2023년03월11일년 정보보안기사 필기시험 기출문제 답안

【1과목 : 20문제】 시스템 보안	1	2	3	4	5	6	7	8	9	10
	①	①	②	③	②	②	③	①	④	②
	11	12	13	14	15	16	17	18	19	20
	②	②	④	②	④	④	①	②	②	④

【2과목 : 20문제】 네트워크 보안	21	22	23	24	25	26	27	28	29	30
	①	④	①	②	②	②	③	②	①	④
	31	32	33	34	35	36	37	38	39	40
	③	①	④	②	③	①	③	②	②	①

【3과목 : 20문제】 어플리케이션 보안	41	42	43	44	45	46	47	48	49	50
	④	③	④	②	④	④	②	③	④	①
	51	52	53	54	55	56	57	58	59	60
	②	④	④	④	①	④	②	③	④	①

【4과목 : 20문제】 정보 보안 일반	61	62	63	64	65	66	67	68	69	70
	②	①	③	④	①	①	③	④	①	④
	71	72	73	74	75	76	77	78	79	80
	①	④	①	③	④	④	②	①	④	④

【5과목 : 20문제】 정보보안 관리 및 법규	81	82	83	84	85	86	87	88	89	90
	②	②	②	③	④	②	④	②	④	①
	91	92	93	94	95	96	97	98	99	100
	③	④	④	③	①	③	④	④	②	③

전자문제집 CBT 홈페이지 : https://www.cbtestpro.kr

최신 수정 자료와 해설(오타・오답・규정변경)은 cbtestpro.kr 웹 및 앱에서 확인하세요.

기출문제의 저작권은 출제기관에 있습니다. cbtestpro.kr 및 관련 앱에서는 편집 및 재구성 작업만 하였음을 밝힙니다.

CBT기출문제

전자문제집 CBT

빠르고 효과적으로 배워 시험 합격을 노려라!

Download on the App Store

GET IT ON Google Play

【1과목】 시스템 보안 (20문제)

1. 윈도우 시스템의 사용자 계정 및 패스워드를 암호화하여 보관하고 있는 SAM(Security Account Manager)에 대한 설명으로 틀린 것은?

❶ HKEY_LOCAL_MACHINE\SAM에 저장된 키는 일반계정도 확인할 수 있다.

② 크래킹을 통해 패스워드를 얻을 수 있다.

③ 운영체제가 작동하는 한 접근할 수 없도록 잠겨져 있다.

④ 레지스트리 HKEY_LOCAL_MACHINE\SAM에 구체화된 자료들을 실제로 저장한다.

2. 디스크 스케줄링 알고리즘 중 엘리베이터 알고리즘이라고 불리는 기법은?

❶ SCAN

② SSTF

③ C-SCAN

④ FCFS

3. 윈도우에서 제공하는 BitLocker에 대한 설명으로 틀린 것은?

① 윈도우 7에서도 가능하다.

❷ exFAT 파일 시스템은 지원하지 않는다.

③ USB 저장매체도 지원 가능하다.

④ 텍스트 파일 형태의 복구키를 제공한다.

4. EDR(Endpoint Detection Response) 솔루션의 주요 기능으로 옳지 않은 것은?

① 보안사고 탐지 영역

② 보안사고 통제 영역

❸ 보안사고 확산 영역

④ 보안사고 치료 영역

5. Window 서버의 보안 옵션 설정 중 보안 강화를 위한 설정으로 옳지 않은 것은?

① “로그온 하지 않고 시스템 종료 허용”을 “사용 안함”으로 설정하였다.

❷ 원격 관리를 위해 “원격 시스템에서 강제로 종료” 정책의 “Administrators” 외 서버에 등록된 계정을 모두 등록하였다.

③ “이동식 미디어 포맷 및 꺼내기 허용” 정책이 “Administrators” 로 되어 있다.

④ “SAM 계정과 공유의 익명 열거 허용 안함” 정책을 설정하였다.

6. 웹사이트의 쿠키(cookie)에 대한 설명으로 틀린 것은?

① Set-Cookie 헤더를 통해 쿠키를 설정

❷ 여러개의 값을 추가시 “/” 특수문자를 사용

③ 쿠키의 구조는 이름=값 형태로 구성

④ 사용자 PC에 저장

7. 다음 문장에서 설명하는 공격으로 올바르게 짝지어진 것은?

- (㉠) : 시스템 또는 서비스의 ID, 패스워드에 대해서 도구를 이용하여 ID, 패스워드를 자동 조합하여 크랙하는 공격
- (㉡) : 시스템 또는 서비스의 ID, 패스워드에 대해서 도구를 이용하여 ID, 패스워드를 크랙하기 위해서 ID와 패스워드가 될 가능성이 있는 단어를 사전파일로 만들어놓고 사전파일의 단어를 대입하여 크랙하는 공격

① ㉠ : Warwalking, ㉡ : Evil Twin

② ㉠ : 사전 공격, ㉡ : 무차별 공격

❸ ㉠ : 무차별 공격, ㉡ : 사전 공격

④ ㉠ : Evil Twin, ㉡ : Wardriving

8. 내부 정보 유출 차단용 보안솔루션에 대한 설명으로 틀린 것은?

❶ 문서암호화 솔루션 : PC에 저장되는 파일을 암호화하고 외부로 유출시 복호화 기능

② 내부정보 유출 방지 솔루션 : 메일, 메신저, 웹 등을 통해 발생할 수 있는 중요정보 유출을 탐지, 차단

③ 문서중앙화 시스템 : 문서 작업의 결과가 원천적으로 PC에 남지 않으므로 파일 유출을 차단

④ 네트워크 방화벽 : PC 메신저나 웹 메일 등 내부정보유출 수단으로 쓰이는 프로그램을 네트워크 방화벽에서 도메인 기준으로 차단

9. 리눅스 환경에서 로그에 대한 설명으로 틀린 것은?

① secure 로그 : 사용자의 원격 로그인 정보를 저장

② dmesg 로그 : 시스템 부팅 관련 시스템 메시지 저장

③ lastlog 로그 : 사용자가 로그인한 마지막 로그를 저장

❹ wtmp 로그 : 사용자의 루트 접속 기록 저장

10. 윈도우 시스템 암호화에 대한 설명으로 틀린 것은?

