

1. 다음 지문에서 설명하는 기법은 무엇인가?

가. 그림 또는 문장 속에 비밀자료를 숨겨서 전달하는 방법
나. 그림의 픽셀 중 일부를 저장하고 싶은 데이터로 대체하여 저장하는 방법
다. 원본 그림과 대체된 그림을 육안으로 보서는 구별할 수 없다.

- ① 전자서명(Digital Signature)
- ② 인증서(Certificate)
- ③ 스테가노그래피(Steganography)
- ④ 제로데이 공격(Zero-Day Attack)

2. Diffie-Hellman 알고리즘은 비밀키를 공유하는 과정에서 특정 공격에 취약할 가능성이 존재한다. 이러한 취약점을 이용하여 공격하는 방법은 무엇인가?

- ① DDoS(Distributed Denial of Service) 공격
- ② 중간자 개입(Man-In-The-Middle) 공격
- ③ 세션 하이재킹(Session Hijacking) 공격
- ④ 강제지연(Forced-Delay) 공격

3. 다음 중 암호화 키와 복호화 키가 서로 다른 암호화 알고리즘은 무엇인가?

- ① DES 알고리즘
- ② IDEA 알고리즘
- ③ AES 알고리즘
- ④ RSA 알고리즘

4. AES 알고리즘에 관한 설명 중 옳지 않은 것은 무엇인가?

- ① AES는 128, 192, 256비트 키를 사용하고 키 크기에 따라 각각 10, 12, 14 라운드를 갖는다.
- ② 마스터 키의 크기가 달라도 라운드 키는 모두 128비트이다.
- ③ AES는 바이트 기반 암호이다.
- ④ 안전성을 보장하기 위하여 AES는 모든 라운드에 대치, 치환, 뒤섞음, 키덧셈의 네 종류 변환을 사용한다.

5. 다음 중 공개키 암호 시스템의 장점이 아닌 것은 무엇인가?

- ① 키의 분배가 용이하다.
- ② 사용자의 증가에 따라 관리할 키의 개수가 상대적으로 적다.
- ③ 암호화 및 복호화가 빠르다.
- ④ 키 변화의 빈도가 적다.

6. 다음 중 전자서명(Digital Signature)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

- ① 인증(Authentication) 기능을 제공하며 개인키로 암호화된 메시지를 제3자의 공개키로 복호화 할 경우 메시지를 읽을 수 없다.
- ② 비밀성(Confidentiality) 기능을 제공하며 대칭키 암호화 알고리즘을 이용하여 전자서명을 생성할 수 있다.

- ③ 무결성(Integrity) 기능을 제공하며 메시지의 부분 또는 전체를 바꿀 경우 복호화된 메시지를 통해 변경 여부를 확인할 수 있다.
- ④ 부인방지(Non-Repudiation) 기능을 제공하며 송신자의 개인키와 공개키를 가지고 암호화와 복호화하여 저장된 메시지를 생성할 수 있다.

7. 다음 중 로봇프로그램과 사람을 구분하는 방법의 하나로 사람이 인식할 수 있는 문자나 그림을 활용하여 자동 회원가입 및 게시물 포스팅을 방지하는데 사용하는 방법은 무엇인가?

- ① 해시함수(Hash Function)
- ② 인증서(Certificate)
- ③ 전자서명(Digital Signature)
- ④ 캡차(CAPTCHA)

8. 다음 중 공인인증서의 설명으로 옳지 않은 것은 무엇인가?

- ① 공인인증서는 사용자의 공개키와 사용자의 ID정보를 결합하여 인증기관의 전자서명을 포함한 문서이다.
- ② 공인인증서에는 버전, 발행자, 유효기간, 알고리즘 식별자, 사용자의 개인키 등이 포함되어 있다.
- ③ 인증기관이 자신의 키를 이용하여 전자서명을 생성 후, 인증서에 첨부하고, 인증기관 키를 사용하여 인증서의 유효성을 확인한다.
- ④ 공인인증서 관련한 표준으로 X.509가 있으며 대부분의 인증서는 이 표준을 따르고 있다.

