2020-국가직-9급-정보시스템보안-가형-해설-곽후근

문 1. 해시함수 알고리즘에 해당하지 않는 것은?
① SHA1
② MD5
③ RMD160
④ IDEA
정답 체크
(4) 대칭키 암호 알고리즘이다.
오답 체크
(1), (2), (3) 해시함수 알고리즘이다.

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
정답 체크
(2) 컴퓨팅 리소스, 서버, 네트워킹 등을 제공한다.
오답 체크
(1) 국민들에게는 개인정보를 안전하게 관리하는 조직에게 객관적으로 식별할 수 있는 기준을 제시하여 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계이다.
(3) 전자메일, 웹 컨퍼런스, 협업, CRM, ERP 등을 제공한다.
(4) 정보통신망의 안전성 및 정보의 신뢰성을 확보하고, 조직의 정보보호 수준 제고를 위하여 관리적·기술적·물리적 보호조치를 종합한 것으로, 조직의 관리체계를 효과적으로 수립하도록 2001년 모델을 개발하여 국내 표준으로 제정되었으며 관리체계의 기본 틀이자 공통 프레임워크로 활용되고 있다.

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.
정답 체크
(1) grep에 대한 설명이고, touch는 파일의 생성과 파일의 날짜, 시간을 변경하는 명령어이다. 파일이 존재하지 않을 경우 크기가 0인 파일을 생성하기도 한다(테스트용으로 파일을 만들 때 사용).
오답 체크
(2) 파일의 소유자 또는 그룹을 변경하는 명령어이다(change owner).
(3) 파일이나 디렉토리를 이동할 때 사용하는 명령어이다(move).
(4) 마운트된 파일 시스템의 크기와 용량을 보여주는 명령어이다(disk free).

문 4. 디지털 포렌식의 원칙 중에 “수집된 증거가 위변조되지 않았음을 증명해야 한다”는 원칙은?
① 정당성의 원칙
② 신속성의 원칙
③ 무결성의 원칙
④ 연계 보관성의 원칙
정답 체크
(3) 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 함을 의미한다.
오답 체크
(1) 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(2) 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
(4) 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.

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.
정답 체크
(2) 안티 리버싱은 리버스 엔지니어링을 어렵게 만드는 기술이다.
오답 체크
(1) 안티 디버거 중 타이밍 체크는 프로세스가 디버깅 중 CPU 연산 시간이 정상적으로 실행되었을 때보다 많이 걸린다는 점에서 착안한다. RDTSC(Read Time-Stamp Counter) 명령은 두 구간 사이의 Time Stamp 값을 비교하는 것이고, 시간이 많이 걸리는 특정 구간을 디버깅 중으로 판단하고 프로그램이나 디버거를 종료한다.
(3) OllyDbg는 바이너리 코드 분석을 위한 x86 디버거이이고, IDA (Pro)는 역공학을 위한 바이너리 검사 툴이다.
(4) 실행 파일(이진 코드)로부터 소스 코드를 얻어내는 공격 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
정답 체크
(1) SMS(문자 메시지)와 Phishing의 약자이다. Phishing은 Private Data(개인 정보)와 Fishing(낚시)의 약자이다. 공격자가 문자 메시지에 URL을 보내고, 사용자가 이를 클릭하면 해킹 툴이 스마트폰에 설치되어 개인 정보가 탈취된다.
오답 체크

(2) 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입을 위한 백도어, 트로이목마 설치, 원격 접근, 내부 사용 흔적 삭제, 관리자 권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램의 모음이다.
(3) 국가 및 산업의 중요 기반 시설을 제어하는 SCADA(Supervisory Control And Data Acquisition) 시스템을 대상으로 한 웜이다. 전파를 위해 윈도우 서버 서비스의 취약점을 이용해 공유 폴더를 공격했으며 윈도우 쉘 .lnk(바로가기) 취약점을 이용해 USB를, 윈도우 프린트 스풀러 서비스의 취약점인 공유 프린터를 전파 개체로 활용했다.
(4) 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 행위를 말한다. 하드웨어, 소프트웨어를 활용한 방법에서부터 전자적, 음향기술을 활용한 기법까지 다양한 키로깅 방법이 존재한다.