① BitLocker는 윈도우 운영체제에서 제공하는 볼륨 단위와 암호화 기능이다.

❷ BitLocker는 컴퓨터를 시작하는데 필요한 시스템 파티션 부분도 암호화한다.

③ EFS(Encrypted File Service)는 사용자 단위 데이터 암호화 기능을 제공한다.

④ EFS(Encrypted File Service)는 컴퓨터 단일 또는 복수 사용자에게 대한 파일 및 폴더 단위 암호화를 지원한다.

11. AI나 머신러닝의 이미지 인식에 있어서 이미지 속에 인간이 감지할 수 없는 노이즈나 작은 변화를 주어 AI 알고리즘의 특성을 악용하여 잘못된 판단을 유도하는 공격은?

① Membership inversion 공격

❷ Adversarial 공격

③ Poisoning 공격

④ Model inversion 공격

12. 다음은 포맷스트링의 종류를 설명하고 있다. 형식에 대한 매개변수는?

매개변수	형식
%d	정수형 10진수 상수(integer)
(㉠)	문자스트링
(㉡)	16진수 양의 정수
(㉢)	%n의 반인 2바이트 단위

① ㉠ : %s, ㉡ : %o, ㉢ : %lf

❷ ㉠ : %s, ㉡ : %x, ㉢ : %hn

③ ㉠ : %c, ㉡ : %o, ㉢ : %lf

④ ㉠ : %c, ㉡ : %x, ㉢ : %hn

13. netstat 명령어를 통해 확인할 수 없는 정보는?

① 소켓을 열고 있는 프로세스 ID, 프로세스 이름

② 라우팅 테이블 정보

③ 열린 포트 정보

❹ 데이터 패킷

14. 리눅스에서 제공하는 Cron 기능에 대한 설명으로 틀린 것은?

① crontab –r 명령어로 등록된 데이터를 삭제할 수 있다.

❷ 루트 권한으로 실행은 불가능하다.

③ 특정 시간에 작업해야 하는 명령어 실행이 가능하다.

④ 파이썬, 펄 등의 스크립트 언어도 실행이 가능하다.

15. Visual Basic 스크립트를 이용한 악성코드에 대한 설명으로 옳은 것은?

① 웹브라우저에서 실행될 경우 스크립트가 브라우저에 내장되므로 파일의 내용을 확인하기 어렵다.

② 독립형으로 개발할 경우 파일 생성에 제한을 받아 웜형 악성코드를 만들지 못한다.

③ 확장자는 VBA 이다.

❹ 러브버그라고 불리는 이메일에 첨부되어 전파된 바이러스가 Visual Basic 스크립트로 개발되었다.

16. 다음은 sudo 설정파일(/etc/sudoers)의 내용이다. sudo를 통한 명령 사용이 불가능한 사용자는?

```
%admin ALL=(ALL) ALL
%sudo ALL=(ALL:ALL) ALL
root ALL=(ALL:ALL) ALL
guest3 ALL=(ALL:ALL) ALL
```

① uid=(10)guest1, gid(10)guest1, groups=(10)guest1,3(admin)

② uid=(11)guest2, gid(11)guest2, groups=(11)guest2,4(sudo)

③ uid=(12)guest3, gid(12)guest3, groups=(12)guest3,5(adm)

❹ uid=(13)guest4, gid(13)guest4, groups=(13)guest4,5(adm)

17. 랜섬웨어에 대한 설명으로 틀린 것은?

❶ 단방향 암호화 방식을 주로 사용한다.

② 파일 확장자를 임의 변경한다.

③ 안티바이러스 프로그램을 강제 종료한다.

④ 윈도우 복원 시점을 제거한다.

18. 리버스엔지니어링 분석 방법 중 소스코드를 이해하고 분석하는 방법으로 소프트웨어의 프로그래밍 오류와 구현 오류를 찾을 때 유용한 분석 방법은?

① 블랙박스 분석

❷ 화이트박스 분석

③ 그레이박스 분석

④ 그린박스 분석

19. 침해 당한 리눅스 서버의 하드 디스크를 umount 명령을 통해 분리하는 과정에서 “Device is busy”라는 문구 때문에 분리하지 못하고 있는 상황이다. 디바이스를 사용 중인 프로세스를 찾기 위해 사용할 수 있는 명령어로 옳은 것은?

① mount
❷ lsof
③ ps
④ netstat

20. 다음 중 파일 시스템의 무결성 보장을 위해 점검해야 할 사항으로 옳지 않은 것은?

① 파일의 소유자, 소유그룹 등의 변경 여부 점검
② 파일의 크기 변경 점검
③ 최근에 파일에 접근한 시간 점검
❹ 파일의 symbolic link의 수 점검

【2과목】 네트워크 보안 (20문제)

21. 다음 문장에서 설명하는 보안시스템은?

- 과거 IP 관리 시스템에서 발전한 솔루션으로 기본적인 개념은 IP 관리 시스템과 거의 같고, IP 관리 시스템에 네트워크에 대한 통제를 강화한 보안시스템이다.
- 접근 제어 및 인증 기능은 일반적으로 MAC 주소를 기반으로 수행된다.

❶ NAC
② DRM
③ SSO
④ IDS

22. 봇넷(Botnet) 또는 C&C(Command & Control)에 많이 사용되는 프로토콜로 IRC(Internet Relay Chat) 프로토콜이 있다. 다음 중 IRC의 기능이 아닌 것은?

① 다수의 사용자들과 텍스트 메시지를 공유
② 사용자들 간의 파일 전송
③ 한 클라이언트의 사용자가 다른 클라이언트 상에서 실행 가능한 메시지 전송
❹ 바이러스 프로그램의 제작

23. 어느 회사의 메일 서버가 스팸 메일 발송 경유지로 악용하는 사례가 발생하였다. 이 때 보안관리자는 pcap 파일을 통해 패킷 분석을 진행하고자 보기와 같은 필터링을 실행하엿다. 다음 필터링 결과에 대한 설명으로 옳은 것은?

```
SMTP.req.command == "EHLO"
```

❶ 이메일 서비스 확장 지원 세션을 시작한 것을 필터링
② SMTP 세션을 시작한 것을 필터링
③ 서버에 인증을 시작한 것을 필터링
④ 메일 데이터 전송을 한 것을 필터링

24. 리버싱을 하기 위해서는 여러 가지 도구가 필요하다. 제시된 도구들과 그 역할이 올바르게 짝지어진 것은?

