청하거나 전송할 때 보내는 패킷으로 GET, POST와 같은 메소드를 사용한다.

문 20. XSS는 'Cross Site Scripting'의 약자로 줄여서 CSS라고도 부르지만, 웹 레이아웃과 스타일을 정의할 때 사용되는 캐스케이딩 스타일 시트(Cascading Style Sheets)와 혼동되어 일반적으로 XSS라고 부른다. 일반적인 XSS 공격 수행 과정을 순서대로 바르게 나열한 것은?

가. 해당 웹 서비스 사용자가 공격자가 작성해 놓은 XSS 코드에 접근한다. 물론 사용자는 자신이 공격자가 작성해 놓은 XSS 코드에 접근한다는 것을 인지하지 못한다. 사용자는 어떤 게시판의 글을 읽는 과정에서 공격자의 XSS 코드에 접근하게 된다. 나. 사용자의 시스템에서 XSS 코드가 실행된다. 다. 웹 서버는 사용자가 접근한 XSS 코드가 포함된 게시판의 글을 사용자에게 전달한다. 라. 임의의 XSS 취약점이 존재하는 서버에 XSS 코드를 작성하여 저장한다. 일반적으로 공격자는 임의의 사용자나 특정인이 이용하는 게시판을 공격한다. 마. XSS 코드가 실행된 결과가 공격자에게 전달되고 공격자는 공격을 종료한다.

① 라 → 가 → 나 → 다 → 마
② 라 → 가 → 다 → 나 → 마
③ 라 → 다 → 가 → 나 → 마
④ 라 → 다 → 나 → 가 → 마