2022-해경1차-정보관리론-해설-곽후근

1. 보안 관리 대상에 대한 〈보기〉의 설명에서 (　　)에 들어갈 용어로 다음 중 가장 옳은 것은?

〈 보 기 〉
(　㉠　) : 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
(　㉡　) : 자산에 손실을 초래할 수 있는 원하지 않는 사건의 잠재적 원인이나 행위자를 말한다.
(　㉢　) : 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.

① ㉠ 로그　㉡ 위험　㉢ 쿠키
② ㉠ 로그　㉡ 위협　㉢ 세션
③ ㉠ 백업　㉡ 위험　㉢ 세션
④ ㉠ 백업　㉡ 위협　㉢ 쿠키

정답 체크
②
ㄱ. 로그: 운영 체제나 다른 소프트웨어가 실행 중에 발생하는 이벤트나 각기 다른 사용자의 통신 소프트웨어 간의 메시지를 기록한 것을 의미한다. 로그를 활용하면 공격자를 추적할 수 있다.
ㄴ. 위협: 정보자산의 보안에 부정적 영향을 줄 수 있는 외부의 환경 또는 사건(이벤트)을 의미한다.
ㄷ. 세션: 연결 설정 과정(로그인)을 통해 연결을 맺고 있는 상태를 의미한다. 연결 해제 과정(로그오프)을 하지 않고 웹브라우저를 닫으면 세션은 남아 있는 상태가 되어 공격자가 이를 악용할 수 있다.
오답 체크
① 위험: 자산의 취약한 부분에 위협요소가 발생하여 자산의 손실, 손상을 유발한 잠재성(가능성)을 의미한다. 위험은 자산, 취약점, 위협의 상관관계(함수)로 표현할 수 있다.
③ 백업: 백업 센터나 백업 장비를 이용해서 자신이 처리하고 있는 데이터를 백업하는 것을 의미한다. 백업을 하게 되면 가용성 공격(DoS)을 막을 수 있다.
④ 쿠키: 고객이 특정 홈페이지를 접속할 때 생성되는 정보를 담은 임시 파일로 크기는 4KB 이하로 작다. 쿠키는 애초 인터넷 사용자들의 홈페이지 접속을 돕기 위해 만들어졌다. 특정 사이트를 처음 방문하면 아이디와 비밀번호를 기록한 쿠키가 만들어지고 다음에 접속했을 때 별도 절차 없이 사이트에 빠르게 연결할 수 있다.

2. 다음 중 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 가장 옳지 않은 것은?
① 생성된 수열의 비트는 무작위로 발생한다.
② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 있어야 한다.
③ 시드(seed)라고 불리는 입력 값은 외부에 알려지지 않도록 비밀로 하여야 한다.
④ 고정값 시드(seed)를 입력받아 결정적 알고리즘을 사용하여 출력 비트열을 생성한다.

정답 체크
(2) 다른 부분 수열로부터 추정될 수 없어야 한다(예측 불가능성).

오답 체크
(1) 통계적 치우침이 없는 무작위성을 의미한다.
(3) 시드를 통해 난수가 만들어지므로 비밀로 해야 한다.
(4) 결정적 알고리즘으로 해시, 대칭키, 공개키 알고리즘 등을 사용한다.

3. 다음 중 중앙 집중형 인증 방식인 커버로스 (Kerberos)에 대한 설명으로 가장 옳지 않은 것은?
① 신뢰받는 제3자인 키 배포기관이 구성원들 중간에 개입하는 방법이다.
② 커버로스는 세션키를 이용한 티켓 기반 인증 기법을 제공한다.
③ 인증 서버가 사용자에게 발급한 티켓(승인 티켓)은 유효기간 내에 재사용할 수 있다.
④ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

정답 체크
(4) Kerberos와 Active Directory를 이용하여 SSO를 구축할 수 있다.
오답 체크
(1) 신뢰받는 제3자인 AS와 TGS가 중간에 개입한다.
(2) 세션키인 K_{c-tgs}와 K_{c-v}를 사용한다.
(3) TGT는 유효기간(Lifetime2) 내에 재사용이 가능하다.