㉠ OllyDbg	ⓐ PE 파일의 구조와 동작 확인
㉡ Procexp	ⓑ 파일 이벤트 정보 확인
㉢ Filemonitor	ⓒ 프로세스 동작 정보 확인

① ㉠-ⓐ, ㉡-ⓑ, ㉢-ⓒ
❷ ㉠-ⓐ, ㉡-ⓒ, ㉢-ⓑ
③ ㉠-ⓒ, ㉡-ⓑ, ㉢-ⓐ
④ ㉠-ⓒ, ㉡-ⓐ, ㉢-ⓑ

25. 스니핑(sniffing) 기법으로 틀린 것은?

① Switch Jamming
❷ SYN Flooding
③ ARP Redirect
④ ICMP Redirect

26. 2016년에 처음 발견되었으며, IP 카메라나 가정용 라우터와 같은 IoT 장치를 주요 공격 대상으로 삼는 DDoS 공격용 봇넷은?

① 님다(Nimda)
❷ 미라이(Mirai)
③ 스턱스넷(Stuxnet)
④ SQL슬래머(Slammer)

27. ARP 스푸핑(Spoofing)은 LAN(Local Area Network) 상에서 MAC 주소를 조작하는 공격기법이다. 이에 대한 설명으로 옳은 것은?

① 시스템의 ARP 테이블을 동적(Dynamic)으로 관리한다.

② ping [ip주소] 명령을 사용하여 시스템을 모니터링한다.

❸ arp –s [ip주소] [mac 주소] 명령을 통해 ARP 테이블을 관리한다.

④ nslookup [mac 주소] 명령을 사용해 통신경로를 절대경로로 설정한다.

28. Tcpdump 를 사용한 패킷 스니핑에 관한 설명이다. 괄호 안에 들어갈 적당한 말은?

- (㉠) : 동일 Segment 내 패킷을 복제하여 정보를 수집한다.
- (㉡) : 목적지의 MAC 주소가 같지 않아도 패킷을 폐기하지 않고 수신한다.

① ㉠ : 포트 스캐닝, ㉡ : 단일 모드

❷ ㉠ : 포트 미러링, ㉡ : 무차별 모드

③ ㉠ : 포트 미러링, ㉡ : 단일 모드

④ ㉠ : 포트 스캐닝, ㉡ : 무차별 모드

29. 네트워크 침입탐지와 방지를 위해 ModSecurity를 설치 운용하고자 한다. ModSecurity 정책 설정을 위해 SecAuditEngine에서 설정할 수 없는 것은?

❶ DetectionOnly

② On

③ Off

④ RelevantOnly

30. 정찰공격(reconnaissance attack)을 위해 사용되는 도구가 아닌 것은?

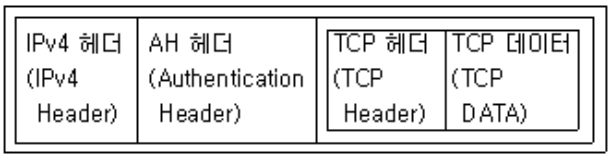
① 핑 스윕(Ping sweep)

② 포트 스캔(Port scan)

③ 패킷 스니퍼(Packet sniffer)

❹ 포트 리다이렉션(Port redirection)

31. 다음 IPv4(IP version 4) 데이터그램에 대한 설명으로 옳은 것은?



① IPsec(IP Security) 터널모드(Tunnel)의 데이터그램이다.

② IPsec(IP Security)의 AH(Authentication Header)가 적용되어 TCP헤더와 TCP데이터는 암호화되어 있다.

❸ IPsec(IP Security)의 AH(Authentication Header)가 적용되어 SA(Security association)를 식별할 수 있다.

④ IPsec(IP Security)의 AH(Authentication Header)가 적용되어 IPv4 헤더에 무결성, 인증을 위한 데이터가 추가된 데이터그램이다.

32. 네트워크 처리 능력을 개선하고자 VLAN을 구성할 때 VLAN 오/남용을 경감시키기 위한 방법으로 옳지 않은 것은? (단, 스위치에 연결된 호스트들을 그룹으로 나누어서 VLAN-1(native)과 VLAN-2로 그룹을 설정하였다고 가정한다.)

❶ 관리상 VLAN 관리 정책 서버(VMPS)를 사용한다.

② native VLAN 포트 (VLAN ID 1)에 대한 접근을 제한한다.

③ 트렁크 포트들의 native VLAN에 신뢰할 수 없는 네트워크를 붙이지 않는다.

④ 모든 포트에 동적 트렁킹 프로토콜(DTP)을 꺼 놓는다.

33. 다음 문장은 어떤 스푸핑(spoofing) 공격인가?

32bit IP 주소를 48bit의 네트워크 카드 주소[MAC Address]로 대응시켜 주는 프로토콜로 실제 IP 주소를 통해 네트워크 연결을 시도하면 TCP/IP 에서는 해당 IP에 해당하는 네트워크 카드 주소를 찾아 연결하게 된다. 이더넷 환경에서 공격대상자의 cache 테이블에 공격자가 원하는 IP에 대한 네트워크 카드 주소[MAC Address] 쌍을 업데이트하여 공격대상자의 패킷 흐름을 공격자가 원하는 방향으로 조절하여 공격하는 기술이다.

① e-mail 스푸핑

② IP 스푸핑

③ DNS 스푸핑

❹ ARP 스푸핑

34. 네트워크 공격 유형이 아닌 것은?

① 패킷 스니핑 공격

❷ 포맷스트링 공격

③ 서비스거부 공격

④ 스푸핑 공격

35. IDS(Intrusion Detection System)에 대한 설명으로 틀린 것은?

① 감사와 로깅할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않는다.

② 네트워크에서 백신과 유사한 역할을 하는 것으로 네트워크를 통한 공격을 탐지하기 위한 장비이다.

