

1과목 : 과목 구분 없음

1. 다음에서 설명하는 프로토콜은?

- 인터넷 환경에서 오류에 관한 처리를 지원한다.
- 네트워크 계층의 프로토콜로, 오류가 발생한 IP 패킷에 대하여 그 원인을 송신 호스트에 전달한다.
- 전송과정에서 문제가 발생하면 필요할 경우 라우터에 의해 이 프로토콜 메시지가 자동으로 발생한다.

- ① ICMP                      ② IGMP  
③ ARP                      ④ FTP

2. HTTPS에 의해 암호화되지 않는 통신 요소는?

- ① 요청 문서 URL              ② 문서의 내용  
③ 포트 번호                  ④ HTTP 헤더의 내용

3. 커beros(Kerberos) 버전4에 대한 설명으로 옳지 않은 것은?

- ① MIT에서 개발되어 공공 및 상업 영역에서 사용된다.  
② 신뢰하는 제3자 인증 서비스를 사용한다.  
③ 클라이언트, 응용 서버, 커beros 서버(키분배센터)로 구성된다.  
④ 원격 인증에 사용하기에는 부적절하다.

4. 스니핑(sniffing) 공격에 대한 설명으로 옳은 것은?

- ① 네트워크 트래픽에서 데이터를 도청하는 수동적 공격이다.  
② 네트워크 장비에 대량의 트래픽을 전송하여 서비스를 중단시키는 공격이다.  
③ 공격자가 다른 사용자의 IP 주소를 사용하여 네트워크에 접근하는 공격이다.  
④ 공격자가 특정 값을 찾아내기 위해 모든 조합을 시도하는 공격이다.

5. 다음에서 설명하는 기술은?

트래픽의 경로를 지정하는 제어 평면과 트래픽 전송을 수행하는 데이터 평면을 분리하며, OpenFlow 프로토콜 등을 통해 네트워크를 프로그램할 수 있다.

- ① BSS(Business Support System)  
② OSS(Operation Support System)  
③ SDN(Software Defined Networking)  
④ MPLS(Multi-Protocol Label Switching)

6. SSL/TLS에 대한 공격유형에 해당하지 않는 것은?

- ① ESP 공격  
② PKI 공격  
③ 레코드와 응용 데이터 프로토콜 공격  
④ 핸드셰이크 프로토콜 공격

7. POP3에 대한 설명으로 옳지 않은 것은?

- ① POP3는 서버로부터 메일을 다운로드하는 기능을 제공한다.

다.

- ② POP3 서버의 well-known 포트는 25번이다.  
③ +OK 응답은 요구한 명령을 성공적으로 처리했음을 의미한다.  
④ POP3 클라이언트와 서버는 명령과 응답으로 동작한다.

8. IPv4 데이터그램 형식에 대한 설명으로 옳지 않은 것은?

- ① 'Flags'는 단편화(fragmentation)와 관련이 있는 필드이다.  
② 'Time To Live'는 데이터그램이 방문할 수 있는 최대 라우터의 수를 나타내는 필드이다.  
③ 'Total Length'는 헤더를 제외한 IP 데이터그램의 길이를 나타내는 필드이다.  
④ 'Protocol'은 IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 나타내는 필드이다.

9. 다음에서 설명하는 네트워크 관리 기능은?

- 가능한 한 효과적인 실행을 보장하기 위하여 네트워크를 감시하고 제어한다.
- 통계 정보를 수집하고, 시스템 상태 미력 기록을 유지·검사하며, 시스템 성능을 측정하고, 지연 시간과 대역폭 사용률, 패킷 처리율 등을 단계별 또는 시간별로 관리한다.

- ① 장애 관리                      ② 구성 관리  
③ 성능 관리                      ④ 보안 관리

10. 공개키 기반 구조 X.509(PKIX) 모델에서 종단 개체(end entity)와 인증 기관(certificate authority) 간의 관리 기능에 해당하지 않는 것은?