9. 디스크 스케줄링 정책 중 큐의 항목을 순차적으로 처리하는 것은 무엇인가?

- ① SSTF(Shortest Service Time First)
- ② FIFO(First-In-First-Out)
- ③ SCAN
- ④ C-SCAN(Circular SCAN)

10. 컴퓨터의 메모리는 사용되는 방식에 따라 여러 개의 영역으로 나누어 생각할 수 있는데 프로그램 실행 중 malloc()등의 system call로 할당되어 사용되다가 free()등의 system call로 해제되는 영역은 무엇인가?

- ① Text 영역
- ② Data 영역
- ③ Stack 영역
- ④ Heap 영역

11. 유닉스(Unix) 운영체제에서 파일에 대한 권한을 모두 허용 (-rwxrwxrwx)하는 모드(명령어)는 무엇인가?

- ① chmod 777
- ② chmod a-rwx
- ③ chmod 666
- ④ chmod ug+rw

12. 리눅스(Linux) 사용자의 패스워드를 암호화하여 저장하고 있는 파일은 무엇인가?

- ① /etc/shadow
- ② /etc/passwd
- ③ /etc/skel
- ④ /etc/group

13. 윈도우(Windows)에서 지원하지 않는 파일시스템은 무엇인가?

- ① FAT32
- ② EXT2
- ③ NTFS
- ④ FAT16

14. 윈도우(Windows) 시스템의 레지스트리(Registry)에 대한 설명으로 옳지 않은 것은 무엇인가?

- ① HKEY_CLASSES_ROOT는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 어플리케이션에 대한 맵핑 정보 등을 갖고 있다.
- ② HKEY_CURRENT_USER는 시스템이 시작할 때 사용하는 하드웨어 프로파일 정보를 저장하고 있다.
- ③ HKEY_USERS는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.
- ④ HKEY_LOCAL_MACHINE은 시스템에 있는 하드웨어, 소프트웨어 정보를 갖고 있다.

15. 다음은 윈도우7 운영체제의 명령어 창에서 어떤 명령어를 실행한 출력 결과의 일부이다. 실행한 명령어는 무엇인가?

이미지 이름	PID	세션 이름	세션#	메모리 사용
=====	=====	=====	=====	=====
System Idle Process	0	Services	0	12 K
System	4	Services	0	284 K
smss.exe	472	Services	0	844 K
csrss.exe	592	Services	0	4,672 K
csrss.exe	648	Console	1	16,528 K
csrss.exe	656	Services	0	4,288 K
wininit.exe	708	Services	0	9,260 K
services.exe	732	Services	0	8,900 K
lsass.exe	740	Console	1	6,244 K
winlogon.exe	768	Services	0	4,580 K
lsm.exe	868	Services	0	7,340 K
svchost.exe	928	Services	0	5,780 K
nvsvc.exe	960	Services	0	6,564 K
svchost.exe	1048	Services	0	3,228 K

- ① netstat -an
- ② ipconfig /all
- ③ tasklist
- ④ arp -a

16. 유닉스(Unix) 운영체제의 로그파일과 그 로그파일에 기록되는 내용을 바르게 짝지은 것은 무엇인가?

가. history	- 각 사용자별 수행한 명령을 기록
나. sulog	- su 명령어의 로그를 기록
다. xferlog	- 실패한 로그인 시도를 기록
라. loginlog	- FTP 파일 전송 내역을 기록

- ① 가, 나
- ② 가, 다
- ③ 나, 다
- ④ 다, 라

17. 다음 지문에서 설명하는 공격은 무엇인가?