❸ 네트워크를 통한 공격을 탐지할뿐 아니라 차단을 수행한다.

④ 설치 위치와 목적에 따라 HIDS와 NIDS로 나뉠 수 있다.

36. 윈도우즈 시스템에서 포트번호와 서비스명 및 전송 프로토콜이 올바르게 연결된 것은?

❶ 138-NetBIOS 데이터그램 서비스-UDP

② 139-NetBIOS 세션 서비스-UDP

③ 110-POP3-UDP

④ 143-IMAP-UDP

Download on the App Store 전자문제집 CBT(App Store) :[다운로드]
GET IT ON Google Play 전자문제집 CBT(Google Play) :[다운로드]

37. 다음 문장의 (가), (나)에 들어갈 말로 올바르게 연결된 것은?

- (가) 은/는 악의적인 프로그램을 건전한 프로그램처럼 포장하여 일반 사용자들이 의심없이 자신의 컴퓨터 안에서 이를 실행시키고 실행된 (가) 은/는 특정 포트를 열어 공격자의 침입을 돕고 추가적으로 정보를 자동 유출하며 자신의 존재를 숨긴다.
- (나) 은/는 OS에서 버그를 이용하여 루트권한 획득 또는 특정 기능을 수행하기 위한 공격 코드 및 프로그램을 의미한다.

① 가 : Exploit, 나 : Trojan

② 가 : Imapd, 나 : Trojan

❸ 가 : Trojan, 나 : Exploit

④ 가 : Exploit, 나 : Imapd

38. 다음 문장에서 설명하는 VPN(Virtual Private Network)으로 옳은 것은?

- OSI 7 Layer 중 2 Layer에서 동작
- IKE(Internet Key Exchange)와 ESP(Encapsulation Security Payload)를 사용
- 대부분의 운영체제 및 네트워크 장비에서 지원

① PPTP

❷ L2TP

③ SSTP

④ SSH

39. 다음은 스노트(snot)룰 예시이다. 룰의 구성에 대한 설명으로 틀린 것은?

```
alert tcp any any -> any 80 (msg:"HTTP Get Flooding Detect"; content:"GET/HTTP1"; depth 13; nocase; threshold; type threshold, track by src, count 10, seconds 1; sid:1000001)
```

① alert를 발생하고 로그를 남긴다.

❷ 패턴 매칭시 대소문자를 구분한다.

③ content를 첫 번째 바이트로부터 13번째 바이트 범위안에서 검사한다.

④ 출발지를 기준으로 매 1초동안 10번째 이벤트마다 action을 수행한다.

40. 무선LAN 통신에서 패스프레이즈와 같은 인증없이 단말과 액세스 포인트간의 무선 통신을 암호화하는 것은?

❶ Enhanced Open

② FIDO2

③ WebAuthn

④ WPA3

【3과목】 어플리케이션 보안 (20문제)

41. 다음 문장에서 설명하는 공격 위협은?

> 해당 취약점이 존재할 경우 브라우저를 통해 특정 디렉터리 내 파일 리스트를 노출하여 응용시스템의 구조를 외부에 허용할 수 있고, 민감한 정보가 포함된 설정 파일 등이 노출될 경우 보안상 심각한 위험을 초래할 수 있다.

① 정보 누출
② 악성 콘텐츠
③ 크로스사이트 스크립팅
❹ 디렉터리 인덱싱

42. 다음 중 무선 인터넷 보안 기술에 대한 설명이 맞게 짝지어진 것은?

① WAP(Wireless Application Protocol) - 무선 전송계층 보안을 위해 적용한다.
② WTLS(Wireless Transport Layer Security) - 이동형 단말기에서 인터넷에 접속하기 위해 고안된 통신 규약이다.
❸ WSP(Wireless Session Protocol) - 장시간 활용하는 세션을 정의하고 세션 관리를 위해 Suspend/Resume 기능과 프로토콜 기능에 대한 협상이 가능하다.
④ WTP(Wireless Transaction Protocol) - IEEE 802.11i 표준에 정의된 보안규격으로 RC4 알고리즘을 기반으로 한다.

43. PGP(Pretty Good Privacy)에서 사용하는 암호 알고리즘이 아닌 것은?

① RSA
② SHA
③ Diffie-Hellman
❹ AES

44. 익명 FTP 보안 대책 수립에서 익명 FTP에 불필요한 항목(계정 등)을 제거하기 위한 파일의 경로로 옳은 것은?

① /etc/pam.d/ftp
❷ /etc/ftpusers
③ $root/etc/passwd
④ /bin/etc/pub

45. 홈·가전 IOT 제품들의 주요 보안위협 원인으로 틀린 것은?

① 인증메커니즘 부재
② 물리적 보안 취약점
③ 강도가 약한 비밀번호
❹ 취약한 DBMS 버전

46. 다음 중 SQL Injection의 공격 유형이 아닌 것은?

① 인증 우회
② 데이터 노출
③ 원격 명령 실행
❹ 서비스 거부

47. 버퍼오버플로우 공격을 막기 위해 사용을 권장하는 프로그램 함수는?

① strcat( )
❷ strncat( )
③ gets( )
④ sscanf( )

48. 다음 문장에서 설명하는 것은?

> 주문정보의 메시지 다이제스트와 지불정보의 메시지 다이제스트를 합하여 다시 이것의 메시지 다이제스트를 구한 후 고객의 서명용 개인키로 암호화한다.

① 복합서명
② 복합암호화
❸ 이중서명
④ 이중암호화

49. 다음 문장에서 설명하는 공격 대응 방법은?

> 악성봇에 감염된 PC를 해커가 제어하지 못하도록 하는 방법으로 악성봇이 해커의 제어 서버에 연결 시도시 특정 서버로 우회 접속되도록 하여 해커의 악의적인 명령을 전달받지 못하도록 한다.

① DNS 라우팅
② DNS 스푸핑
③ DNS 웜홀
❹ DNS 싱크홀

50. 안드로이드 앱 구조 요소 중 앱 실행시 반드시 필요한 권한을 선언하며, 안드로이드 빌드 도구 및 안드로이드 운영체제에 관한 필수 정보를 설명하는 파일은?

