1과목 : 시스템 보안

1. 서버 시스템의 접근통제 관리에 대한 설명으로 틀린 것은?

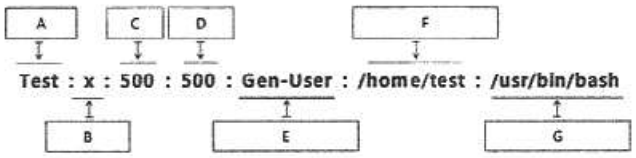
① 윈도우 시스템 이벤트에는 시스템, 어플리케이션, 보안 이벤트가 있으며 감사로그는 제어판-관리도구-로컬보안설정-감사정책에서 각각 설정할 수 있다.

❷ 윈도우 시스템은 도메인 환경에서 사용자 인증을 위하여 레지스트리가 익명의 사용자에 의해 접근할 수 있도록 설정하여야 한다.

③ iptables, tcp wrapper 도구를 사용하면 서버 시스템의 네트워크 접근통제 기능을 설정할 수 있다.

④ Unix 서버 시스템에서 불필요한 파일에 설정된 SUID와 SGID 비트를 제거하여 실행 권한이 없는 프로그램의 비인가된 실행을 차단하여야 한다.

2. 다음은 passwd 파일 구조를 나타내는 그림이다. "G"가 의미하는 것은?



① 홈디렉터리 위치 ❷ 지정된 셸(Shell)

③ 패스워드 ④ 설명

3. 안드로이드 adb를 통해 접속 후 쓰기 가능한 디렉터리는?

① /system/ ② /data/app

❸ /data/local/tmp/ ④ /bin/

4. 다음 문장에서 설명하는 공격 위협은?

> 웹 사이트에 개인정보, 계정정보, 금융정보 등의 중요정보가 노출되거나 에러 발생시 과도한 정보(애플리케이션 정보, DB정보, 웹 서버 구성 정보, 개발과정의 코멘트 등)가 노출될 경우, 공격자들의 2차 공격을 위한 정보로 활용될 수 있다.

① XPath 인젝션 ② 디렉터리 인덱싱

③ 운영체제 명령 실행 ❹ 정보 누출

5. 인증 장치에 대한 설명으로 옳은 것은?

① USB 메모리에 디지털 증명서를 넣어 인증 디바이스로 하는 경우 그 USB 메모리를 접속하는 PC의 MAC 어드레스가 필요하다.

❷ 성인의 홍채는 변화가 없고 홍채 인증에서는 인증 장치에서의 패턴 갱신이 불필요하다.

③ 정전용량 방식의 지문인증 디바이스 LED 조명을 설치한 실내에서는 정상적으로 인증할 수 없게 될 가능성이 높다.

④ 인증에 이용되는 접촉형 IC 카드는 카드 내의 코일의 유도 기전력을 이용하고 있다.

6. 컴퓨터 시스템에 대한 하드닝(Hardening) 활동으로 틀린 것은?

① 사용하지 않는 PDF 소프트웨어를 제거하였다.

❷ 시스템 침해에 대비하여 전체 시스템에 대한 백업을 받아두었다.

③ 운영체제의 감사 기능과 로깅 기능을 활성화하였다.

④ 운영체제 보안 업데이트를 수행하였다.

7. 다음 문장에서 설명하는 기억 장치의 메모리 반입 정책은?

> 입력된 프로그램을 수용할 수 있는 공간 중 가장 큰 공간을 할당한다.

① 최초 적합(First fit) ② 최상 적합(Best fit)

❸ 최악 적합(Worst fit) ④ 다음 적합(Next fit)

8. 악성프로그램에 대한 설명으로 틀린 것은?

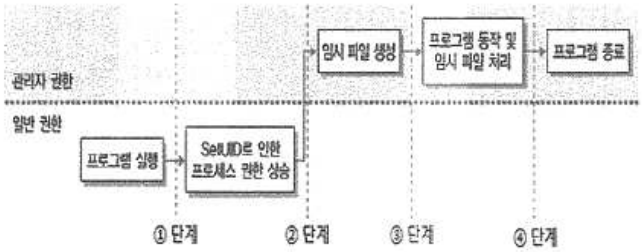
① 바이러스 : 한 시스템에서 다른 시스템으로 전파하기 위해서 사람이나 도구의 도움이 필요한 악성프로그램이다.

② 웜 : 한 시스템에서 다른 시스템으로 전파하는데 있어서 외부의 도움이 필요하지 않은 악성프로그램이다.

❸ 백도어 : 사용자의 동의없이 설치되어 컴퓨터 정보 및 사용자 개인정보를 수집하고 전송하는 악성프로그램이다.

④ 논리 폭탄 : 합법적 프로그램 안에 내장된 코드로서 특정한 조건이 만족되었을 때 작동하는 악성 코드이다.

9. 다음은 SUID 프로그램이 일반 권한에서 관리자 권한으로 상승하여 처리하는 정상적인 과정을 나타내고 있다. 심볼릭 링크를 이용한 레이스 컨디션 공격이 실행되는 단계는?



① 1단계 ② 2단계

❸ 3단계 ④ 4단계

10. 다음은 IDS Snort Rule이다. Rule이 10~11번째 2바이트의 값이 0xFFFF인지를 검사하는 Rule이라 할 때 ㉠~㉢의 올바른 키워드는 무엇인가?

```
alert tcp any any → any any ( flow: to_server;
㉠:"|FF FF|:" ㉡:9; ㉢:2; msg:"Error";, sid:
1000002; )
```

① ㉠ : value, ㉡ : offset, ㉢ : content

② ㉠ : value, ㉡ : content, ㉢ : offset

③ ㉠ : content, ㉡ : depth, ㉢ : offset

❹ ㉠ : content, ㉡ : offset, ㉢ : depth

11. 매크로 바이러스에 대한 설명으로 틀린 것은?

① 플랫폼과 무관하에 실행된다.