4. 다음 중 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화 되어 있는 파일로 가장 옳은 것은?
① /etc/group ② /etc/passwd
③ /etc/shadow ④ /etc/login.defs

정답 체크
③ /etc/shadow: 사용자 패스워드가 암호화
오답 체크
① /etc/group: 그룹이 등록되어 있는 파일
② /etc/passwd: 사용자에 대한 관리 정보
④ /etc/login.defs: 사용자 계정의 설정(쉘)과 관련된 기본 값을 정의한 파일

5. 다음 중 유닉스 로그파일에 대한 설명으로 가장 옳지 않은 것은?
① lastlog : 사용자들이 마지막으로 로그아웃한 정보를 가지고 있다.
② utmp : 현재 로그인한 사용자 정보를 가지고 있다.
③ wtmp : 로그인과 로그아웃, 시스템 부팅 정보를 가지고 있다.
④ sulog : su(switch user) 명령어를 실행한 정보를 가지고 있다.

정답 체크
(1) 사용자들의 최근 접속 정보를 가지고 있다.
오답 체크
(2) 유닉스에서 현재 시스템에 로그인한 사용자의 상태 출력(로깅)한다.
(3) 유닉스에서 사용자들의 로그인, 로그아웃, 시스템 재부팅 정보를 로그로 남긴다.

(4) su(switch user)는 권한 변경에 대한 로그이다.

6. 다음 중 hwp, pdf, doc 등의 문서를 암호화하여 외부 유출 시에도 기업 내부 정보를 보호하는 것으로 가장 옳은 것은?
① DRM ② CDR ③ NFV ④ EDR

정답 체크
(1) 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 불법복제를 막고 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통·관리까지를 일괄적으로 지원하는 기술이다.
오답 체크
(2) 파일을 스캔해 구조를 분석하고, 문제 있는 부분을 제거하고 다시 파일을 재조합해 안전한 파일로 제공한다.
(3) 네트워크 기술을 가상화 환경에서 동적으로 구성하고 운영하는 기술이다.
(4) 엔드포인트(고객)와 네트워크 이벤트를 모니터링하고, 발생 가능한 공격 행위에 대해 탐지, 조사, 리포트한다.

7. 다음 중 개인정보영향평가 시 고려하여야 할 사항으로 가장 옳지 않은 것은?
① 처리하는 개인정보의 수 ② 개인정보처리자의 인가 여부
③ 정보주체의 권리를 해할 가능성 및 그 위험 정도 ④ 개인정보의 제3자 제공 여부

정답 체크
(2) 개인정보처리자의 인가 여부는 개인정보영향평가 시 고려하지 않는다.
오답 체크
(1), (3), (4) “개인정보 보호법” 제33조(개인정보 영향평가)상 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항

8. 다음 중 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 가장 옳지 않은 것은?
① 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.
② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.
③ 메시지 자체를 암호화 또는 복호화 할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.
④ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화 할 수 있다.

정답 체크
(1) 하이브리드 암호 시스템은 공개키 암호를 이용하여 대칭키를 암호화하므로 대칭키 암호의 키 교환 문제가 발생하지 않는다.
오답 체크

(2) 암호화에 사용된 대칭키를 상대방에게 전달할 때 상대방의 공개키로 암호화를 수행한다.
(3) 메시지 암호화/복호화에는 대칭키를 사용한다.
(4) 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화할 수 있다.

9. 다음 중 유닉스에서 파일의 속성을 검색하는 find 옵션으로 가장 옳지 않은 것은?
① mtime : 파일의 내용이 수정된 시간을 기준으로 검색한다.
② atime : 파일에 접근한 시간을 기준으로 검색한다.
③ ctime : 파일 속성, 권한, 크기가 변경된 시간을 기준으로 검색한다.
④ rtime : 파일 실행 일자를 기준으로 검색한다.

정답 체크
(4) 해당 옵션을 존재하지 않는다.
오답 체크
(1) modified time이다.
(2) access time이다.
(3) create time이다.

10. 다음의 ㉠ ~ ㉢에 해당되는 대칭키 암호 알고리즘을 가장 옳게 나열한 것은?