❶ AndroidManifest.xml

② MainActivity

③ activity_main.xml

④ build.gradle

51. 이메일 클라이언트를 이용해 이메일을 발송하는 경우 SMTP가 사용된다. 인증절차 후 이메일을 발송하는 절차로 옳은 것은? (문제 오류로 가답안 발표시 2번으로 발표되었지만 확정답안 발표시 모두 정답처리 되었습니다. 여기서는 가답안인 2번을 누르면 정답 처리 됩니다.)

① EHLO>MAIL>RCPT>DATA>QUIT

❷ EHLO>AUTH>RCPT>MAIL>DATA>QUIT

③ AUTH>EHLO>RCTP>DATA>QUIT

④ AUTH>EHLO>RCTP>MAIL>DATA>QUIT

52. 다음 중 안드로이드 시스템 권한에 대한 설명으로 틀린 것은?

① ACCESS_CHECKIN_PROPERTIES : 체크인 데이터베이스의 속성테이블 액세스 권한

② LOADER_USAGE_STATS : 액세스 로그 읽기 권한

③ SET_PROCESS_LIMIT : 제한처리 지정 권한

❹ CHANGE_COMPONENT_ENABLED_STATE : 환경 설정 변경 권한

53. XSS(Cross-Site Scripting)에 대한 설명으로 틀린 것은?

① XSS 공격은 다른 사용자의 정보를 추출하기 위해 사용되는 공격 기법을 말한다.

② 사용자가 전달하는 입력값 부분에 스크립트 태그를 필터링 하지 못하였을 때 XSS 취약점이 발생한다.

③ Stored XSS는 게시판 또는 자료실과 같이 사용자가 글을 저장할 수 있는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 기법을 말한다.

❹ Reflected XSS는 웹 애플리케이션상에 스크립트를 저장해 놓은 것이다.

54. 검색엔진에서 자동으로 사이트를 수집 및 등록하기 위해서는 사용하는 크롤러(Crawler)로부터 사이트를 제어하기 위해서 사용하는 파일은?

① crawler.txt

② access.conf

③ httpd.conf

❹ robots.txt

55. 안드로이드(Android) 플랫폼을 기반으로 개발된 모바일 앱의 경우, 디컴파일 도구 이용시 실행파일(.apk)을 소스코드로 쉽게 변환시킬 수 있어 앱 구조 및 소스코드를 쉽게 분석할 수 있다. 이를 방지하기 위한 기술은?

❶ 난독화

② 무결성 점검

③ 안티 디버깅

④ 루팅

56. 다음 중 DNS 증폭 공격(DNS Amplification DDoS Attack)에 대한 설명으로 틀린 것은?

① DNS 질의는 DNS 질의량에 비하여 DNS 서버의 응답량이 훨씬 크다는 점을 이용한다.

② DNS 프로토콜에는 인증 절차가 없다는 점을 이용한다.

③ Open DNS Resolver 서버에 DNS Query의 Type을 “Any”로 요청한다.

❹ 대응 방안으로 DNS 서버 설정을 통해 내부 사용자의 주소만 반복쿼리(Interactive Query)를 허용한다.

57. 다음 문장에서 설명하는 데이터베이스의 보안 사항은?

> 각 사용자에 대해 참조 테이블의 각 열에 대한 권한을 설정하는 것이 불편해서 만든 가상 테이블이다.

① DDL(Data Definition Language)

❷ 뷰(View)

③ SQL(Structed Query Language)

④ DCL(Data Control Language)

58. 어플리케이션의 공유 라이브러리에 대한 호출을 확인하기 위해 사용되는 리눅스의 디버깅 유틸리티는?

① windbg

② jdbc

❸ ltrace

④ tcpdump

59. 다음 문장에서 설명하는 것은?

> 모든 거래 당사자가 상호 운영성과 일관성이 확보된 환경에서 안전하게 전자상거래 정보를 사용할 수 있도록 개방형 기반 구조를 제공하는 것을 목표로 하여 전자상거래를 위해 UN/CEFACT와 민간 비영리 IT 표준화 컨소시엄인 OASIS가 개발한 전자상거래 분야 개방형 표준이다.

① EDI(Electronic Data Interchange)

② XML/EDI

③ XML(Extensible Markup Language)

❹ ebXML(Electronic Business Extensible Markup Language)

60. 다음 설명과 같이 서버에서 활성화 여부를 점검해야하는 프로토콜은?

> - 파일 전송을 위한 프로토콜로서 FTP 서비스보다 구조가 단순하며, 적은 양의 데이터를 보낼 때 사용한다.
> - 주로 원격의 부팅파일을 불러오거나 설치 프로세스를 시작하기 위한 초기 데이터 호출 용도로 사용한다.
> - 사용시 인증절차가 없어 보안에 취약하다.

❶ tftp

② vsftp

③ ftp

④ proftp

【4과목】 정보 보안 일반 (20문제)

61. CRL(Cetificate Revocation List)에 포함되는 정보는?

① 만료된 디지털 인증서의 공개키

❷ 만료된 디지털 인증서 일련번호

③ 만료일 내에 만료된 디지털 인증서의 공개키

④ 만료일 내에 만료된 디지털 인증서 일련 번호

62. 다음 문장은 어떤 인증방식을 설명한 것인가?

> 원격 사용자 인증시 유발되는 패스워드 재사용 공격을 방지하기 위한 기술이며, 사용시마다 매번 바뀌는 일회성 사용자 인증암호 및 체계로 사용자의 관리 소홀이나 패스워드가 노출되는 것을 방지하기 위한 인증방식이다.

❶ OTP

② UTP

③ SEP

④ 전자화폐

63. SSL/TLS에 대한 설명으로 옳은 것은?

① SSL/TLS을 사용하고 있는 기업은 신뢰할 수 있기 때문에 신용카드 번호를 보내도 된다.

② SSL/TLS에서는 공개키가 서버로부터 오기 때문에 클라이언트는 공개키를 가지고 있지 않아도 서버를 인증할 수 있다.

❸ SSL/TLS 1.3을 사용하면 통신의 기밀성을 확보할 수 있다.