② 주로 이메일을 통해 감염된다.

③ 문서 파일의 기능을 악용한다.

❹ EXE 형태의 자동화된 기능을 포함한다.

12. Window에서 파일이 삭제된 직후 일정 시간(기본 15초)안에 동일한 이름의 파일이 생성되는 경우 방금 삭제된 파일의 테이블 레코드를 재사용하는 경우가 있다. 이러한 특징을 갖는 기능은?

❶ 파일시스템 터널링(File system tunneling)
② Shellbags
③ 윈도우 파일 프로텍션
④ 타임스톰핑

13. 리눅스 Capabilities에서 실행 바이너리에 커널 모듈을 올리거나 내릴 수 있는 권한을 할당할 수 있는 Capability는 무엇인가?

① CAP_CHOWN ② CAP_AUDIT_CONTROL
❸ CAP_SYS_MODULE ④ CAP_MAC_ADMIN

14. 다음 중 로그의 성격이 다른 것은?

① 데이터베이스 로그 ② 웹서버 로그
③ 메일서버 로그 ❹ 유닉스 계열의 syslog

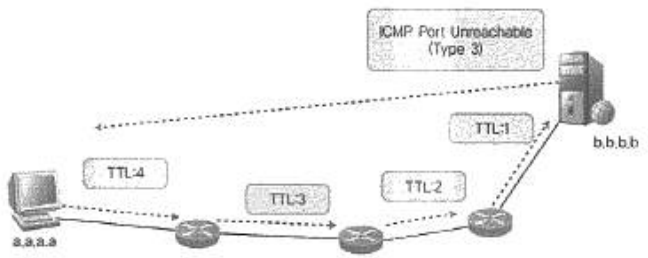
15. 윈도우 운영체제의 레지스트리에 대한 설명으로 틀린 것은?(문제 오류로 확정답안 발표시 3, 4번이 정답처리 되었습니다. 여기서는 3을 누르시면 정답 처리 됩니다.)

① 시스템 구성정보를 저장하는 데이터베이스로 SYSTEM.DAT, USER.DAT 파일을 말한다.
② 레지스트리는 regedit.exe 전용 편집기에 의해서만 편집이 가능하다.
❸ 윈도우 레지스트리 키는 HKEY_CLASS_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG 등이 있다.
④ 레지스트리 백업 및 복구는 shell.exe를 구동하여 행한다.

16. 대부분의 응용 프로그램에서 생성된 파일은 그 응용 프로그램이 생성한 파일임을 인식할 수 있도록 항상 동일한 몇 바이트를 파일 내부의 특정 위치에 가지고 있다. 특정위치의 고정값이 의미하는 것은?

❶ 시그니처(Signature) ② 확장자(Extensions)
③ 메타데이터(Metadata) ④ 레코드(Record)

17. 다음 그림은 a.a.a.a 시스템에서 UDP 패킷을 TTL=1부터 하나씩 늘려가면서 b.b.b.b로 전송하고, TTL=4일 때 b.b.b.b 시스템에 UDP 패킷이 도달하고 ICMP Port Unreachable(Type 3) 패킷이 a.a.a.a 시스템으로 돌아왔다. 무엇을 하기 위한 과정인가?



① ICMP scan ❷ traceroute
③ ping ④ UDP scan

18. 다음 문장에서 설명하는 Window 시스템의 인증 구성 요소는?

- 사용자에게 SID(Security Identifier)를 부여한다. - SID에 기반하여 파일이나 디렉토리에 대한 접근 허용 여부를 결정한다. - 이에 대한 감사 메시지를 생성한다.

① LSA(Local Security Authority)
② LAM(Local Authentication Manager)
③ SAM(Security Account Manager)
❹ SRM(Security Reference Monitor)

19. BIOS에 대한 설명으로 틀린 것은?

① 하드디스키의 구성, 종류, 용량을 확인할 수 있다.
❷ 전원이 공급되지 않으면 정보가 유지되지 않는다.
③ 운영체제와 하드웨어 사이의 입출력을 담당하는 펌웨어이다.
④ BIOS에 저장된 시스템 시간은 포렌식 관점에서 중요하다.

20. 다음 중 인증의 방법이 아닌 것은?

① 당신이 알고 있는 것(Something You Know)
❷ 당신이 위치를 알고 있는 곳(Somewhere You Know)
③ 당신이 가지고 있는 것(Something You Have)
④ 당신 모습 자체(Something You Are)

2과목 : 네트워크 보안

21. 패킷 필터링을 위한 규칙에 대한 설명으로 틀린 것은? (단, 서비스에 사용되는 포트는 기본값이며, Internal은 내부, External은 외부 네트워크를 의미한다.)

번호	From	To	Service	Action
1	Internal	External	80/TCP	Allow
2	Any	169.168.2.25	21/TCP	Allow
3	Internal	169.168.10.10	53/TCP	Allow
4	Any	Any	Any	Duny

① 내부에서 외부로 나가는 웹 서비스에 대해서 허용한다.
② 서버(169.168.2.25)로 FTP 서비스 연결은 어디에서나 가능하나 데이터 전송은 원활하게 이루어지지 않을 수 있다.
③ 필터링 규칙에 명시하지 않은 모든 프로토콜에 대해서는 거부한다.
❹ 서버(169.168.10.10)로 DNS 서비스는 내부에서 이용이 가능하나 Message 정보가 512 바이트보다 클 경우에는 허용하지 않는다.

22. UDP Flooding의 대응 방안으로 틀린 것은?

① 미사용 프로토콜 필터링
❷ 도착지 IP별 임계치 기반 차단
③ 패킷 크기 기반 차단
④ Anycast를 이용한 대응

23. 클라우드 시스템 및 서비스와 관련한 보안 측면의 설명으로 틀린 것은?

