네트워크 보안

문 1. 전송 과정에서 발생한 데이터 오류를 검출하고 검출된 오류를 정정할 수 있는 것은?

① BCD 코드
② 단일 패리티 비트
③ 해밍(Hamming) 코드
④ 체크섬

문 2. 방화벽과 침입탐지시스템의 장점을 결합한 네트워크 보안 장비로, 트래픽 모니터링과 유해 트래픽 차단을 목적으로 하는 것은?

① Honey Pot
② IPS
③ NAC
④ DMZ

문 3. 다음에서 설명하는 SSL 프로토콜은?

> 메시지의 무결성과 기밀성을 제공하기 위하여, 클라이언트와 서버 간 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증 코드 생성 및 암호화 과정 등을 수행한다.

① Alert Protocol
② Record Protocol
③ Handshake Protocol
④ Change Cipher Spec Protocol

문 4. IPsec의 SA(Security Association)을 생성하기 위한 키 관리 방식은?

① EAPOL
② OSPF
③ DKIM
④ IKE

문 5. 163.152.175.62/26이 클래스 없는 주소(classless address)로 주어졌다. 해당 IP 주소가 속한 네트워크에 대한 설명으로 옳은 것만을 모두 고르면?

> ㄱ. /26에서의 26은 prefix의 길이를 의미한다.
> ㄴ. 네트워크 내의 주소 개수는 128개이다.
> ㄷ. 네트워크 마스크는 255.255.255.128이다.
> ㄹ. 네트워크에는 주소 163.152.175.15/26이 포함된다.

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

문 6. 다음은 SSL 프로토콜에서 쌍방이 응용 데이터를 전송하기 전에, 인증 및 키 합의를 위하여 교환한 메시지의 일부를 나타낸 것이다. 메시지가 발생하는 순서를 바르게 나열한 것은? (단, 순서 중간에 다른 메시지가 포함될 수 있음)

> ㄱ. Client_Key_Exchange
> ㄴ. Certificate
> ㄷ. Change_Cipher_Spec

① ㄱ → ㄴ → ㄷ
② ㄱ → ㄷ → ㄴ
③ ㄴ → ㄱ → ㄷ
④ ㄴ → ㄷ → ㄱ

문 7. IEEE 802.11i의 키 관리에 대한 다음 설명에서 (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

> AAAK라고도 불리는 MSK는 IEEE 802.1X 프로토콜에 의해 인증 단계에서 생성된다. 인증의 마지막 과정이 끝나고 나면 AP(Access Point)와 STA(클라이언트 스테이션)는 (가)를 공유하게 된다. (가)로부터 AP와 STA 간의 통신에 사용할 (나)가 만들어지는데, (나)의 일부인 (다)가 사용자의 무선 데이터 패킷의 암호화에 사용된다.

	(가)	(나)	(다)
①	PMK	PTK	TK
②	PMK	TK	PTK
③	PTK	PMK	TK
④	PTK	TK	PMK

문 8. 방화벽 유형의 하나인 응용 레벨 게이트웨이에 대한 설명으로 옳은 것은?

① 외부 네트워크와 내부 네트워크 간의 직접적인 패킷 교환을 허용한다.
② OSI 참조 모델의 응용 계층에서 동작하며 여러 응용 서비스에 대하여 하나의 프록시로 구현된다.
③ 단순 패킷 필터링 방식에 패킷들의 상태 정보를 관리하는 기능이 추가된 것이다.
④ 응용 프로그램 수준의 트래픽을 기록하고 감시하기가 용이하며, 추가로 사용자 인증과 같은 부가 서비스를 지원할 수 있다.

문 9. TCP RFC 793을 준수하는 시스템의 닫혀 있는 포트에 대하여 TCP FIN, NULL, Xmas 스캔을 한 경우 시스템의 반응으로 옳은 것은?

① ICMP 도달 불가능 오류 메시지
② 아무 응답 없음
③ RST
④ RST + ACK

문 10. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?
① 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.
② 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.
③ TCP/IP 프로토콜을 사용하는 인터넷에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.
④ MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.