④ SSL/TLS에서는 통신 전의 데이터, 통신 중의 데이터, 통신 후의 데이터를 보호해준다.

64. 해시값과 메시지 인증 코드(Message Authentication Code, MAC)에 대한 설명으로 틀린 것은?

① 해시값만을 통해 두사람이 문서를 주고 받았을 때 MITM(Man-In-The-Middle, 중간자 공격)공격을 받을 수 있다. 즉, 해시값을 보고 수신된 문서 위변조에 대한 상호신뢰를 확신할 수 없다.

② 해시값에 암호개념을 도입한 것이 HMAC(Hash Message Authentication Code)이며, 이때 메시지 송수신자는 비밀키(Encryption Key) 또는 세션키(session Code)를 사전에 안전한 채널을 통해 공유해야 한다.

③ 메시지 인증을 위해서는 사용되는 Message Digest(해시값)는 메시지 저장소에 파일이 위변조되지 않았다는 것을 보장하기 위해서 사용하기도 한다.

❹ 메시지 크기와 상관없이 MAC 생성과정, 즉 해시값 생성, 암호화 등이 속도는 균일하여 다른 암호화 알고리즘에 비해 속도가 빠르다.

65. OTP(One Time Password)와 HSM(Hardware Security Module)에 대한 설명으로 틀린 것은?

❶ OTP는 공개키를 사용한다.

② OTP는 PKI를 개변 연동한다.

③ HSM의 안정성 인증 적용 표준은 FIPS 140-2 이다.

④ HSM은 공개키를 사용한다.

66. 다음 문장에서 설명하는 원칙은?

> 모든 사용자는 현재 작업을 완료하는데 필요한 최소한의 권한만 가진 사용자 계정으로 로그온해야 하며, 그 이상의 권한을 부여하지 않는다.

❶ 최소 권한

② 필요 권한

③ 불필요 권한

④ 등급 권한

67. 다음 중 빅데이터 비식별화 처리기법 중 가명처리 방법에 해당하는 것은?(문제 오류로 가답안 발표시 3번으로 발표되었지만 확정답안 발표시 모두 정답처리 되었습니다. 여기서는 가답안인 3번을 누르면 정답 처리 됩니다.)

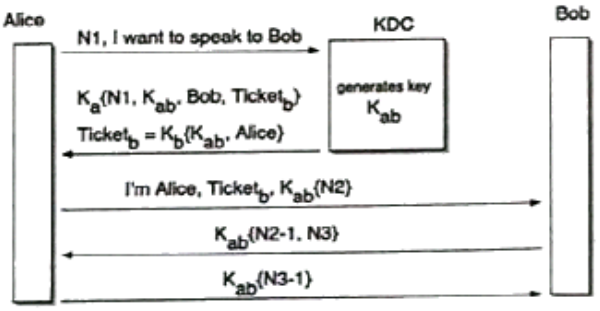
① 총계처리

② 랜덤 라운딩

❸ 암호화

④ 재배열

68. 다음 그림의 Needham-Schroeder 프로토콜에 대한 설명으로 틀린 것은?



① 사용자 Alice는 사용자 Bob과 공유할 대칭키를 KDC에게 생성해주도록 요청한 후 사용자 Bob과 안전하게 공유하게 된다.

② 사용자 Alice와 KDC, 사용자 Bob과 KDC 간에 전달되는 메시지는 사전에 공유된 대칭키인 마스터키를 이용하여 암호화되어 전달되므로 안전하게 보호된다.

③ 사용자 Alice와 Bob이 난수 N2와 N3를 암호화해서 교환하고 암호화된 N2-1과 N3-1을 받는 이유는 상호인증 기능을 수행하는데 목적이 있다.

❹ 이 방식은 공격자가 Ticketb와 Kab{N2}를 스니핑하여 복제한 후 복제된 메시지와 Alice로 위장한 자신의 신분 정보를 보내는 재전송공격에 취약한 단점이 있다.

69. 보안 인증기법에 대한 설명으로 틀린 것은?

❶ OTP 인증기법은 지식기반 인증방식으로 고정된 시간 간격 주기로 난수값을 생성하고, 생성된 난수값과 개인 PIN 번호 입력을 통해 인증시스템의 정보와 비교하여 사용자 인증을 수행한다.

② ID/PW 인증기법은 지식기반 인증방식으로 타 인증방식에 비해 구축비용이 적고 사용하기 편리하다는 장점이 있다.

③ 공인인증서 인증기법은 소유기반 인증방식으로 별도 매체의 고유정보를 제시하도록 함으로써 사용자 인증을 수행한다.

④ I-PIN(Internet Personal Identification Number)는 지식기반 인증방식으로 'ID/PW'와 주민번호를 대체하기 위하여 만들어졌다.

70. 다음 중 OCSP(Online Certificate Status Protocol : 온라인 인증서 상태 프로토콜) 서버의 응답값 중 인증서 상태표시 메시지가 아닌 것은?

① good

② revoked

③ unknown

❹ bad

71. 다음 문장에서 설명하는 사전 키 분배 방식은?

> 키 분배센터(KDC : Key Distributin Center)에서 두 노드에게 임의의 함수값을 전송하면 두 노드는 전송받은 정보로부터 두 노드 사이의 통신에 필요한 세션키를 생성한다.

❶ Blom 방식
② 커버로스 방식
③ 공개키분배 방식
④ 키 로밍 방식

72. 다음은 Diffie-Hellman 알고리즘에 대한 내용을 설명한 것이다. 괄호 안에 들어가야 할 내용은?

> Diffie-Hellman 알고리즘은 이산로그 문제에 기반을 두고 있다. 키 분배 센터는 큰 소수 p를 선정하고, 원시근 g를 찾아 공개한다. 가입자는 (㉠)를 선정하고 (㉡)를 계산하여 공개한다.

① ㉠ : 공개키, ㉡ : 개인키
② ㉠ : 마스터키, ㉡ : 공개키
③ ㉠ : 임시키, ㉡ : 고정키
❹ ㉠ : 개인키, ㉡ : 공개키

73. 다음 문장에서 설명하는 접근통제 구성요소는?