〈 보 기 〉
㉠ DES의 암호화 강도가 점점 약해지면서 이를 대체하기 위한 알고리즘으로 현재 미국 연방정부 표준 블록 암호 알고리즘(NIST FIPS 197)으로 사용
㉡ 국내에서 민간 부분인 인터넷, 전자상거래, 무선통신 등에서 민감 정보 및 프라이버시 보호를 위해 한국인터넷진흥원(KISA)이 주축이 되어 개발한 128/256 비트 암호키를 지원하며 IFTF 및 ISO/IEC 국제표준으로 채택된 바 있음
㉢ 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안 기술연구소 주도로 경량 환경 및 하드웨어의 효율성 향상을 위해 개발된 128 비트 블록 암호 알고리즘으로 128/192/256 비트 암호화 키를 지원

① ㉠ AES ㉡ SEED ㉢ ARIA
② ㉠ AES ㉡ ARIA ㉢ SEED
③ ㉠ ARIA ㉡ SEED ㉢ AES
④ ㉠ ARIA ㉡ AES ㉢ SEED

정답 체크
(1) AES : 128비트 블록 길이, 128/192/256 비트 키 길이를 가진다. 키의 길이에 따라 10/12/14 라운드가 결정되며 SPN 구조(별도의 복호화기가 필요)를 가진다.
SEED : 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.
ARIA : 128비트 블록 길이, 128/192/256 비트 키 길이를 가진다. 키의 길이에 따라 12/14/16 라운드가 결정되며 Involutional SPN 구조(SPN 구조임에도 별도의 복호화기가 필요 없음)를 가진다.

오답 체크
(2), (3), (4) 주어진 선지에서 순서가 뒤바뀌었다.

11. 서버 관리자가 사용할 수 있는 보안용 소프트웨어 중 그 용도가 가장 다른 것은?
① AWstats ② Nessus
③ Acunetix ④ Nmap

정답 체크
(1) 웹, 스트리밍 미디어, 메일 및 FTP 서버와 같은 인터넷 서비스의 데이터를 분석하는 데 적합한 오픈 소스 웹 분석보고 도구이다.
오답 체크
(2) 원격지에서 다양한 방법을 통해 시스템이나 네트워크의 알려진 취약성에 대하여 점검을 수행한다.
(3) 해커들이 사용하는 웹 해킹 방법으로 웹 애플리케이션의 취약점을 찾는 휴리스틱 웹 취약점 스캐너이다.
(4) 가장 대표적인 포트 또는 IP 스캔 프로그램으로서 로컬 및 네트워크 시스템에 대한 스캔을 통해 자신이 관리하는 시스템에 자신도 알지 못하는 포트가 열려 있는지를 확인할 수 있는 도구다.

12. 리눅스 서버 관리자 A씨는 피해 시스템을 점검하던 중 다음과 같은 시스템 바이너리 파일들이 변조된 것을 확인하였다. 공격자의 입장에서 파일을 변조한 이유가 가장 옳지 않게 연결된 것은?
① ps, top : 특정 프로세스 정보를 숨김
② w, who : 특정 사용자의 정보를 숨김
③ ls, du : 특정 파일이나 디렉토리를 숨김
④ ifconfig : 특정 IP에서의 접속을 숨김

정답 체크
(4) w, who를 변조한다.
오답 체크
(1) 프로세스 관련 바이러리 파일이다.
(2) 로그 관련 바이러리 파일이다.
(3) 파일과 디렉토리 관련 바이너리 파일이다.

13. 다음은 FTP(File Transfer Protocol) 서비스에 대한 내용을 설명한 것이다. 가장 옳지 않은 것은?
① 전송계층 프로토콜로 TCP를 사용하고 있으며, 클라이언트 서버 모델로 구성되어 있다.
② IETF에 따라 RFC 959로 정의된다.
③ 기본적으로 액티브 모드(Active mode)와 패시브 모드(Passive mode)를 지원한다.
④ 제어 연결은 21 포트를, 데이터 연결은 512 이후 포트를 사용한다.

정답 체크
(4) 데이터 연결을 20 포트를 사용한다.

오답 체크
(1) TFTP는 UDP를 사용한다.
(2) 개정된 RFC는 1579, 2228, 2428이다.
(3) 데이터 채널은 서버쪽에서 연결하면 액티브이고, 클라이언트쪽에서 연결하면 패시브이다.