① 클라우드 서비스를 구동하기 위해 필수적인 가상화 시스템 내 하이퍼바이저가 취약할 경우 이를 활용하는 여러 개의 가상머신(VM)이 동시에 피해를 입을 가능성을 고려해야 한다.

② 기존 네트워크 보안기술(방화벽, IPS/IDS)로는 가상화 내부 영역에 대한 침입탐지가 어렵다.

③ 사용자의 가상머신들의 상호 연결되어 내부의 가상머신에서 다른 가상 머신으로서 패킷스니핑, 해킹, DDoS 공격, 악성코드전파 등의 공격 경로가 존재한다.

❹ 가상화 기술 중 스토리지 가상화와 네트워크 가상화에 보안 위협이 존재하나 메모리 가상화에는 보안 위협이 존재하지 않는다.

24. 다음 중 원격지 서버의 스니핑 모니터링 프로그램인 sentinal을 이용하여 스니퍼를 탐지하는 예시와 그에 대한 의미로 틀린 것은?

① ./sentinel -a -t 211.47.65.4 : ARP 테스트

② ./sentinel -d -f 1.1.1.1 -t 211.47.65.4 : DNS 테스트

③ ./sentinel-e -t 211.47.65.4 : Etherping 테스트

❹ ./sentinel-t 211.47.65.4 -f 1.1.1.1 -d -a - : 3개의 테스트 중 하나만 테스트

25. 다음 문장의 괄호 안에 들어갈 명령어를 순서대로 나열한 것은?

> 시스코 라우터에서 CPU 평균 사용률을 보기 위해서는 (㉠)의 명령어를 사용하고 라우터 인터페이스 하드웨어 정보를 보기 위해서는 (㉡)을 사용하며, 메모리의 전체 용량, 사용량, 남은 용량 등을 확인하기 위해서는 (㉢) 명령어를 사용한다.

① ㉠ : show process, ㉡ : show controllers, ㉢ : show flash

❷ ㉠ : show process, ㉡ : show controllers, ㉢ : show memory

③ ㉠ : show process, ㉡ : show interface, ㉢ : show flash

④ ㉠ : show process, ㉡ : show interface, ㉢ : show memory

26. 다음 문장에서 설명하는 해커의 분류는?

> - 해킹수행코드가 적용될 수 있을 만한 취약점을 발견할 때까지 여러 번 시도해 시스템 침투해 성공하는 경우도 있으며, 성공된 해킹에 대해 자랑하고 다닌다.
> - 보안상 취약점을 새로 발견하거나 최근 취약점을 주어진 상황에 맞게 바꿀만한 능력이 없다.

① Elite ② Script Kiddie

❸ Developed Kiddie ④ Lamer

27. SNMP 커뮤니티 스트링에 대한 설명으로 틀린 것은?

① 기본적으로 Public, Private으로 설정된 경우가 많다.

② 모든 서버 및 클라이언트에서 동일한 커뮤니티 스트링을 사용해야만 한다.

③ MIB 정보를 주고 받기 위하여 커뮤니티 스트링을 사용한다.

❹ 유닉스 환경에서 커뮤니티 스트링 변경은 일반 권한으로 설정한다.

28. TCP 세션 하이재킹의 공격 순서로 옳은 것은?

> ㉠ 공격자는 스니핑을 하여 세션을 확인하고 적절한 시퀀스 넘버를 획득한다.
> ㉡ 서버는 새로운 시퀀스 넘버를 받아들이며, 다시 세션을 연다.
> ㉢ RST 패킷을 보내 서버쪽 연결만을 끊는다. 서버는 잠시 closed 상태가 되나 클라이언트는 그대로 established 상태로 남는다.
> ㉣ 공격자는 새로 시퀀스 넘버를 생성하여 서버로 보낸다.
> ㉤ 공격자는 정상적인 연결처럼 서버와 시퀀스 넘버를 교환하고 공격자와 서버 모두 established 상태가 된다.

① ㉠→㉡→㉢→㉣→㉤ ② ㉠→㉣→㉢→㉡→㉤

③ ㉠→㉡→㉣→㉢→㉤ ❹ ㉠→㉢→㉣→㉡→㉤

29. 침입탐지 시스템(Intrusion Detection System)의 이상 탐지(anomaly detection) 방법 중 다음 문장에서 설명하는 방법은 무엇인가?

> - 과거의 경험적인 자료를 토대로 처리한다.
> - 행위를 관찰하고 각각의 행위에 대한 프로파일을 생성한다.
> - 프로파일들을 주기적으로 관찰하여 이상을 측정한다.

① 예측 가능한 패턴 생성(Predictive Pattern Generation)

❷ 통계적 접근법(Statictical Approaches)

③ 비정상적인 행위 측정 방법들의 결합(anomaly measures)의 결합

④ 특징 추출(Feature Selection)

30. 다음 중 일반적으로 사용되는 서비스와 해당 서비스의 기본 설정 포트연결이 틀린 것은?

① SSH(Secure Shell) - 22

② SMTP(Simple Mail Transfer Protocol) - 25

❸ FTP(File Transfer Protocol) - 28

④ HTTPS(Hyper-Text Transfer Protocol over Secure layer) - 443

31. 네트워크 도청을 예방하기 위한 대책으로 틀린 것은?

❶ 업무용 무선 AP와 방문자용 AP를 같이 사용한다.

② 무선 AP의 비밀번호는 쉽게 예측하지 못하는 안전한 비밀번호로 설정한다.

③ 업무용 단말기는 방문자용 AP에 접속하지 않도록 조치한다.

④ 중요 정보는 암호화 통신을 이용하여 전송한다.

32. 다익스트라(Dijkstra) 알고리즘을 사용하는 라우팅 프로토콜에 대한 설명으로 틀린 것은?

① 대규모 망에 적합한 알고리즘이다.

❷ 거리벡터 알고리즘이다.
③ OSPF에서 사용된다.
④ 링크상태 알고리즘이다.