> 시스템 자원에 접근하는 사용자 접근모드 및 모든 접근통제 조건 등을 정의

❶ 정책
② 매커니즘
③ 보안모델
④ OSI 보안구조

74. 온라인 인증서 상태 프로토콜(OCSP : Online Centificate Status Protocol)에 대한 설명으로 틀린 것은?

① OCSP는 X.509를 이용한 전자 서명 인증서의 폐지 상태를 파악하는데 사용되는 인터넷 프로토콜이다.
② RFC 6960으로 묘사되며, 인터넷 표준의 경로가 된다.
❸ 온라인 인증서 상태 프로토콜을 통해 전달받는 메시지들을 AES로 암호화되며, 보통 HTTP로 전달받는다.
④ 이 프로토콜의 도입 이유 중 하나는 고가의 증권 정보나 고액의 현금 거래 등 데이터 트랜잭션의 중요성이 매우 높은 경우 실시간으로 인증서 유효성 검증이 필요하기 때문이다.

75. 다음 중 신규 OTP 기술에 대한 설명으로 틀린 것은?

① 거래연동 OTP란 수신자계좌번호, 송금액 등의 전자금융 거래 정보와 연동되어 OTP를 발생시키는 OTP로 정의된다.
② USIM OTP는 사용자의 휴대폰의 USIM내에 OTP모듈 및 주요정보를 저장하여 OTP를 안전하게 생성하고 인증을 수행하는 OTP이다.
③ 스마트 OTP란 IC칩 기반의 스마트카드와 NFC 기능을 지원하는 스마트폰에 OTP를 발생시키는 것이다.
❹ MicroSD OTP란 사용자 휴대폰의 MicroSD내에 OTP 모듈 및 주요정보를 저장하여 복제가 되지 않는 안전한 IC칩 기반의 OTP이다.

76. 메시지 인증 코드(MAC)의 재전송 공격을 예방하기 위한 방법으로 옳지 않은 것은?

① 순서 번호
② 타임스탬프
③ 비표
❹ 부인방지

77. 암호화 장치에서 암호화 처리시에 소비 전력을 측정하는 등 해당 장치 내부의 비밀 정보를 추정하는 공격은?

① 키로거
❷ 사이드채널 공격
③ 스미싱
④ 중간자 공격

78. RSA 암호시스템에서 다음의 값을 이용한 암호문 C값은?

> - 조건 : 공개값 e=2, 비밀값 d=3, 평문 P=5, 모듈러 n=4
> - 암호문 C = 평문 Pe mod n

❶ 1
② 3
③ 5
④ 7

79. 다음 중 스마트카드에 대한 설명으로 틀린 것은?

① 접촉식 스마트카드는 리더기와 스마트카드의 접촉부(CHIP) 사이의 물리적 접촉에 의해 작동하는 스마트카드이다.

② SIM카드는 가입자 식별 모듈(Subscriber Identification Module)을 구현한 IC 카드이다.

③ 인증 데이터 저장을 위해 서명된 정적 응용 프로그램 데이터와 인증기관(CA)의 개인키로 발행자의 공개키를 암호화된 데이터를 스마트카드에 저장한다.

❹ 인증기관(CA)의 개인키를 스마트카드 단말에 배포한다.

80. 다음 중 접근통제 정책이 아닌 것은?

① MAC

② DAC

③ RBAC

❹ ACL

【5과목】 정보보안 관리 및 법규 (20문제)

81. 보통의 일반적인 데이터로부터 비밀정보를 획득할 수 있는 가능성을 의미하며, 사용자가 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하는 것은? (문제 오류로 가답안 발표시 2번으로 발표되었지만 확정답안 발표시 2, 4번이 정답처리 되었습니다. 여기서는 가답안인 2번을 누르시면 정답 처리 됩니다.)

① 집합(aggregation)

❷ 추론(inference)

③ 분할(partition)

④ 셀 은폐(cell suppression)

82. 이 표준은 조직이나 기업이 정보보안 경영시스템을 수립하여 이행하고 감시 및 검토, 유지, 개선하기 위해 필요한 요구사항을 명시하며, 국제표준화기구 및 국제전기기술위원회에서 제정한 정보보호 관리체계에 대한 국제표준이다. Plan-Do-Check-Action(PDCA, 구축-실행-유지-개선) 모델을 채택하여 정보자신의 기밀성, 무결성, 가용성을 실현하기 위하여 관련 프로세스를 체계적으로 수립, 문서화하고 이를 지속적으로 운영, 관리하는 표준은?

① ISMS-P

❷ ISO27001

③ ISMS

④ ISO27701

83. A 쇼핑몰에서 물품 배송를 위해 B 배송업체와 개인정보처리 업무 위탁 계약을 맺었고 이름, 주소, 핸드폰번호를 전달하였다. A 쇼핑몰이 B 배송업체를 대상으로 관리 감독할 수 없는 것은?

① B 배송업체의 직원을 대상으로 개인정보보호 교육을 한다.

❷ B 배송업체에서 개인정보취급자를 채용할 것을 요청해야 한다.

③ B 배송업체가 개인정보를 안전하게 처리하고 있는지 점검해야 한다.

④ B 배송업체가 재위탁을 하지 못하도록 제재한다.

84. 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은?

① 범죄의 예방 및 수사를 위하여 필요한 경우

② 시설안전 및 화재 예방을 위하여 필요한 경우

❸ 쇼핑몰 고객의 이동경로 수집·분석 및 제공을 위하여 필요한 경우

④ 교통단속을 위하여 필요한 경우

85. 다음 문장에서 설명하는 위험분석을 방법론은?

- 어떤 사건도 기대대로 발생하지 않았다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법
- 적은 정보를 가지고 전반적인 가능성을 추론할 수 있고, 위험분석팀과 관리층 간의 원활한 의사소통을 가능케 한다. 그러나 발생 가능한 사건의 이론적인 추측에 불과하고 정확도, 완성도, 이용기술의 수준 등이 낮을 수 있음

① 과거자료 분석법

② 확률 분포법

③ 델파이법

❹ 시나리오법

86. 다음 문장에서 설명하는 포렌식 수행 절차 단계는?

