[정보시스템 구축관리>시스템 보안 구축>시스템 보안 설계]

[기출 예상 문제]

1. 다음 중 DoS 공격 유형이 아닌 것은?

① 플러드(Ping Flood)
② 스머프(Smurf) 공격
③ PoD(Ping of Death)
④ Handshaking

[기출 예상 문제]

2. 고성능 컴퓨터를 이용해 초당 엄청난 양의 접속신호를 한 사이트에 집중적으로 보냄으로써 상대 컴퓨터의 서버를 접속 불능 상태로 만들어 버리는 해킹 수법은?

① Smurfing ② Snooping
③ Sniffing ④ Swapping

[기출 예상 문제]

3. 정보 시스템의 데이터나 자원을 정당한 사용자가 적절한 대기 시간 내에 사용하는 것을 방해하는 행위. 주로 시스템에 과도한 부하를 일으켜 정보 시스템의 사용을 방해하는 공격 방식은?

① Ping of Death ② DoS
③ SYN Flooding ④ LAND 공격

[기출 예상 문제]

4. 아래 설명에서 악성 코드에 감염된 컴퓨터를 뜻하는 용어로 가장 적절한 것은?

감염된 대량의 숙주 컴퓨터를 이용해 특정 시스템을 마비시키는 사이버 공격. 공격자는 다양한 방법으로 일반 컴퓨터를 감염시켜 공격 대상의 시스템에 다량의 패킷이 무차별로 보내지도록 조정한다. 이로 인해 공격 대상 시스템은 성능이 저하되거나 마비된다.

① 트로이 목마 ② 봇넷(BOTNET)
③ 좀비 컴퓨터 ④ C&C 서버

[기출 예상 문제]

5. 다음은 무엇에 대한 설명인가?

독일 지멘스사의 원격 감시 제어 시스템(SCADA)의 제어 소프트웨어에 침투하여 시스템을 마비하게 하는 바이러스. 원자력 발전소와 송·배전망, 화학 공장, 송유·가스관과 같은 산업 기반 시설에 사용되는 제어 시스템에 침투하여 오동작을 유도하는 명령 코드를 입력해서 시스템을 마비하게 하는 악성 코드이다.

① 스턱스넷(stuxnet)
② 무작위 대입 공격(brute force attack)
③ 랜섬웨어(ransomware)
④ 트랩도어(trap door)

[정보시스템 구축관리>시스템 보안 구축>시스템 보안 설계]

[기출 예상 문제]

6. 다음은 무엇에 대한 설명인가?

다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격을 말한다.
공격 방법에는 내부자에게 악성코드가 포함된 이메일을 오랜 기간 동안 꾸준히 발송해 한 번이라도 클릭되길 기다리는 형태, 스턱스넷(Stuxnet)과 같이 악성코드가 담긴 이동식 디스크(USB) 등으로 전파하는 형태, 악성코드에 감염된 P2P 사이트에 접속하면 악성코드에 감염되는 형태 등이 있다.

① APT
② Zero Day Attack
③ Worm Virus
④ Dummy Hub

[기출 예상 문제]

7. '컴퓨터에 근거지를 둔 지렁이와 같은 기생충'이란 의미를 가진다. 컴퓨터 바이러스와 달리 다른 프로그램을 감염시키지 않고 자기 자신을 복제하면서 통신망 등을 통해서 널리 퍼지는 바이러스는 무엇인가?

① TearDrop 공격
② DDos(Distributed Denial of Service attack)
③ 스미싱(SMishing)
④ 웜 바이러스(Worm virus)

[기출 예상 문제]

8. 다음은 무엇에 대한 설명인가?

네트워크상에서 남의 정보를 염탐하여 불법으로 가로채는 행위

① 스누핑(Snooping)
② 스니핑(Sniffing)
③ 스푸핑(Spoofing)
④ 스머핑(Smurfing)

[기출 예상 문제]

9. 보안 서버에 대한 설명으로 가장 거리가 먼 것은?

① SSL 인증서를 적용해야하는 웹사이트는 개인정보를 취급하는 일부 사이트가 해당된다.
② 보안 서버는 웹서버에 인증서나 암호화 소프트웨어를 설치하여 암호 통신이 가능하도록 하는 것이다.
③ 웹서버에 보안서버 인증 솔루션이 설치되어 있으면 정보를 안전하게 전송할 수 있다.
④ 개인정보를 암호화 하여 정보를 송수신하면 제 3자가 탈취하더라도 암호화되어 있어 확인이 불가능하다.