14. 다음 중 블록 암호 알고리즘의 종류가 아닌 것은?
① RC5 ② DES ③ MD5 ④ IDEA

정답 체크
(3) 해시 알고리즘이다.
오답 체크
(1), (2), (3) 블록 암호(대칭키) 알고리즘이다.

15. 다음은 윈도우 부팅 순서이다. 가장 옳게 나열한 것은?

〈 보 기 〉
㉠ MBR - 부팅 매 체에 대한 기본적인 파일 시스템 정보가 들어 있는 MBR 정보를 읽는다.
㉡ POST - 하드웨어 자체가 시스템에 문제가 없는지 기본적인 사항을 체크하는 과정
㉢ NTLDR - 하드디스크의 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며 boot.ini 파일의 내용을 읽는다.
㉣ NTDETECT.com - 설치된 하드웨어를 검사한다.
㉤ ntoskrnl.exe - HAL.dll을 로드한다.
㉥ CMOS - 사용자가 설정한 기본 사항을 읽어시스템에 적용한다.

① ㉥ - ㉢ - ㉣ - ㉠ - ㉤ - ㉡ ② ㉡ - ㉥ - ㉢ - ㉣ - ㉠ - ㉤
③ ㉡ - ㉥ - ㉠ - ㉢ - ㉣ - ㉤ ④ ㉥ - ㉠ - ㉤ - ㉡ - ㉢ - ㉣

정답 체크
(3) 윈도우 XP, 윈도우 서버 2000/2003의 부팅 순서는 다음과 같다.
㉡ 1단계: POST(Power On Self Test)의 실행, BIOS(Basic Input/Output system)에서 POST를 실행한다(하드웨어 체크).
㉥ 2단계: 기본 부팅 관련 설정사항 로드, CMOS(Complementary Metal-Oxide Semiconductor)에서 BIOS는 CMOS에 설정되어 있는 시스템 설정 사항 및 부팅과 관련된 여러 가지 정보를 읽어 시스템에 적용한다.
㉠ 3단계: MBR(Master Boot Record, 마스터 부트 레코드) 로드
•MBR은 저장 매체의 첫 번째 섹터(LBA 0)에 위치하는 512바이트의 영역으로, 부팅 매체에 대한 기본 파일 시스템 정보이다. 단, LBA는 보조기억장치의 Logical Block Addressing을 의미한다.
•'Missing operating system'은 운영체제가 설치되지 않았거나 CMOS에서 부팅 매체를 잘못 설정했을 때 확인한다.
㉢ 4단계: NTLDR(NT Loader) 실행, 하드 디스크의 부팅 파티션에 있는 프로그램으로, 윈도우 서버 2000이 부팅될 수 있도록 간단한 파일 시스템을 실행하고 boot.ini 파일의 내용을 읽어 가능한 부팅 옵션을 보여준다. 여기서, 활성 파티션은 C 드라이브를 의미한다.
㉣ 5단계: NTDETECT.com 실행, 하드웨어 검사를 수행한다. 여기서, 하드웨어 검사란 PC의 CPU

유형, 버스 유형, 비디오 보드 유형, 키보드와 마우스 종류, 컴퓨터에 장착되어 있는 직렬 포트와 병렬 포트, 플로피 드라이브 등의 검사를 의미한다.
㉤ 6단계: ntoskrnl.exe(NT OS Kernel) 실행, HAL.DLL(Hardware Abstraction Layer) 로드 단계
•커널 로드: 윈도우 서버 2000은 시스템 설정을 로드하고, 이것을 HKEY_LOCAL_MACHINE₩System₩CurrentControlset₩Services에 저장한다. 이 정보를 확인하여 로드할 드라이브와 그 순서를 결정한다.
•커널 초기화: 드라이브에 대한 현재의 제어 설정을 검사하고 작업을 시작한다.
•서비스 로드: 세션 관리자 서브 시스템(smss.exe)과 Win32 서브 시스템을 로드한다.
•서브 시스템 시작: 윈도우 서브 시스템이 초기화, Win32 서브 시스템은 로그인을 처리하고 Winlogon.exe를 시작한다. Ctrl+Alt+Delete를 누르면 로그인 창이 활성화되고 계정과 패스워드 입력받아 로컬 보안 인증 서버(Local Security Authentication Server, Lsass.exe)에 보내고 계정과 패스워드를 전달받은 로컬 보안 인증 서버는 보안 계정 관리자(SAM; Security Accounts Manager)에 저장된 정보와 비교한다. 일치하면 Userinit.exe 프로세스가 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion₩Winlogon의 셸 값에서 참조되는 셸을 실행한다.