문 11. IPv4 헤더의 필드 중, IP 패킷이 방문할 수 있는 최대 라우터 수를 제한하기 위한 것은?
① Time To Live
② Fragment Offset
③ Header Checksum
④ Flags

문 12. TCP 포트 번호 143을 사용하는 메일 접속 프로토콜로, 사용자가 폴더를 생성하고 폴더에 메시지를 할당하는 기능을 제공하는 것은?
① HTTP
② SMTP
③ POP3
④ IMAP

문 13. ICMP Echo Request 패킷을 브로드캐스트 주소로 전송하여 많은 양의 응답 패킷이 공격 대상으로 전송되게 하는 서비스 거부 공격은?
① Ping of Death
② SYN Flooding
③ Smurf
④ Land

문 14. IPsec 터널 모드를 사용하는 VPN(Virtual Private Network)에 대한 설명으로 옳지 않은 것은?
① 인터넷과 같은 공중망을 이용하여 사설망의 효과를 얻기 위한 기술이다.
② 내부 네트워크의 호스트는 보안 게이트웨이를 거쳐서 통신함으로써 자신의 본래 IP 주소를 외부 네트워크에 노출하지 않는다.
③ 내부 IPv4 패킷의 전체를 암호화하고 선택적으로 인증할 수 있다.
④ IPv6의 경우에는 New IP Header를 사용하지 않고, 본래 헤더를 그대로 사용한다.

문 15. 커버로스 버전 4의 메시지 교환 중, 클라이언트(C)가 서버(V)의 서비스를 얻기 위해 티켓발행서버(TGS)에게 보내는 메시지에 포함되지 않는 것은?
① C가 인증서버(AS)로부터 받은 티켓
② V의 식별자
③ C와 V가 사용할 공유비밀키
④ C와 TGS의 세션키로 암호화된 타임스탬프

문 16. 사설 주소를 이용하는 내부 네트워크를 인터넷에 연결하는 NAT(Network Address Translation) 라우터에 대한 설명으로 옳지 않은 것은?
① 여러 개의 사설 주소는 내부 통신을 위하여 사용하고, 한 개 이상의 전역 인터넷 주소는 외부 통신을 위하여 사용하도록 해 준다.
② 변환 테이블을 이용하여 내부에서 외부로 전송하고자 하는 모든 패킷의 발신지 주소를 전역 주소로 변환해 준다.
③ 외부 인터넷에서 라우터뿐만 아니라 사설 주소를 사용하는 호스트를 식별할 수 있다.
④ 내부 네트워크 호스트와 외부 서버 프로그램들이 다대다 관계를 가질 수 있도록, 변환 테이블에는 IP 주소 외에 전송 계층의 포트 번호와 같은 추가적인 정보가 포함될 수 있다.

문 17. ARP에 대한 설명으로 옳지 않은 것은?
① 호스트와 라우터는 IP 주소와 MAC 주소의 매핑 정보를 캐시 테이블에 가지고 있다.
② 캐시 테이블 정보를 공격자 호스트의 MAC 주소로 업데이트하게 하는 ARP 스푸핑 공격을 통해 스니핑이 발생할 수 있다.
③ 한 호스트의 캐시 테이블은 서브넷상의 모든 호스트와 라우터에 대한 엔트리를 가지고 있어야 한다.
④ ARP의 요청은 브로드캐스트되고, 응답은 유니캐스트된다.

문 18. TCP의 3-Way Handshaking을 통한 서버와의 연결 설정 과정에서, 연결에 성공한 클라이언트 측의 연결 상태 천이 다이어그램상의 상태 변화의 순서를 바르게 나열한 것은?
① CLOSED → SYN_RCVD → ESTABLISHED
② CLOSED → SYN_SENT → ESTABLISHED
③ LISTEN → SYN_RCVD → ESTABLISHED
④ LISTEN → SYN_SENT → ESTABLISHED

문 19. IDS의 오용 탐지(misuse detection) 기법에 대한 설명으로 옳은 것은?
① 이미 발견되어 알려진 공격 패턴과 일치하는지를 검사하여 침입을 탐지한다.
② 오탐률이 높지만 새로운 공격 기법을 포함한 광범위한 공격을 탐지할 수 있다.
③ 정상적이고 평균적인 상태의 범주를 벗어나 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생할 경우에 침입 탐지를 알린다.
④ 데이터 마이닝 등을 활용하여 수집한 다양한 정보를 분석하므로 많은 학습 시간이 소요된다.

문 20. IPsec의 ESP에서 재전송 공격(replay attack)을 방지하기 위해 사용하는 것은?
① Sequence Number
② SPI(Security Parameters Index)
③ ICV(Integrity Check Value)
④ Next Header