[정보시스템 구축관리>시스템 보안 구축>시스템 보안 설계]

[기출 예상 문제]
10. 다음은 무엇에 대한 설명인가?

(ㄱ) 로그인하려는 사용자가 누구인지 계정정보를 입력받아 시스템에 접속 권한을 가진 사용자인가를 검증하는 단계
(ㄴ) 식별을 완료한 뒤 현재 접속하려는 사용자가 입력한 계정의소유자가 맞는가를 비밀번호와 같은 검증수단을 이용해 확인하는 것

① (ㄱ) 인증 (ㄴ) 식별
② (ㄱ) 인증 (ㄴ) 검증
③ (ㄱ) 식별 (ㄴ) 인증
④ (ㄱ) 식별 (ㄴ) 검증

[기출 예상 문제]
11. 다음 중 인증기술의 4가지 유형이 아닌 것은?

① 지식기반 인증 ② 사람기반 인증
③ 소유기반 인증 ④ 행위기반 인증

[기출 예상 문제]
12. 웹 사이트에 주민 등록 번호 대신 이용할 수 있는 사이버 신원 확인 번호로서 인터넷상에서 주민 등록 번호가 유출되어 도용되는 부작용을 막기 위해 만든 서비스는 무엇인가?

① Authentication ② OTP
③ QR code ④ i-PIN

[기출 예상 문제]
13. 다음 중 서버보안에 의한 접근 제어에 포함되지 않는 것은?

① 인증 ② 인가
③ 감사 ④ 검증

[기출 예상 문제]
14. 다음 설명 중 (ㄱ)~(ㄷ)에 들어갈 용어로 가장 적절한 것은?

(ㄱ)은/는 시스템에 로그온할 수 있는 사람을 결정하고, (ㄴ)은/는 인증된 사람이 생기는 것을 결정하며, (ㄷ)은/는 해당 사용자가 무엇을 하였는지를 밝힌다.

① (ㄱ) 책임 (ㄴ) 인가 (ㄷ) 식별 및 인증
② (ㄱ) 인가 (ㄴ) 식별 및 인증 (ㄷ) 책임
③ (ㄱ) 식별 및 인증 (ㄴ) 인가 (ㄷ) 책임
④ (ㄱ) 책임 (ㄴ) 식별 및 인증 (ㄷ) 인가

[기출 예상 문제]
15. 다음 중 정보보안의 핵심 3원칙이 아닌 것은?

① 제한성 ② 기밀성
③ 가용성 ④ 무결성

[정보시스템 구축관리>시스템 보안 구축>시스템 보안 설계]

[기출 예상 문제]

16. 다음 중 보안 아키텍처에 대한 설명으로 가장 거리가 먼 것은?

① 보안정책 최상위 레벨에서 보안 목표, 보안 조직, 관계 법령 등의 원칙이 정의되어야 한다.
② 세부적으로 관리적, 논리적, 기술적인 보안 지침을 포함한다.
③ 보안 아키텍처는 보안 수준에 변화가 생겨도 기본 보안 아키텍처의 수정 없이 지원할 수 있어야 한다.
④ 물리적 보안의 관리 업무 주체는 사람이다.

[기출 예상 문제]

17. 보안 수립 및 구축 절차로 가장 적절한 것은?

ㄱ. 보안 아키텍처 현황 분석
ㄴ. 보안 현황 파악
ㄷ. 목표 수립 및 과제 정의
ㄹ. 현행 보안 아키텍처 정의

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

[기출 예상 문제]

18. 다음은 무엇에 대한 설명인가?

기업 업무의 연속성을 위한 네트워크, 시스템 등의 주요 인프라에 대한 위협 요인을 사전에 분석하여 예방하고 위협 요인 발생시 적절히 대응하기 위한 정책, 프로세스, 기술적 요인 등을 의미한다.

① 보안 인증 ② 보안 프레임워크
③ 보안 아키텍처 ④ 보안 솔루션

[기출 예상 문제]

19. 보안 프레임워크에 영향을 주는 요소가 아닌 것은?