33. IPSec을 구축하기 위해 SA를 사용한다. SA 매개변수에 포함되는 내용으로 틀린 것은?
① AH Information
❷ Routing Protocol
③ IPSec Protocol Mode
④ Sequence Number Counter

34. 최근 장시간 악성코드를 잠복시킨 후 일정 시간이 되면 공격을 시도하여 정보 유출 및 내부망 마비 등 피해를 유발시키는 APT 공격이 잦아지고 있다. APT는 무엇의 약자인가?
① Advanced Pain Threat
② Advanced Post Threat
③ Advanced Persistent Target
❹ Advanced Persistent Threat

35. BYOD(Bring Your Own Device)의 보안 기술 중 다음 문장에서 설명하는 모바일 기기 보안 기술은?

> 한 개의 모바일 기기에 동일한 OS의 다중 인스턴스를 제공하는 소프트웨어 기반의 방법으로서 업무용과 개인용의 두 모드를 동시에 사용할 수 있도록 하는 기술

① 클라우드 DaaS(Desktop As A Service)
❷ 모바일 가상화(Hypervisors)
③ 컨테이너화(Containerization)
④ 가상데스크톱 인프라(Virtual Desktop Infrastructure)

36. 다음 문장의 괄호 안에 들어갈 말은?

> Anti Sniffer 도구들의 특징은 로콜 네트워크에서 네트워크 카드의 ( ) 여부를 체크하여 스니퍼가 돌고 있는지를 파악한다.

① Duplex Mode ② MAC
❸ Promiscuouse Mode ④ ARP

37. 다음 공개 해킹도구 중 사용용도가 다른 도구(소프트웨어)는?
① 넷버스(Netbus) ② 스쿨버스(Schoolbus)
③ 백오리피스(Back Orifice) ❹ 키로그23(Keylog23)

38. RFID 보안 기술에서 암호 기술을 사용하는 보호대책은?
① Kill 명령어 기법
② 블로커 태그 기법
❸ XOR(Exclusive OR) 기반 원타임 패드 기법
④ Sleep 명령과 Wake 명령어 기법

39. 포트 스캐너로 유명한 Nmap에서 대상 시스템의 운영체제를 판단할 때 이용하는 기법을 가장 잘 표현하고 있는 것은?
① Telnet 접속시 운영체제가 표시하는 고유한 문자열을 분석하는 배너 그래빙(banner grabbing)
② 운영체제별로 지원하는 서비스 및 열려 있는 포트의 차이
③ 운영체제별로 고유한 식별자 탐지
❹ TCP/IP 프로토콜 표준이 명시하지 않은 패킷 처리 기능의 운영체제별 구현

40. 리눅스 환경에서 트래픽을 분석하기 위해 MRTG(Multi Router Traffic Grapher)를 사용한다. 다음 중 MRTG를 설치 및 수행하는데 필요없는 프로그램은?
① C Compiler ② Perl
③ Gd Library ❹ Libpcap

3과목 : 어플리케이션 보안

41. PGP 서비스와 관련하여 디지털 서명 기능을 위해 사용되는 알고리즘은?(문제 오류로 확정답안 발표시 2, 3번이 정답처리 되었습니다. 여기서는 2번을 누르시면 정답 처리 됩니다.)
① 3DES ❷ DSS/SHA
③ RSA ④ Radix-64

42. OTP에 대한 설명으로 틀린 것은?
❶ 의미있는 숫자로 구성된다.
② 비밀번호 재사용이 불가능하다.
③ 비밀번호 유추가 불가능하다.
④ 사전 공격(Dictionary Attack)에 안전하다.

43. 웹 어플리케이션 취약성 조치방안에 대한 설명으로 틀린 것은?
❶ server side session 방식은 침해 가능성도 있고, 구조상 다양한 취약점에 노출될 수 있으므로 가볍고 안전한 client side의 cookie를 사용한다.
② 모든 인자에 대해 사용 전에 입력값 검증을 수행하도록 구성한다.
③ 파일 다운로드시 위치는 지정된 데이터 저장소를 지정하여 사용하고 데이터 저장소 상위로 이동되지 않도록 구성한다.
④ SSL/TLS와 같은 기술을 이용하여 로그인 트랙잭션 전체를 암호화한다.

44. 다음 문장에서 설명하는 FTP 공격은?

> - FTP서버가 데이터를 전송할 때 목적지가 어디인지 검사하지 않는 설계상의 문제점을 이용한 공격이다.
> - FTP서버의 전송 목적지 주소를 임의로 지정하여 FTP 서버를 경유해 임의의 목적지로 메시지나 자료를 전송하도록 할 수 있다.

❶ FTP Bounce Attack ② Anonymous FTP Attack
③ TFTP Attack ④ FTP Anyconnect Attack

45. 웹 어플리케이션의 취약성을 악용하는 공격 방법 중 웹 페이지에 입력한 문자열이 perl의 system 함수나 PHP의 exec 함수 등에 건네지는 것을 이용해 부정하게 쉘 스크립트를 실행시키는 것은?
① HTTP header injection

❷ OS command injection
③ CSRF(cross-site request forgery)
④ Session hijacking

46. 다크웹(Dark Web)에 대한 설명으로 틀린 것은?

① 공공인터넷을 사용하는 오버레이 네트워크(Overlay Network)이다.
❷ 딥웹(Deep web)은 다크웹의 일부분이다.
③ 토르(TOR)같은 특수한 웹브라우저를 사용해야만 접근할 수 있다.
④ 다크넷에 존해하는 웹사이트를 의미한다.

47. 다음 문장에서 설명하는 것은?

> - 카드사용자, 상점, 지불-게이트웨이간에 안전한 채널을 제공한다.
> - 신용카드번호가 상점에는 알려지지 않고 지불-게이트웨이에 알려진다.
> - 상점에 의한 사기 가능성이 감소한다.
> - 서명 기능이 있어 부인방지 서비스를 제공한다.