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.
정답 체크
(2) 로컬 백도어에 대한 설명이고, 원격 백도어는 계정에 패스워드를 입력하고 로그인한 것처럼 원격으로 관리자 권한을 획득해 시스템에 접근하고, 네트워크에 자신의 포트를 개방한다.
오답 체크
(1), (4) NetBus, Back Orifice, Schoolbus 등은 트로이 목마로써 백도어 기능을 가진다.
(3) 서버의 셸을 얻어내 관리자로 권한 상승(Privilege Escalation)할 때 사용한다.

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
정답 체크
(1) malloc, new를 이용한 동적 메모리 할당이 해당된다.
오답 체크
(2) 지역변수, 복귀주소, 매개변수 등을 저장한다.
(3) 실행 코드(컴파일 수행 후의 이진파일)가 저장된다.
(4) 전역변수, 정적변수가 저장된다.

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

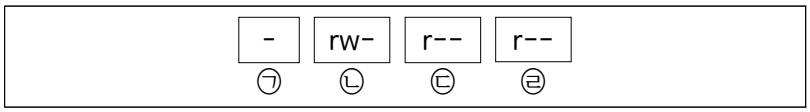
입출력에 대한 사용자의 접근 가능성이 높은 함수를 사용한다.
④ 버퍼 오버플로우 공격의 대응 방법 중에는 Non-Executable Stack, Stack Guard, Stack Shield가 있다.
정답 체크
(3) 해당 함수들은 모두 버퍼 오버플로우에 취약한 함수이다.
오답 체크
(1) 스택과 힙에서 복귀 주소를 변경하거나 메모리의 내용을 변경한다.
(2) 버퍼를 넘치면 복귀 주소 등을 변경할 수 있다.
(4) 스택 또는 힙에서 실행을 금지하거나, 카나리아(밀고자)를 사용하거나, 복귀 주소를 특수 스택에 저장한다.

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.
정답 체크
(4) FAT를 개선한 파일 시스템이 NTFS이다.
오답 체크
(1) 컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관 또는 조직하는 체제를 가리키는 말이다.
(2) 오늘날 많은 리눅스 배포판에서 주 파일 시스템으로 쓰이고 있다.
(3) 데이터 블록의 개수, 실린더 그룹의 개수, 데이터 블록의 크기 및 조각 등의 정보를 가진다.

문 11. 인증, 무결성, 부인봉쇄, 기밀성 등의 기능을 지원하는 이메일 보안 기술은?
① TFTP
② S/MIME
③ WEP
④ WPA
정답 체크
(2) 안전한 전자메일 전송을 위한 산업체 표준 규약이다. 기존 MIME 형식의 전자메일 서비스에 암호 및 보안 서비스가 추가된 구조이다.
오답 체크
(1) FTP와 마찬가지로 파일을 전송하기 위한 프로토콜이지만, FTP보다 더 단순한 방식(인증을 사용하지 않음)으로 파일을 전송한다. (예: 임의의 시스템이 원격 시스템으로부터 부팅 코드를 다운로드)
(3) 1997년 재정된 802.11 표준에서 도입되었던 WEP는 전통적인 유선 네트워크와 비슷한 데이터 보안성을 제공하기 위해 만들어졌다. 64비트 또는 128비트 키값을 사용하는 WEP는, 한때 매우 보편적으로 사용되었으며 라우터의 보안 설정에서 가장 우선적으로 표시되는 옵션이었다. 2001년 초, 암호학자들이 몇 가지 치명적인 취약점을 발견하였으며, 이를 이용하면 누구나 구할 수 있는 소프트웨어를 사용해 몇 십 분만에 WEP 연결을 크랙할 수 있다.
(4) WEP의 취약점 때문에 그 대안으로 나온 것이다. IEEE 802.11i(WPA2)의 주요 부분을 구현하는 프로토콜이고, 802.11i가 완성되기까지, WEP의 대안으로 일시적으로 사용하기 위해 개발되었다. 48비트 초기벡터를 사용하고, RC4

를 사용한다.

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.
정답 체크
(1) 일반 파일을 의미하고, 디렉토리는 'd'로 나타낸다.
오답 체크
(2) 소유자가 읽고 쓸수 있다.
(3) 그룹이 읽을 수 있다.
(4) 제3의 사용자가 읽을 수 있다.