① Compliance
② Security Threat
③ Business Opportunity
④ Vulnerability

[기출 예상 문제]

20. ISO/IEC 27001 보안 통제 항목이 아닌 것은?

① 보안 정책 ② 통신 및 운영 관리
③ 접근 제어 ④ 보호 과정

[정보시스템 구축관리>시스템 보안 구축>시스템 보안 구현]

[기출 예상 문제]
1. 시스템에서의 로그파일 분석과 관리에 대한 설명으로 가장 거리가 먼 것은?

① 시스템에 이상 징후가 발생했을 때, 시스템 관리자가 가장 마지막으로 확인해 보는 것이 로그파일이다.
② 해킹 흔적 등을 확인하기 위해서 서버관리자는 로그 파일을 분석한다.
③ 어디서, 누가, 어떻게 들어와서 어떤 작업을 했는지를 확인하려 할 때 로그파일을 분석한다.
④ 관리해야 할 로그파일의 수와 로그파일이 어떤 경로로 남겨지는지에 대해서 정확히 알고있어야 한다.

[기출 예상 문제]
2. 다음 설명의 빈 칸에 들어갈 용어는?

리눅스의 기본적인 로그들은 ( )에 의해서 제어가 되며, ( )의 설정 파일인 /etc/syslog.conf 파일을 수정함으로써 이 파일들의 저장위치와 저장파일명을 변경할 수도 있다.

① xferlog　　② syslogd
③ boot　　④ kernel

[기출 예상 문제]
3. Windows 시스템에서 기본 이벤트 로그가 저장되는 경로로 가장 적절한 것은?

① C:₩Windows₩System32₩winevt₩Logs
② C:₩Users₩user₩Roaming₩Intel₩Wireless
③ C:₩Windows₩debug
④ C:₩Windows₩Logs₩NetSetup

[기출 예상 문제]
4. 다음 중 Windows 이벤트뷰어 로그의 종류가 아닌 것은?

① 시스템 로그　　② 보안 로그
③ 운영체제 로그　　④ 응용 프로그램 로그

[기출 예상 문제]
5. 다음은 무엇에 대한 설명인가?

응용 프로그램이나 프로그램에서 기록한 이벤트가 포함된다. 예를 들어 데이터베이스 프로그램에서 응용 프로그램 로그에 파일 오류를 기록할 수 있다. 로그할 이벤트는 응용프로그램 개발자가 결정한다.

① 보안 로그　　② 응용 프로그램 로그
③ 임시 로그　　④ 개발 로그

[정보시스템 구축관리>시스템 보안 구축>시스템 보안 구현]

[기출 예상 문제]
6. 접근 통제, 침입 차단 및 탐지, DDoS 탐지 등을 수행하여 외부로부터 불법적인 침입을 막는 기술이나 시스템을 의미하는 용어로 가장 적절한 것은?

① 방화벽 ② 보안 솔루션
③ 로컬 보안 정책 ④ 보안 취약점

[기출 예상 문제]
7. 다음은 무엇에 대한 설명인가

정보시스템의 보안을 위협하는 침입행위가 발생할 경우 이를 탐지, 적극 대응하기 위한 시스템이다. 이상 탐지는 비정상적인 행위나 자원의 사용을 탐지하고 오용 탐지는 미리 입력해 둔 공격 패턴이 있는지를 탐지한다.

① IDS ② DMZ ③ IPS ④ UTM

[기출 예상 문제]
8. 기업 내부자의 고의나 실수로 인한 외부로의 정보 유출을 방지하는 솔루션은 무엇인가?

① DLP ② NAC ③ VPN ④ ESM

[기출 예상 문제]
9. 사전에 인가하지 않은 누리꾼이나 보안 체계를 갖추지 않은 정보기기의 통신망(네트워크) 접속을 적절히 조절하는 일 또는 솔루션이다. 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공하는 보안 솔루션은 무엇인가?

① VPN ② UTM ③ NAC ④ IPS

[기출 예상 문제]
10. 웹/애플리케이션/서버 보안장비는 알려진 유형의 웹 해킹 공격을 탐지하고 방어하며 각종 개인정보의 유출을 탐지 및 차단할 수 있어야한다. 웹/애플리케이션/서버 보안장비 중 운용서버의 정상적인 프로그램이나 데이터를 파괴하도록 개발된 악성 프로그램을 치료하는 프로그램을 의미하는 용어로 가장 적절한 것은?