① SSL(Secure Socket Layer)
❷ SET(Secure Electronic Transaction)
③ SOC(Security Operation Center)
④ Lattice Security Model

48. DNS 캐시 포이즈닝으로 분류되는 공격은?

① DNS 서버의 소프트웨어 버전 정보를 얻어 DNS 서버의 보안 취약점을 판단한다.
❷ PC가 참조하는 DNS 서버에 잘못된 도메인 관리 정보를 주입하여 위장된 웹서버로 PC 사용자를 유도한다.
③ 공격 대상의 서비스를 방해하기 위해 공격자가 DNS 서버를 이용하여 재귀적인 쿼리를 대량으로 발생시킨다.
④ 내부 정보를 얻기 위해 DNS 서버에 저장된 영역 정보를 함께 전송한다.

49. DDos 공격 형태 중 자원 소진 공격이 아닌 것은?

❶ ICMP Flooding ② SYN Flooding
③ ACK Flooding ④ DNS Query Flooding

50. 다음 표의 소극적·적극적 암호공격 방식의 구분이 옳은 것은?

	소극적 공격	적극적 공격
①	트래픽 분석	삽입공격
②	재생공격	삭제공격
③	메시지 변조	재생공격
④	메시지 변조	삽입공격

❶ ① ② ②
③ ③ ④ ④

51. 다음 문장의 괄호 안에 알맞은 용어는?

> 과거 ( )공격은 불특성 다수를 대상으로 데이터를 암호화하고 이에 대한 몸값을 요구하는 방식이 대부분이었다. 그러나 최근에는 높은 금액을 지불할 수 있는 대규모 엔터프라이즈 환경이 주로 공격 대상이 되고 있고 암호화 뿐만 아니라 데이터 유출 후 인터넷 공개를 미끼로 협박하는 형태의 공격 방식으로 진화되고 있다. 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다.

① 워터링 홀 ② 스팸
③ 스피어피싱 ❹ 랜섬웨어

52. MS SQL 서버의 인증 모드에 대한 설명 중 성격이 다른 하나는?

① SQL Server 기본 인증 모드이다.
② 데이터베이스 관리자가 사용자에게 접근 권한 부여가 가능하다.
③ 윈도우즈 인증 로그온 추적시 SID 값을 사용한다.
❹ 트러스트되지 않은 연결(SQL 연결)을 사용한다.

53. 다음 문장에서 설명하는 보안솔루션은?

> - 한번의 로그인만으로 기업의 각종 시스템이나 인터넷 서비스에 접속하게 해주는 보안 응용 솔루션이다.
> - 각각의 시스템마다 인증 절차를 밟지 않고도 1개의 계정만으로 다양한 시스템에 접근할 수 있어 ID, 비밀번호에 대한 보안 위험 예방과 사용자 편의 증진, 인증 관리비용의 절감 효과가 있다.

① DRM ❷ SSO
③ OTP ④ APT

54. 데이터베이스 보안 방법으로 틀린 것은?

① 데이터베이스 서버를 백업하며 관리한다.
❷ Guest 계정을 사용하여 관리한다.
③ 데이터베이스 쿼리만 웹 서버와 데이터베이스 서버 사이에 통과할 수 있도록 방화벽을 설치한다.
④ 데이터베이스 관리자만 로그인 권한을 부여한다.

55. 다음 문장에서 설명하는 웹 공격의 명칭은?

> 브라우저로 전달되는 데이터에 포함된 악성 스크립트가 개인의 브라우저에서 실행되어 공격이 진행되는 웹 해킹의 일종이다.

❶ XSS(Cross Site Scripting)
② SQL(Structured Query Language) Ingection
③ CSRF(Cross-site request forgery)
④ 쿠키(Cookie) 획득

56. 버퍼오버플로우에 대한 보안 대책이 아닌 것은?

① 운영체제 커널 패치
② 경계 검사를 하는 컴파일러 및 링크 사용

③ 스택내의 코드 실행 금지
❹ 포맷 스트링 검사

57. SSO(Single Sign On)와 관련이 없는 것은?
① Delegation 검사 ② Propagation 방식
③ 웹 기반 쿠키 도메인 SSO ❹ 보안토큰

58. S/MIME의 주요 기능이 아닌 것은?
① 봉인된 데이터(Enveloped data)
② 서명 데이터(Signed data)
③ 순수한 데이터(Clear-signed data)
❹ 비순수 서명과 봉인된 데이터(Unclear Signed and Enveloped data)

59. DNS(Domain Name System)에 대한 설명으로 틀린 것은?
① DNS 서비스는 클라이언트에 해당하는 리졸버(resolver)와 서버에 해당하는 네임서버(name server)로 구성되며, DNS 서비스에 해당되는 포트 번호는 53번이다.
② 주(primary) 네임서버와 보조(secondary) 네임서버는 DNS 서비스 제공에 필요한 정보가 포함된 존(zone) 파일을 기초로 리졸버로부터의 요청을 처리한다.
③ ISP 등이 운영하는 캐시 네임서버가 관리하는 DNS 캐시에 IP 주소, UDP 포트번호, DNS 메시지 ID값이 조작된 정보를 추가함으로써 DNS 캐시 포이즈닝(poisoning) 공격이 가능하다.
❹ DNSSEC 보안 프로토콜은 초기 DNS 서비스가 보안 기능이 포함되지 않았던 문제점을 해결하기 위해 개발되었으며, DNS 데이터의 비밀성, 무결성, 출처 인증 등의 기능을 제공한다.

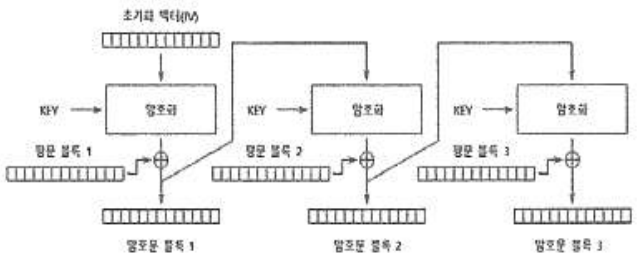
60. 다음 문장에서 설명하는 전자서명 기법은?