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.
정답 체크
(4) 해당 정보는 쿠키가 아닌 로그를 통해 저장되는 정보이다.
오답 체크
(1) 클라이언트에 생성되는 4KB의 텍스트 파일이다.
(2) ID/PW, 검색 기록 등의 정보가 저장된다.
(3) 텍스트 파일이라 실행될 수 없다.

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
정답 체크
(4) SEED는 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 2월 한국인터넷진흥원과 국내 암호전문가들이 순수 국내기술로 개발한 128비트 블록 암호 알고리즘이다. 2009년 256

비트 키를 지원하는 SEED 256을 개발하였다.
오답 체크
(1) 대표적인 공개키 암호 알고리즘이다.
(2) DES를 대신할 블록 암호가 필요했고, 이를 위해 개발된 것이 트리플 DES이다. DES보다 강력하도록 DES를 3단 겹치게 한 암호 알고리즘이다.
(3) 2000년에 미국 표준 기술 연구소(NIST)에 의해 제정된 암호화 방식이다. AES의 후보로서 다수의 대칭 암호 알고리즘을 제안했지만, 그 중에서 Rijndael(라인델)이라는 대칭 암호 알고리즘이 선정되었다.

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.
정답 체크
(3) 세션 하이재킹 기법에 대한 설명이다.
오답 체크
(1), (2) 공격자가 의도한 삭제나 구매 등을 수행한다.
(4) 웹브라우저를 신용하므로 웹브라우저의 요청이 정당할 것이라 판단한다.

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
정답 체크
(4) 한정된 자원을 동시에 이용하려는 여러 프로세스가 자원의 이용을 위해 경쟁을 벌이는 현상이다. 레이스 컨디션을 이용하여 root 권한을 얻는 공격을 의미한다.
오답 체크
(1) 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다. 힙을 이용한 공격도 가능하다.
(2) printf() 사용된 %s와 같은 문자열을 가리켜 포맷 스트링이라 한다. 포맷 스트링을 조작하면(%n을 사용) 임의의 메모리 주소의 쓰기 혹은 복귀 주소를 변경할 수 있다.
(3) 전사공격, 사전공격, 사회공학, 레인보우 테이블 공격 등이 존재한다.

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.
정답 체크
(2) 재전송 공격에 해당한다.
오답 체크
(1) 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.
(3) "or"나 "="의 특수문자를 걸러낸다.
(4) 2021년에도 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
정답 체크
(3) 이블 트윈(Evil Twin, 악의적 쌍둥이) 공격 기법에 해당한다. 이블 트윈은 가짜 페이스북 ID를 의미하기도 한다.
오답 체크
(1) 프로그램에 문제가 알려지고 난 후 보안패치가 나올 때까지 시간차를 이용해 공격하는 기법을 말한다. 그러므로 로그를 통해 공격을 확인할 수 없다.
(2) 악성코드(봇)에 의한 에이전트를 전파하고, 좀비 PC에 의한 공격을 수행한다. 좀비 PC로 구성된 네트워크를 봇넷(Botnet)이라고 한다. DoS는 1:1로 공격하지만, DDoS는 N:1로 공격을 수행한다.
(4) TCP 3중 연결(3way-handshake)를 이용하는 DDoS 공격으로 공격자는 출발지 IP를 공격대상의 IP로 위조하여 syn 패킷을 다수의 반사서버로 전송하여 공격대상이 이 장비들이 응답하는 syn-ack 패킷을 받아 서비스가 거부 상태가 된다.

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 주고 받는 정보를 보호하는 데 사용된다.
④ Request는 웹서버에 데이터를 요청하거나 전송할 때 보내는 패킷으로 GET, POST와 같은 메소드를 사용한다.
정답 체크
(1) 요청한 페이지를 찾을 수 없다는 것을 의미한다.
오답 체크
(2) 1.0은 TCP 세션을 유지하지 않고, 1.1은 TCP 세션을 유지한다.
(3) HTTP에 SSL/TLS(4계층 암호화)를 적용한다.
(4) GET은 URL을 이용하고, POST는 헤더를 이용한다.

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

정답 체크

(2) 접속자가 많은 웹 사이트를 대상으로 공격자가 XSS 취약점이 있는 웹 서버에 공격용 스크립트(script)를 입력시켜 놓으면, 방문자가 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격하는 방식이다(저장 XSS).