가. 두 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법
나. 공격 조건으로 프로그램에 root권한의 SetUID가 설정되어야 함
다. 대응 방법으로는 임시파일 사용 시 링크상태, 파일의 종류, 파일의 소유자, 파일의 변경여부 등을 점검

- ① 힙 오버플로우(Heap Overflow) 공격
- ② 레이스 컨디션(Race Condition) 공격
- ③ 스택 오버플로우(Stack Overflow) 공격
- ④ 코드(Code) 기반 공격

18. OSI 7계층 중 다음 내용을 수행하는 계층은 무엇인가?

가. 메시지 분할 및 조립, 순서화
나. 포트주소 지정
다. 연결제어
라. 다중화와 역다중화

- ① 전송층(Transport Layer)
- ② 링크층(Link Layer)
- ③ 네트워크층(Network Layer)
- ④ 세션층(Session Layer)

19. 다음은 TCP 제어 플래그에 대한 설명이다. 옳지 않은 것은 무엇인가?

- ① TCP 제어 플래그는 TCP 연결제어나 전송 데이터를 관리하기 위해 사용된다.
- ② URG 패킷은 순서에 상관없이 우선적으로 전송된다.
- ③ SYN 패킷은 TCP 통신에서 세션 확립을 위해 가장 먼저 전송된다.
- ④ RST 패킷은 송신측에서 더 이상 보낼 데이터가 없을 때 전송된다.

20. 다음 중 프로토콜과 포트번호의 연결이 옳지 않은 것은 무엇인가?

- ① HTTP - 80
- ② SMTP - 25
- ③ DNS - 53
- ④ TELNET - 20

21. 다음 지문에서 설명하는 것은 무엇인가?

가. 침입탐지시스템(IDS, Intrusion Detection System)의 일종이다.
나. Rule을 이용한 침입탐지 분석 기능을 가지고 있다.
다. 네트워크상에서 실시간 트래픽 분석, 프로토콜 분석이 가능하다.

- ① Snort
- ② Sniffer
- ③ Strings
- ④ Encase

22. 데이터 통신에서 사용되는 통신방식에 대한 설명 중 옳은 것은 무엇인가?
- ① Half-duplex 방식은 한쪽에서 데이터를 보내고 난 이후, 다른 한쪽에서 데이터 전송이 가능하다.
 - ② Full-duplex 방식은 수신측에서는 송신측으로 응답할 수 없다.
 - ③ Half-duplex 방식은 키보드(입력)와 모니터(출력) 사이의 전송이다.
 - ④ Full-duplex 방식은 양방향으로 송수신이 가능하나, 한 순간에는 반드시 한쪽 방향으로만 전송 가능하다.

23. Traceroute 명령은 자신의 컴퓨터가 인터넷을 통해 목적지를 찾아가면서 거치는 구간의 정보를 기록하는 유틸리티이다. 이때 ICMP 프로토콜과 IP헤더의 () 필드를 사용하여 라우팅 경로를 추적한다. ()에 들어 갈 적합한 단어는 무엇인가?
- ① 버전
 - ② TOS
 - ③ TTL
 - ④ Checksum

24. 다음 중 서비스 거부 공격에 의해 직접적으로 위협받을 수 있는 정보보호의 요소는 무엇인가?
- ① 무결성
 - ② 부인방지
 - ③ 기밀성
 - ④ 가용성

25. 컴퓨터의 네트워크 연결 상태를 점검하기 위해 netstat 명령을 사용하였다. 다음 중 옳지 않은 것은 무엇인가?
- ① LISTENING - 연결을 위하여 접속을 대기하고 있는 상태
 - ② CLOSED_WAIT - 완전히 종료된 상태
 - ③ ESTABLISHED - 서로 연결된 상태
 - ④ TIME_WAIT - 연결이 종료되었거나 다음 연결을 위해 대기하고 있는 상태

26. 다음 중 지문에서 설명하는 공격 방식과 바르게 짝지어진 것은 무엇인가?