> 전자화폐의 일종인 e-cash는 익명성을 제공하기 위해 서명자가 문서의 내용을 보지 않은 상태에서 전자서명을 생성하는 기법을 사용한다.

① 다중서명 ② 그룹서명
❸ 은닉서명 ④ 검증자 지정서명

4과목 : 정보 보안 일반

61. 다음은 특정 블록 암호 운영 모드의 암호화 과정이다. 해당하는 모드는?



① ECB 모드(Electronic Code Book Mode)
② CBC 모드(Cipher Block Chaining Mode)
❸ CFB 모드(Cipher Feedback Mode)
④ OFB 모드(Output Feedback Mode)

62. 접근통제 모델에 대한 각각의 설명 중 옳은 것은?
① 비바(Biba) 모델 : 임의적 접근통제(DAC: Doscretionary Access Control)를 기반으로 하는 상태 머신 모델이다.
② 벨-라파듈라(Bell-Lapadula) 모델 : 객체에 대한 무결성 또는 가용성을 유지하는데 중점을 두고 있으며, 기밀성의 측면에는 대처하지 않는다.
③ 비바(Biba) 모델 : 비밀 채널을 방지하며, 내부 및 외부 객체 일관성을 보호한다.
❹ 클락-윌슨(Clark-Wilson) 모델 : 허가 받은 사용자가 허가 받지 않고 데이터를 수정하는 것을 방지한다.

63. 해시함수의 분류 중 MDC(Modification Detection Cryptography)에 포함되지 않는 알고리즘은?
① MD(Message Digest)
② SHA(Secure Hash Algorithm)
③ LSH(Lightweight Secure Hash)
❹ H-MAC(Hash-MAC)

64. 실시간으로 인증서 유효성을 검증하는 OCSP(Online Certificate Status Protocol)의 서비스가 아닌 것은?
① ORS : 온라인 취소상태 확인서비스
② DPD : 대리인증 경로 발전 서비스
❸ CRL : 인증서 폐지 목록 확인서비스
④ DPV : 대리인증 경로 검증 서비스

65. 접근통제정책 구성요소에 대한 설명으로 틀린 것은?
① 사용자 : 시스템을 사용하는 주체이다.
② 자원 : 사용자가 사용하는 객체이다.
❸ 행위 : 객체가 행하는 논리적 접근통제이다.
④ 관계 : 사용자에게 승인된 허가(읽기, 쓰기, 실행)이다.

66. 다음 중 전자서명인증업무지침에 따라 공인인증기관이 지켜야 할 구체적인 사항이 아닌 것은?
① 공인인증서의 관리에 관한 사항
② 전자서명생성정보의 관리에 관한 사항
③ 공인인증기관 시설의 보호에 관한 사항
❹ 공인인증기관 지정 절차에 관한 사항

67. IAM(Identity Access Management)에 대한 설명으로 틀린 것은?
① 전사적 계정관리, 권한관리의 구현에 필요한 모든 요소들을 일반적으로 IAM이라고 부른다.
② IAM은 계정관리를 담당하는 IM분야와 권한통제를 담당하는 AM으로 나눠진다.
③ 사용자가 시스템을 사용하기 위해 로그인 ID를 발급하는 과정을 프로비저닝이라고 한다.
❹ 사용자가 시스템에 로그인할 때 본인임을 증빙하는 과정을 인가(Authorization)라고 한다.

68. 전자서명을 적용한 예에 해당되지 않는 것은?
① Code Signing ② X.509 Certificate
③ SSL/TLS Protocol ❹ Kerberos Protocol

69. 다음 문장과 같이 처리되는 프로토콜은?

㉠ A는 자신의 비표인 R_A, 자신의 ID, B의 ID가 포함된 메시지를 KDC에 전송한다.
㉡ KDC는 암호화된 메시지를 A에게 전송한다. 이 안에는 A의 비표, B의 ID, A와 B의 세션키 및 B에게 줄 암호화된 티켓이 포함되어 있다. 전체 메시지는 A의 키로 암호화되어 있다.
㉢ A는 B의 티켓을 B에게 보낸다.
㉣ B는 자신의 시도인 R_B를 A와 B의 세션키로 암호화 된 뒤에 A에게 보낸다.
㉤ A는 B의 시도에 대한 응답으로 R_B-1을 A와 B의 세션키로 암호화한 뒤에 B에게 보낸다.

① Diffie-Hellman ❷ Needhan-Schroeder
③ Otway-Rees ④ Kerberos

70. 송신자 A와 수신자 B가 RSA를 이용하여 키를 공유하는 방법에 대한 설명으로 틀린 것은?

① 미국 MIT의 Rivest, Shamir, Adelman이 발표한 공개키 암호화 방식으로 이해와 구현이 쉽고, 검증이 오랫동안 되어서 가장 널리 쓰이고 있다.
② A가 암호화 되지 않은 평문으로 A의 공개키를 B에게 전송한다.
③ B는 공유 비밀키를 생성, A에게서 받은 A의 공개키로 암호화 전송한다.
❹ A는 자신의 공개키로 공유 비밀키를 추출하고 데이터를 암호화 전송한다.

71. 암호문에 대응하는 일부 평문이 가용한 상황에서의 암호 공격 방법은?

① 암호문 단독 공격 ❷ 알려진 평문 공격
③ 선택 평문 공격 ④ 선택 암호문 공격

72. 합성수 n을 사용하는 RSA 전자서명 환경에서 메시지 M에 대해 난수 r에 공개 검증키 e를 가지고 reM mod n값을 서명자에게 전송하는 전자서명 기법은 무엇인가?

❶ 은닉서명 ② 위임서명
③ 부인방지 서명 ④ 이중서명

73. 다음 문장에서 설명하는 위험분석 방법론을 옳게 연결한 것은?