- ① 등록(registration)  
② 키 쌍 복구(key pair recovery)  
③ 키 쌍 갱신(key pair update)  
④ 교차 인증(cross-certification)

11. SMS에 포함된 URL을 클릭하면 악성 앱이 설치되는 스미싱을 예방하는 방법으로 옳지 않은 것은?

- ① 보호되지 않는 무선 공유기의 사용을 금지한다.  
② 스마트폰 환경 설정에서 알 수 없는 출처 앱 설치를 허용한다.  
③ 모바일 백신을 설치하여 스마트폰의 보안 상태를 주기적으로 점검한다.  
④ 스마트폰 운영체제를 항상 최신 버전으로 업데이트하여 보안상 취약점이 없도록 관리한다.

12. 다음에서 설명하는 보안 기술은?

- 사전에 수립한 규칙에 따라 패킷을 차단 또는 허용한다.
- 접근 제어가 가장 기본적이고 중요한 기능이다.
- 구현 방식에 따라 패킷 필터링과 프록시 방식 등이 있다.

- ① SSO                              ② VLAN  
③ DLP                              ④ Firewall

13. 다음에 기술된 IEEE 802.11i RSN의 동작 단계를 순서대로

나열한 것은?

- (가) 인증(authentication)  
(나) 탐색(discovery)  
(다) 안전 데이터 전송(protected data transfer)  
(라) 키 생성 및 분배(key generation and distribution)

- ① (가)→(나)→(다)→(라)      ② (가)→(나)→(라)→(다)  
③ (나)→(가)→(라)→(다)      ④ (나)→(라)→(가)→(다)

14. SNMP에서 관리 대상 장치 내부 객체들에 대한 정보 저장소를 나타내는 용어는?

- ① MIB      ② Community  
③ PDU      ④ Agent

15. 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격은?

- ① DNS 스푸핑 공격      ② E-mail 스푸핑 공격  
③ IP 스푸핑 공격      ④ ICMP 리다이렉트 공격

16. 다음과 같이 각 문자에 숫자를 배정할 때, 시저 암호 치환식  $C = (P + 3) \bmod 26$ 을 활용하여 평문 STUDY를 암호화한 것은? (단, 치환식에서 C는 암호문, P는 평문이다)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- ① VWXGB      ② UVWFA  
③ TUVEZ      ④ VWXFN

17. SSL Handshake 프로토콜의 2단계 '서버 인증과 키 교환 (server authentication and key exchange)'에서 인증서 (certificate) 메시지가 사용되지 않는 기법은?

- ① RSA 기법      ② Anonymous DH 기법  
③ Ephemeral DH 기법      ④ Fixed DH 기법

18. 전자 서명(digital signature)에 대한 설명으로 옳지 않은 것은?

- ① 서명된 문서는 기밀성이 보장된다.  
② 서명된 문서는 데이터가 변조되지 않았음을 보장하는 무결성을 만족한다.  
③ 한 번 생성된 서명을 다른 문서의 서명으로 사용할 수 없다.  
④ 전자 서명과 관련된 표준으로 DSS가 있다.

19. NAC(Network Access Control) 시스템에 대한 설명으로 옳지 않은 것은?

- ① ARP 방식은 차단하려는 단말에 ARP 스푸핑 패킷을 보내 네트워크 접근을 제어한다.  
② 802.1x 방식은 802.1x RADIUS 서버와 802.1x를 지원하는 스위치가 필요하다.  
③ 소프트웨어 에이전트 설치 방식은 네트워크에 접속하려는 모든 클라이언트에 에이전트를 설치할 필요는 없다.  
④ VLAN 방식은 인가받지 않은 클라이언트가 인가된 클라이언트와는 다른 별도의 VLAN으로 격리된다.

20. IPSec에 대한 설명으로 옳지 않은 것은?

- ① 네트워크 계층에서 동작하는 보안 프로토콜이다.  
② 트래픽을 암호화하고, 무결성을 보장하며, 인증을 제공한다.  
③ 전송 모드와 터널 모드가 있다.  
④ IPSec에서 AH 프로토콜은 페이로드 데이터를 암호화한다.

전자문제집 CBT PC 버전 : [www.comcbt.com](http://www.comcbt.com)

전자문제집 CBT 모바일 버전 : [m.comcbt.com](http://m.comcbt.com)

기출문제 및 해설집 다운로드 : [www.comcbt.com/x](http://www.comcbt.com/x)

전자문제집 CBT란?

종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.

PC 버전 및 모바일 버전 완벽 연동

교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

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