① 웹방화벽 ② 쉘 모니터
③ 서버 백신 ④ Anti-DDoS

[정보시스템 구축관리>시스템 보안 구축>시스템 보안 구현]

[기출 예상 문제]

11. 취약점 분석 및 평가 프로세스 절차를 올바르게 나열한 것은?

ㄱ. 진단결과를 분석 및 평가한다.
ㄴ. 발견된 취약점에 대한 방안을 수립한다.
ㄷ. 취약점 진단 대상을 선정하고 정보를 수집한다.
ㄹ. 취약점 분석 및 평가 계획을 수립한다.
ㅁ. 체크리스트 이용 취약점 진단을 수행한다.
ㅂ. 진단 영역별 진단 결과에 대한 보고서를 작성한다.

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

[기출 예상 문제]

12. 취약점 분석에 대한 설명으로 가장 거리가 먼 것은?

① 정보보안 시스템의 현황 및 용도를 파악하고 취약점 진단 대상을 선정한다.
② 취약점 진단은 기술적 진단만 점검한다.
③ 각 취약점의 점검항목에 대해 취약점 점수를 지정하고 결과 값을 산출한다.
④ 취약점 분석 대상을 유형별로 그룹화하여 대상 목록을 작성하고, 첫번째로 식별된 목록에 대하여 중요도를 산정한다.

[기출 예상 문제]

13. 취약점 진단을 기술적, 관리적, 물리적 영역으로 구분하였을 때 각 점검 요량에 대한 설명으로 가장 거리가 먼 것은?

① 기술적 점검 요령은 모의 해킹을 통해 확인한다.
② 물리적 점검 요령은 통제 구역을 실사하여 확인한다.
③ 관리적 점검 요령은 수동 점검을 통해 확인한다.
④ 관리적 점검 요령은 관련 문서를 통해 확인한다.

[정답] [정보시스템 구축관리>시스템 보안 구축]

1. 시스템 보안 설계

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
4	1	2	3	1	1	4	1	1	3	2	4	4	3	1	2	3	2	4	4

2. 시스템 보안 구현

1	2	3	4	5	6	7	8	9	10	11	12	13							
1	2	1	3	2	2	1	1	3	3	4	2	3							

[정답 및 해설] [정보시스템 구축관리>시스템 보안 구축>시스템 보안 설계]

시스템 보안 설계 1. ④

DoS 공격 유형
- 플러드(Ping Flood) - UDP 플러드
- PoD(Ping of Death) - 스머프(Smurf) 공격
- SYN 플러드

시스템 보안 설계 2. ①

스머핑(Smurfing)에 대한 설명이다.

시스템 보안 설계 3. ②

DoS(서비스 거부 공격, Denial Of Service)에 대한 설명이다.

시스템 보안 설계 4. ③

좀비 컴퓨터는 악성코드에 감염된 컴퓨터를 뜻한다. C&C서버의 제어를 받아 주로 DDoS 공격 등에 이용된다.

시스템 보안 설계 5. ①

스턱스넷(stuxnet)에 대한 설명이다.

시스템 보안 설계 6. ①

APT(Advanced Persistent Threat, 지능형 지속 공격)에 대한 설명이다.

시스템 보안 설계 7. ④

웜 바이러스(Worm Virus)에 대한 설명이다.

시스템 보안 설계 8. ①

스누핑(Snooping)에 대한 설명이다.

시스템 보안 설계 9. ①

① SSL 인증서를 적용해야하는 웹사이트로는 개인정보를 취급하는 모든 사이트가 해당된다.

시스템 보안 설계 10. ③

(ㄱ) 식별(Identification), (ㄴ) 인증(Authentication)에 대한 설명이다.

시스템 보안 설계 11. ②

인증기술의 4가지 유형
- 지식기반 인증 - 소유기반 인증
- 생체기반 인증 - 행위기반 인증

시스템 보안 설계 12. ④

i-PIN(internet personal identification Number, 인터넷 개인 식별 번호)에 대한 설명이다.

[정답 및 해설] [정보시스템 구축관리>시스템 보안 구축>시스템 보안 설계]

시스템 보안 설계 13. ④

서버보안에 의한 접근 제어에는 인증, 인가, 감사가 포함된다.