㉠ 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대해 발생 가능한 결과들을 추정하는 방법
㉡ 각각의 위협을 상호 비교하여 최종 위협요인의 우선순위를 도출하는 방법

① ㉠ : 확률 분포법, ㉡ : 순위결정법
② ㉠ : 시나리오법, ㉡ : 델파이법
③ ㉠ : 델파이법, ㉡ : 확률 분포법
❹ ㉠ : 시나리오법, ㉡ : 순위결정법

74. 다음 중 공개키 암호의 필요성으로 틀린 것은?

❶ 무결성 ② 키 관리 문제
③ 인증 ④ 부인방지

75. 다음 중 커버로스(Kerberos)의 구성요소가 아닌 것은?

① KDC(Key Distribution Center)
② TGS(Ticket Granting Service)
③ AS(Authetication Service)
❹ TS(Token Service)

76. 공개키 암호 알고리즘이 아닌 것은?

① RSA(Rivest, Shamir, Adelman)
② ECC(Elliptic, Curvem Cryptosystems)
③ ElGamal
❹ Rijndeal

77. 키를 분배하는 방법이 아닌 것은?

① KDC(Key Distribution Center)
② 공개키 암호시스템
③ Diffie-Hellman 키 분배 알고리즘
❹ Kerberos

78. 해시함수 h와 주어진 입력값 x에 대해 h(x)=h(x′)을 만족하는 x′(≠x)를 찾는 것이 계산적으로 불가능한 것을 의미하는 것은?

① 압축성 ② 일방향성
❸ 두 번째 역상저항성 ④ 충돌 저항성

79. 다음 문장에서 설명하는 것은?

- 메시지 전체를 대칭 암호로 암호화하고 대칭 암호키만을 공개키로 암호화한다.
- 대칭 암호키를 메시지로 간주하고 이것을 공개키로 암호화한 것이다.

① 타원 곡선 암호 시스템 ❷ 하이브리드 암호 시스템
③ 세션 키(의사난수 생성기) ④ 이중 암호 시스템

80. 메시지 출처 인증(Message Origin Authentication)에 활용되는 암호 기술 중 대칭키 방식에 해당하는 것은?

① 전자서명 ② 해시함수
③ 이중서명 ❹ 메시지 인증 코드

5과목 : 정보보안 관리 및 법규

81. 주요 직무자 지정 및 관리시 고려해야 할 사항으로 틀린 것은?

① 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하여야 한다.
② 주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고 그 목록을 최신으로 관리하여야 한다.
③ 업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하여야 한다.
❹ 파견근로자, 시간제근로자 등을 제외한 임직원 중 업무상 개인정보를 취급하는 자를 개인정보취급자로 지정하고 목록을 관리하여야 한다.

82. 정보통신기반보호법에서 정하는 주요 정보통신기반시설 보호계획의 수립 등에 포함되지 않는 사항은?

① 주요정보통신기반시설의 취약점 분석·평가에 관한 사항
❷ 정보보호 책임자 지정에 관한 사항
③ 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항
④ 주요정보통신기반시설의 보호에 관하여 필요한 사항

83. 다음 내용에 따른 국내대리인의 필수 공개 정보로 잘못된 것은?

> 국내대리인을 지정해야 하는 국외사업자는 개인정보 처리방침에 국내대리인의 정보를 공개하여야 한다.

① 법인명, 대표명 ② 주소
❸ 고객센터 연락처 ④ 이메일

84. 정보통신기반 보호법에 의거하여 주요정보통신기반시설을 지정할 때 주요 고려사항으로 틀린 것은?

① 다른 정보통신기반시설과의 상호연계성
② 업무의 정보통신기반시설에 대한 의존도
❸ 업무의 개인정보 보유 건수
④ 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

85. 정보통신망 이용 촉진 및 정보 보호 등에 관한 법률에서 정의하는 용어에 대한 설명으로 틀린 것은?

> ㉠ "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 암호화되어 저장된 문서형식의 자료로서 표준화된 것을 말한다.
> ㉡ "개인정보"란 생존 및 사망한 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
> ㉢ "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.
> ㉣ "게시판"이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램이나 기술적 장치를 말한다.

❶ ㉠, ㉡ ② ㉡, ㉢
③ ㉢, ㉣ ④ ㉡, ㉣

86. 조직의 정보보호 교육 대상자에 해당되지 않는 사람은?

❶ 조직의 중요한 고객
② 최고 경영자
③ 조직의 신입직원
④ 조직이 제공하는 정보를 이용하는 일부 외부 이용자 그룹

87. 다음 문장은 위험분석에 관한 설명이다. 괄호 안에 들어갈 내용은?

> - 자산의 (㉠)을 식별하고 존재하는 (㉡)을 분석하여 이들이 (㉢) 및 (㉣) 이 미칠 수 있는 영향을 파악하여 보안위험의 내용과 정도를 결정하는 과정이다.
> - (㉡)은 잠재적 (㉣)이 현실화되어 나타날 손실액과 이러한 손실이 발생할 확률의 곱(잠재적 손실액)이다.

① ㉠ : 위협, ㉡ : 위험, ㉢ : 발생가능성, ㉣ : 취약성
❷ ㉠ : 취약성, ㉡ : 위험, ㉢ : 발생가능성, ㉣ : 위협
③ ㉠ : 위험, ㉡ : 취약성, ㉢ : 위협, ㉣ : 발생가능성
④ ㉠ : 발생가능성, ㉡ : 위협, ㉢ : 취약성, ㉣ : 위험

88. 다음 문장에서 설명하는 위험평가 방법은?

> - 모든 시스템에 기본적인 보호수준을 정하고 이를 달성하기 위한 보호대책을 선택하여 적용할 수 있다.
> - 시간과 비용을 많이 들이지 않고 기본적인 보호대책을 선택하여 적용할 수 있다.
> - 과보호 또는 부족한 보호대책이 적용될 가능성이 존재한다.