16. '사이버위기경보'의 등급 중 복수 정보통신서비스제공자(ISP) 망에 장애 또는 마비가 발생하였을 경우, 발령하는 경보의 단계는 무엇인가?
① 심각 단계 ② 경계 단계
③ 주의 단계 ④ 관심 단계

정답 체크
(2) 침해사고가 다수기관에서 발생했거나 대규모 피해로 확대될 가능성이 증가한다.
오답 체크
(1) 국가 차원의 주요 정보통신망 및 정보시스템 장애 또는 마비가 발생하였다.
(3) 일부 정보통신망 및 정보시스템 장애가 발생하였다.
(4) 위험도가 높은 웜/바이러스, 취약점 및 해킹 기법 출현으로 인해 피해 발생 가능성이 증가하였다.

17. 다음 중 전자우편 보안기술 PGP의 기능으로 가장 옳지 않은 것은?
① 전자서명 ② 암호화
③ 생체인증 ④ 무결성

정답 체크
(3) PGP에 생채인증 기능은 포함되지 않는다.
오답 체크
(1) RSA, DSA를 사용한다.
(2) 대칭키와 공개키를 사용한다.
(4) 해시를 사용한다.

18. 다음의 접근통제 모델(Access Control Model) 중 무결성을 보장하기 위한 모델을 모두 고른 것은?

〈 보 기 〉
㉠ 벨라파듈라(Bell-LaPadula) 모델
㉡ 비바(Biba) 모델
㉢ 클락윌슨(Clark-Wilson) 모델

① ㉠ ② ㉡ ③ ㉠ ㉡ ④ ㉡ ㉢

정답 체크
(4) 비바 : 무결성 모델이다.
클락윌슨 : 무결성 중심의 상업용 모델이다.
오답 체크
(1), (3) ㄱ : 기밀성을 보장하기 위한 모델이다.
(2) ㄷ이 없다.

19. 다음에서 설명하는 키의 종류는 무엇인가?

〈 보 기 〉
㉠ 반복적으로 사용하는 대표키로 안전한 보관이 필요하다.
㉡ 한번만 사용하는 키로 사용이 종료되면 폐기되는 키이다.
㉢ 비대칭 암호시스템에서 전자서명용 검증키이고, 평문 데이터의 암호화용으로 사용한다.

① ㉠ 대칭키 ㉡ 세션키 ㉢ 개인키
② ㉠ 세션키 ㉡ 대칭키 ㉢ 공개키
③ ㉠ 마스터키 ㉡ 세션키 ㉢ 공개키
④ ㉠ 세션키 ㉡ 마스터키 ㉢ 개인키

정답 체크
(3) 마스터키 : 반복적으로 사용하는 키이다.
세션키 : 한번만 사용하는 키이다.
공개키 : 누구에게나 공개되어 있는 키이다.
오답 체크
(1), (2), (4) 개인키 : 전자서명용 생성키이고, 평문 데이터의 복호화용으로 사용한다(개인만 가지고 있음).

20. 해킹 수단과 그 공격 방법에 대한 설명으로 가장 옳지 않은 것은?
① Ransomware : 파일을 암호화한 후 복호화를 조건으로 금전을 요구함
② Rootkit : 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴
③ SQL Injection : 데이터베이스에 질의어를 변조하여 공격함
④ Cross-site Scripting : 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함

정답 체크
(2) 버퍼 오버플로우에 대한 설명이고, Rootkit은 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입

을 위한 백도어, 트로이목마 설치, 원격 접근, 내부 사용 흔적 삭제, 관리자 권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램의 모음이다.

오답 체크

(1) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.

(3) 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.

(4) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.