가. 패킷을 전송할 때 출발지IP주소와 목적지IP주소를 동일하게 만들어 전송하는 공격

나. TCP 3-way handshake 과정 중 Listen 상태에서 SYN을 받은 서버가 SYN/ACK를 전달한 후 ACK를 무한정 기다리게 하는 공격

다. 공격자가 다량의 ICMP Echo Request의 출발지IP주소를 피해시스템의 IP주소로, 목적지IP주소를 Direct Broadcast IP주소로 Spoofing하여 공격

	가	나	다
①	Smurf Attack	SYN Flooding Attack	Land Attack
②	SYN Flooding Attack	Land Attack	Smurf Attack
③	Land Attack	SYN Flooding Attack	Smurf Attack
④	SYN Flooding Attack	Smurf Attack	Land Attack

27. 다음 중 쿠키 세션 위조 공격과 그 방지방법에 대한 설명으로 옳지 않은 것은 무엇인가?
- ① SSO(Single-Sign-On)를 사용하는 응용프로그램의 경우 공격자는 쿠키를 알아냄으로써 공격을 수행할 수 있다.
 - ② 사용자 PC에 저장되는 쿠키정보는 불안전하므로 암호화하여 변조를 방지할 수 있다.
 - ③ 세션이 비활성 상태인 동안에도 발생 가능하다.
 - ④ 세션관리 정보를 서버 측에 저장하고 서버 측 세션을 사용하도록 구현함으로써 쿠키 세션 위조 공격을 방지할 수 있다.

28. 다음은 웹서버 로그에서 볼 수 있는 상태코드(응답코드)로 HTTP/1.1에서 정의한 것이다. 옳지 않은 것은 무엇인가? (상태코드 : 설명)
- ① 200 : OK
 - ② 400 : Access Denied
 - ③ 404 : Not Found
 - ④ 500 : Internal Server Error

29. 다음 지문에서 설명하는 공격 방법은 무엇인가?

가. 웹 서버에 명령을 실행하여 관리자 권한을 획득하는 공격 방법이다.

나. 웹 어플리케이션의 첨부파일에 대한 부적절한 신뢰와 불충분한 점검으로 인해 악의적인 공격코드가 웹 서버로 전송, 실행 되는 방법이다.

다. 파일 업로드 취약점을 이용하여, 이것의 종류로는 서버 명령을 실행할 수 있는 asp, cgi, php, jsp 파일 등이 있다.

- ① 웹셸(Web Shell)
- ② 워터링홀(Watering Hole)
- ③ APT(Advanced Persistent Threats)
- ④ Encase

30. OWASP는 주로 웹에 관한 정보노출, 악성파일 및 스크립트, 보안 취약점을 연구하고 있다. ‘10대 웹 어플리케이션 취약점’ 2013년 에디션에 속하지 않는 것은 무엇인가?
- ① Buffer Overflow(버퍼 오버플로우)
 - ② Broken Authentication and Session Management(인증 및 세션 관리 취약점)
 - ③ Cross Site Scripting(크로스 사이트 스크립팅)
 - ④ Injection(인젝션)

31. 웹과 DB를 연동한 어플리케이션에서 SQL Injection 공격을 방어하기 위한 방법으로 옳지 않은 것은 무엇인가?
- ① DB 어플리케이션을 최소권한으로 구동한다.
 - ② DB에 내장된 프로시저를 사용한다.
 - ③ 원시 ODBC 에러를 사용자가 볼 수 있도록 코딩한다.
 - ④ DB 테이블 이름, 컬럼 이름, SQL구조 등이 외부 HTML에 포함되어 나타나지 않도록 한다.

32. 다음 지문에서 설명하는 DB보안 요구 사항은 무엇인가?

- 가. 기밀이 아닌 데이터로부터 기밀 정보를 얻어내는 가능성을 의미한다.
- 나. DB데이터는 상호연관 가능성이 있어, 데이터에 직접 접근하지 않고도 가용한 데이터 값을 이용할 수 있다.
- 다. 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하는 것을 의미한다.

- ① 추론 방지
- ② 데이터 무결성
- ③ 감사 기능
- ④ 사용자 인증

33. 다음 지문에서 설명하는 시스템은 무엇인가?