- 컴퓨터의 일반적인 하드디스크를 검사할 때는 컴퓨터 시스템 정보를 기록한다.
- 복제 작업을 한 원본 매체나 시스템의 디지털 사진을 찍는다.
- 모든 매체에 적절한 증거 라벨을 붙인다.

① 수사 준비

❷ 증거물 획득

③ 분석 및 조사

④ 보고서 작성

87. 재택·원격근무시 지켜야 할 정보보호 실천 수칙 중 보안관리자가 해야할 일이 아닌 것은?

① 원격 접속 모니터링 강화

② 일정시간 부재시 네트워크 차단

③ 재택근무자 대상 보안지침 마련 및 보안인식 제고

❹ 원격에서 사내 시스템 접근시 VPN을 사용하지 않고 VNC 등 원격 연결 프로그램 사용

88. 다음 문장에서 설명하고 있는 포렌식으로 획득한 증거의 법적인 효력 보장을 위한 5대 원칙은?

> 증거는 절차를 통해 정제되는 과정을 거칠 수 있다. 예를 들면 시스템에서 삭제된 파일이나 손상된 파일을 복구하는 과정 등을 말한다. 이 증거를 법정에 제출하기 위해서는 동일한 환경에서는 반드시 동일한 결과가 생성되어야 하며, 만약 동일한 환경에서 서로 다른 결과가 나온다면 그 증거는 법적으로 유효성을 인정받을 수 없으며, 동일한 결과와 생성에 따른 법적 유효성 보장과 관련된 원칙이다.

① 정당성의 원칙

❷ 재현의 원칙

③ 신속성의 원칙

④ 연계 보관성의 원칙

89. 다음 중 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(클라우드컴퓨팅법)에 따른 클라우드컴퓨팅 기술연구, 도입 및 이용 활성화, 전문인력 양성 등을 전담하는 전담기관에 해당하지 않는 것은?

① 한국지능정보사회진흥원

② 한국지역정보개발원

③ 한국인터넷진흥원

❹ 한국전자통신연구원

90. 과학기술정보통신부장관이 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 법에 정한 기준에 적합한지에 관하여 인증을 할 수 있도록 하는 정보보호 관리체계 인증(ISMS)을 명시한 법률은?

❶ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

② 전자서명법

③ 개인정보보호법

④ 정보통신기반 보호법

91. 다음 중 정보자산 중요도 평가에 관한 설명으로 틀린 것은?

① 기밀성, 무결성, 가용성에 기반하여 자산 중요도를 평가

② 인터넷을 통해 서비스를 제공하는 웹서버는 가용성을 가장 높게 평가

❸ 백업데이터는 내화금고에 보관하고 있으므로 무결성을 가장 낮게 평가

④ 고객 개인정보, 임직원 개인정보를 기밀성을 가장 높게 평가

92. 다음은 CERT가 정의하는 보안사고를 서술한 것이다. 일반 보안사고가 아닌 중대 보안사고에 해당하는 것을 모두 고른 것은?

> ㉠ 악성 소프트웨어(웜, 바이러스, 백도어, 트로이 목마 등)에 의한 침해
> ㉡ 네트워크 및 시스템에 대한 비인가된 침해 시도
> ㉢ 보안 장치의 변경이나 파괴(출입보안, 침입탐지 시스템, 잠금장치, 보안 카메라 등)
> ㉣ 정보자산의 오용으로 대외 이미지에 중대한 손상을 끼친 경우

① ㉠, ㉢

② ㉠, ㉣

③ ㉡, ㉢

❹ ㉢, ㉣

93. 다음 중 금융회사 또는 전자금융업자가 설치·운영하는 정보보호위원회의 심의·의결 사항으로 틀린 것은?

① 정보기술부문 계획서에 관한 사항

② 취약점 분석·평가 결과 및 보완조치의 이행계획에 관한 사항

③ 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항

❹ 기타 정보보호관리자가 정보보안업무 수행에필요하다고 정한 사항

94. 다음 중 정보보호관리체계 인증 범위 내 필수적으로 포함해야 할 자산이 아닌 것은?

① DMZ 구간 내 정보시스템

② 개발서버, 테스트서버

❸ ERP, DW, GroupWare

④ 관리자 PC, 개발자 PC

95. 정보주체의 동의없이 가명정보를 처리할 수 없는 경우는?

❶ 상업적 1:1 마케팅

② 통계작성

③ 과학적 연구

④ 공익적 기록보존

96. 다음 중 사이버 윤리의 개념과 내용으로 옳지 않은 것은?

① 사이버 공간에서 인간의 도덕적 관계에 관심을 갖는다.

② 사이버 세계 속에 거주하는 모든 인간의 책임과 의무를 규정해 주는 것을 의미한다.

❸ 사이버윤리는 기존의 컴퓨터 윤리의 개념을 포함하지는 않는다.

④ 사이버 상의 일탈상황에 따른 구체적인 행동 요령을 알아보는 실증적인 내용으로 연구되고 있다.

97. 다음 중 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제 25조(침해사고 등의 통지 등)에 따라 지체없이 이용자에게 알려야 할 상황이 아닌 것은?

① 해킹, 컴퓨터바이러스 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하며 발생한 사태가 발생한 때

② 이용자 정보가 유출된 때

③ 사전예고 없이 서비스의 중단 기간이 연속해서 10분 이상인 경우이거나 중단 사고가 발생한 때부터 24기간 이내에 서비스가 2회 이상 중단된 경우로서 그 중단된 기간을 합하여 15분 이상 서비스 중단이 발생한 때

❹ 민·관 합동조사단이 발생한 침해사고의 원인 분석이 끝났을 때

98. 로그관리와 관련되는 정보보안 속성은?

① 기밀성

② 무결성

③ 가용성

❹ 책임추적성

99. 다음 중 정량적 위험분석 방법은?

① 델파이법

❷ 과거 자료 분석법

③ 순위 결정법

④ 시나리오법

100. 다음 중 공공기관이 개인정보 파일을 운용하거나 변경하는 경우 개인정보보호위원회에 등록하여 관리가 필요한 사항이 아닌 것은?

① 개인정보파일의 명칭

② 개인정보파일의 운영 근거 및 목적

❸ 개인정보파일의 작성 일시

④ 개인정보파일에 기록되는 개인정보의 항목