시스템 보안 설계 14. ③

- 식별 및 인증: 시스템에 로그온할 수 있는 사람을 결정
- 인가: 인증된 사람이 생기는 것을 결정
- 책임: 해당 사용자가 무엇을 하였는지를 밝힘

시스템 보안 설계 15. ①

정보보안의 3원칙
- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)

시스템 보안 설계 16. ②

② 세부적으로 관리적, 물리적, 기술적인 보안 지침을 포함한다.

시스템 보안 설계 17. ③

보안수립 및 구축 절차
: 보안 현황 파악→현행 보안 아키텍처 정의→보안 아키텍처 현황 분석→목표 수립 및 과제 정의

시스템 보안 설계 18. ②

보안 프레임워크에 대한 설명이다.

시스템 보안 설계 19. ④

보안 프레임워크에 영향을 주는 요소는 Compliance, Security Threat, Business Requirements, Business Opportunity 가 해당한다.

시스템 보안 설계 20. ④

* ISO 27001의 보안 통제 항목(평가 항목)
- 11개 영역, 133개 항목
1) 보안 정책
2) 정보 보안 조직
3) 자산 분류 및 통제: 조직의 자산 보호를 위한 적절한 보호 프로세스
4) 인력 자원 보안
5) 물리적 및 환경적 보안
6) 통신 및 운영 관리
7) 접근 제어
8) 정보 시스템 구축과 개발 및 운영
9) 정보 보안 사고의 관리
10) 사업의 연속성: 중요 업무를 보호하기 위한 프로세스
11) 준거성: 법률, 법규, 규정 등 불일치를 회피하기 위한 대응책

[정답 및 해설] [정보시스템 구축관리>시스템 보안 구축>시스템 보안 구현]

시스템 보안 구현 1. ①

① 시스템에 이상 징후가 발생 했을 때, 시스템 관리자가 가장 먼저 확인해 보는 것이 로그파일이다.

시스템 보안 구현 2. ②

syslogd에 대한 설명이다.

시스템 보안 구현 3. ①

Windows 기본 이벤트 로그 경로
: C:₩Windows₩System32₩winevt₩Logs

시스템 보안 구현 4. ③

Windows 이벤트뷰어 로그 종류
- 응용 프로그램 로그
- 보안 로그
- 시스템 로그

시스템 보안 구현 5. ②

응용 프로그램 로그에 대한 설명이다.

시스템 보안 구현 6. ②

보안 솔루션에 대한 설명이다.

시스템 보안 구현 7. ①

IDS(Intrusion Detection System, 침입 탐지 시스템)에 대한 설명이다.

시스템 보안 구현 8. ①

DLP(Data Loss Prevention, 데이터 유출 방지)에 대한 설명이다.

시스템 보안 구현 9. ③

NAC (Network Access Control, 네트워크 접근 제어)에 대한 설명이다.

시스템 보안 구현 10. ③

서버 백신에 대한 설명이다.

시스템 보안 구현 11. ④

취약점 분석 및 평가프로세스:
1. 취약점 분석 및 평가 계획을 수립한다.
2. 취약점 진단 대상을 선정하고 정보를 수집한다.
3. 체크리스트 이용 취약점 진단을 수행한다.
4. 진단결과를 분석 및 평가한다.
5. 발견된 취약점에 대한 방안을 수립한다.
6. 진단 영역별 진단 결과에 대한 보고서를 작성한다.

[정답 및 해설] [정보시스템 구축관리>시스템 보안 구축>시스템 보안 구현]

시스템 보안 구현 12. ②

② 취약점 진단은 기술적 진단 외에 관리적, 물리적 영역을 구분하여 점검한다.

시스템 보안 구현 13. ②

③ 수동 점검은 기술적 점검 요령에 포함된다.
- 기술적 점검 요령: 점검 도구(툴), 수동 점검, 모의 해킹 등을 통해 확인한다.
- 관리적 점검 요령: 정보 보호 정책·지침 등 관련 문서 확인과 정보 보호 담당자, 시스템 관리자, 사용자 등과의 면담으로 확인한다.
- 물리적 점검 요령: 전산실, 현관, 발전실 등의 통제 구역을 실사하여 확인한다.