❶ 기준선 접근법 ② 비정형 접근법
③ 상세 위험분석 ④ 복합 접근방법

89. 정보보호관리체계 구축시 발생 가능한 문제점과 해결방안에 대한 설명으로 틀린 것은?

① 관련 부서와의 조정이 곤란하다.
② 직원들이 일상 업무에 바빠 관리체계 구축사업에 시간을 내기 어렵다.
❸ 직원들은 자신의 책임을 피하기 위해 문제점이 발생하면 즉시 상사에게 보고하는 경향을 보인다.
④ 관리체계 구축에는 경영자의 리더십이 필수적으로 요구된다.

90. 다음 문장에서 설명하는 시스템 보안평가 기준은?

> - 보안제품 개발자에게 제공되어야 할 서비스에 대한 지침을 제시한다.
> - 구매자에게는 필요한 서비스 지침을 제공한다.
> - 기능성과 보증성에 대한 요구사항으로 구성된다.
> - 기능은 비밀성, 무결성, 가용성, 책임성 4가지로 분류된다.
> - 보증 평가등급은 7개 등급으로 분류된다.

① TCSEC ② ITSEC
❸ CTCPEC ④ CC

91. 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업의 내부관리계획의 내용에 포함되지 않아도 될 사항은?

① 개인정보 보호책임자의 지정에 관한 사항
② 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
③ 개인정보의 암호화 조치에 관한 사항
❹ 개인정보 처리업무를 위탁하는 경우 수탁자에게 대한 관리 및 감독에 관한 사항

92. 비즈니스 연속성에서 고장과 관계된 수용될 수 없는 결과를 피하기 위해 재해 후에 비즈니스가 복귀되어야 하는 최단 시간 및 서비스 수준을 의미하는 것은?
❶ RTO ② WRT
③ RP ④ MTD

93. 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단인 정보보호의 목적으로 틀린 것은?
① 기밀성 서비스 제공 ② 무결성 서비스 제공
③ 가용성 서비스 제공 ❹ 추적성 서비스 제공

94. 위험분석의 구성요소가 아닌 것은?
❶ 비용 ② 취약점
③ 위협 ④ 자산

95. 정보보호의 예방대책을 관리적 예방대책과 기술적 예방대책으로 나누어 볼 때 관리적 예방대책에 속하는 것은?
① 안전한 패스워드를 강제로 사용
② 침입차단 시스템을 이용하여 접속을 통제
③ 가상 사설망을 이용하여 안전한 통신 환경 구현
❹ 문서처리 순서의 표준화

96. 건물 관리 및 화재 등 사고관리를 위해 건물입구를 비추도록 설치된 영상정보처리기기에서 사용할 수 있는 기능으로 옳은 것은?
① 사고를 확인하기 위한 카메라 줌인, 줌아웃
② 범인을 추적하기 위한 카메라 이동
③ 사고 내용을 확인하기 위한 음성 녹음
❹ 사고 내용을 전달하기 위한 영상 전송

97. 다음 문장의 정보보호대책 선정시 영향을 주는 제약사항으로 옳은 것은?

> 많은 기술적 대책들이 직원의 능동적인 지원에 의존하기 때문에 이러한 제약사항을 고려하여야 한다. 만약 직원이 대책에 대한 필요성을 이해하지 못하고 문화적으로 수용할 만하다는 것을 알지 못한다면 대책은 시간이 지날수록 비효율적인 것이 된다.

① 환경적 제약 ② 법적 제약
③ 시간적 제약 ❹ 사회적 제약

98. 개인정보보호 법령에 따른 영상정보처리기기의 설치·운영과 관련하여 정보주체가 쉽게 인식할 수 있도록 설치하는 안내판의 기재 항목이 아닌 것은?
① 설치 목적 ❷ 영상정보 보관기관
③ 설치 장소 ④ 촬영 범위

99. 개인정보보호법상 개인정보 유출사고의 통지, 신고 의무에 대한 설명으로 틀린 것은?
① 정보통신서비스 제공자등은 개인정보의 유출등의 사실을 안 때에는 지체 없이 유출 등의 내역을 해당 이용자에게 알려야 한다.
❷ 정보통신서비스 제공자등은 1천명 이상의 정보주체에 관한 개인정보의 유출등의 사실을 안 때에는 지체 없이 유출 등의 내역을 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.
③ 정보통신서비스 제공자등은 정당한 사유 없이 유출 등의 사실을 안 때에는 24시간을 경과하여 통지·신고해서는 아니 된다.
④ 정보통신서비스 제공자 등은 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 유출 등의 내역을 자신의 인터넷 홈페이지에 30일 이상 게시하여야 한다.

100. 정보보호 거버넌스 국제 표준으로 옳은 것은?
① ISO27001 ② BS10012
❸ ISO27014 ④ ISO27018

1	2	3	4	5	6	7	8	9	10
②	②	③	④	②	②	③	③	③	④
11	12	13	14	15	16	17	18	19	20
④	①	③	④	③	①	②	④	②	②
21	22	23	24	25	26	27	28	29	30
④	②	④	④	②	③	④	④	②	③
31	32	33	34	35	36	37	38	39	40
①	②	②	④	②	③	④	③	④	④
41	42	43	44	45	46	47	48	49	50
②	①	①	①	②	②	②	②	①	①
51	52	53	54	55	56	57	58	59	60
④	④	②	②	①	④	④	④	④	③
61	62	63	64	65	66	67	68	69	70
③	④	④	③	③	④	④	④	②	④
71	72	73	74	75	76	77	78	79	80
②	①	④	①	④	④	④	③	②	④
81	82	83	84	85	86	87	88	89	90
④	②	③	③	①	①	②	①	③	③
91	92	93	94	95	96	97	98	99	100
④	①	④	①	④	④	④	②	②	③