- 가. 공격성향이 있는 자들을 중요한 시스템으로부터 다른 곳으로 끌어내도록 설계된 유도시스템이다.
- 나. 공격자의 동작에 관한 정보를 수집한다.
- 다. 관리자가 반응할 수 있도록 공격자로 하여금 시스템에 충분히 오랜 시간동안 머무르도록 유도한다.

- ① 라디어스(RADIUS)
- ② 허니팟(Honeypot)
- ③ 방화벽(Firewall)
- ④ AAA(Authentication Authorization Accounting)

34. 다음 중 공격 명칭과 공격에 대한 설명이 바르게 짝지어진 것은 무엇인가?

- 가. ARP Spoofing - IP주소를 위·변조하는 공격
- 나. XSS(Cross Site Scripting) - 게시물에 실행코드와 태그의 업로드가 규제되지 않는 경우 이를 악용하여 열람한 타 사용자의 PC로부터 정보를 유출할 수 있는 공격
- 다. MITM(Man-In-The-Middle) 공격 - 통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 정보를 자기 것과 바꾸어 버림으로써 들키지 않고 도청을 하거나 통신 내용을 바꾸는 공격

- ① 가, 나
- ② 가, 다
- ③ 나, 다
- ④ 가, 나, 다

35. 다음 중 공격기법과 그에 대한 설명으로 옳은 것은 무엇인가?

- ① Smurf Attack : IP Broadcast Address로 전송된 ICMP 패킷에 대해 응답하지 않도록 시스템을 설정하여 방어할 수 있다.
- ② Heap Spraying : 아이디와 패스워드 같이 사용자의 입력이 요구되는 정보를 프로그램 소스에 기록하여 고정시키는 방식이다.
- ③ Backdoor : 조직 내에 신뢰할 만한 발신인으로 위장해 ID 및 패스워드 정보를 요구하는 공격이다.
- ④ CSRF : 다른 사람의 세션 상태를 훔치거나 도용하여 액세스 하는 해킹 기법을 말한다.

36. 최근 사이버범죄자들은 인터넷 접속 시 추적을 피하기 위해 VPN(Virtual Private Network)서비스를 이용하고 있다. 다음 중 VPN에서 사용하는 프로토콜이 아닌 것은 무엇인가?

- ① PPTP(Point-to-Point Tunneling Protocol)
- ② L2TP(Layer 2 Tunneling Protocol)
- ③ PGP(Pretty Good Privacy)
- ④ IPSec(Internet Protocol Security)

37. 다음 지문에서 설명하는 공간은 무엇인가?

저장매체의 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간으로, 물리적으로 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 말한다. 램, 드라이브, 파일시스템, 볼륨 등에 나타난다.

- ① 클러스터(Cluster)
- ② 파티션(Partition)
- ③ 섹터(Sector)
- ④ 슬랙(Slack)

38. 다음 지문에서 설명하는 포렌식 도구는 무엇인가?

- 가. Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어이다.
- 나. 컴퓨터 관련 수사에서 디지털 증거의 획득과 분석 기능을 제공하며, 미국에서 1990년대 후반부터 600여개 사법기관에서 컴퓨터 관련 범죄수사에 활용되고 있으며, 미국 법원이 증거능력을 인정하는 독립적인 솔루션이다.
- 다. Windows 환경에서 증거원본 미디어에 어떠한 영향을 미치지 않으면서도 ‘미리보기’, ‘증거사본작성’, ‘분석’, ‘결과보고’에 이르는 전자증거조사의 모든 과정을 수행할 수 있다.

- ① Wireshark
- ② Encase
- ③ KICS
- ④ IDA

39. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조(벌칙) 제1항의 각 호 내용 중 일부를 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

- ① 이용자의 동의를 받지 아니하고 개인정보를 수집한 자
- ② 정보통신망에 침입한 자
- ③ 정보통신망에 장애가 발생하게 한 자
- ④ 타인의 정보를 훼손하거나 타인의 비밀을 판매 또는 도용한 자

40. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신망에 유통되어서는 안 되는 불법정보 관련 조항을 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

- ① 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
- ② 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
- ③ 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인을 모욕하는 내용의 정보
- ④ 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보