네트워크 보안

문 1. 네트워크에 연결된 노드가 사용할 IP 주소를 자동으로 할당해주는 프로토콜은?

① DHCP(Dynamic Host Configuration Protocol)
② ICMP(Internet Control Message Protocol)
③ ARP(Address Resolution Protocol)
④ IGMP(Internet Group Management Protocol)

문 2. 공격 유형에 관한 설명으로 옳지 않은 것은?

① 사회공학적 공격은 신뢰 관계나 인간의 심리를 이용하여 중요한 정보를 획득하는 것이다.
② 무차별(brute force) 공격은 특정 값을 찾아내기 위해 가능한 모든 조합을 시도하는 공격이다.
③ 스니핑은 네트워크상에서 다른 사용자들의 트래픽을 도청하는 것이다.
④ 재연(replay) 공격은 두 개체 간의 패킷을 중간에서 가로채서 변조하여 전송함으로써 정당한 사용자로 가장하는 공격이다.

문 3. 외부와 내부 네트워크의 경계에서 기본적인 패킷 필터링 기능만을 제공하는 데 적합한 네트워크 보안 구성은?

① 스크리닝 라우터
② 스크린드 호스트 게이트웨이
③ 스크린드 서브넷 게이트웨이
④ 응용레벨 게이트웨이

문 4. 스위칭 환경에서의 스니핑 기법이 아닌 것은?

① ICMP 리다이렉트
② 스위치 재밍(jamming)
③ ARP 리다이렉트
④ TCP 세션 하이재킹

문 5. 다음의 ㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?

> 무선 랜에서의 프라이버시 강화를 위하여 IEEE 802.11에서 (㉠)를 정의하였으나, 이 표준에서 무결성 보장과 키 사용의 심각한 약점이 발견되었다. (㉡)에서 이를 개선할 목적으로 IEEE 802.11i의 초안에 기초한 중간 조치로 (㉢)를 공표하였고, 이후 IEEE 802.11i 전체 표준을 따르는 새로운 보안 대책이 등장하게 되었다.

	㉠	㉡	㉢
①	WPA	Wi-Fi Alliance	WPA2
②	WPA	IETF	WPA2
③	WEP	Wi-Fi Alliance	WPA
④	WEP	IETF	WPA

문 6. 거리 벡터가 아닌 링크 상태를 활용하는 자율시스템(autonomous system) 도메인 내의 라우팅 프로토콜은?

① RIP(Routing Information Protocol)
② OSPF(Open Shortest Path First)
③ BGP(Border Gateway Protocol)
④ IGRP(Interior Gateway Routing Protocol)

문 7. SSL(Secure Socket Layer)에서 서버와 클라이언트 간의 인증과 키 교환 메시지를 주고받는 프로토콜은?

① Record
② Handshake
③ Change Cipher Spec
④ Alert

문 8. 클라이언트가 위조된 웹사이트에 접속하게 하는 것을 목적으로 하는 공격 기법은?

① DNS 스푸핑
② ARP 스푸핑
③ 스니핑
④ SYN flooding

문 9. 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로, TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용되는 것은?

① ping
② netstat
③ nmap
④ nbtstat

문 10. 유닉스 시스템의 'traceroute'가 발신지에서 목적지까지의 패킷 전달 경로를 추적하는 과정에서 사용하지 않는 것은?

① ICMP
② TCP
③ UDP
④ IP 패킷의 TTL(Time To Live) 필드

문 11. DMZ(demilitarized zone) 네트워크내에 일반적으로 두지 않는 것은?

① 웹 서버
② 이메일 서버
③ DNS 서버
④ 내부 접속용 데이터베이스 서버

문 12. 다음 설명에 해당하는 네트워크 장비가 바르게 연결된 것은?

(가) 두 개 이상의 LAN을 하나로 연결하는 장치
(나) 여러 대의 컴퓨터를 손쉽게 연결할 수 있도록 여러 개의 입력과 출력 포트를 가지고 있으며, 한 포트에서 수신된 신호를 다른 모든 포트로 재전송하는 장치
(다) 이종 통신망 간에도 프로토콜을 변환하여 정보를 주고받을 수 있는 장치
(라) 패킷의 수신 주소를 토대로 경로를 정해서 패킷을 전송함으로써 둘 이상의 네트워크를 연결하는 장치

	(가)	(나)	(다)	(라)
①	브리지	허브	라우터	게이트웨이
②	브리지	허브	게이트웨이	라우터
③	허브	브리지	게이트웨이	라우터
④	허브	브리지	라우터	게이트웨이

문 13. IPv4의 주소 부족 현상을 해결하기 위한 접근 방법이 아닌 것은?

① NAT
② SNMP
③ IPv6
④ DHCP

문 14. 패킷 재조합의 문제를 악용하여 오프셋이나 순서가 조작된 일련의 패킷 조각들을 보냄으로써 자원을 고갈시키는 서비스 거부(DoS) 공격은?

① Land
② Teardrop
③ SYN flooding
④ Smurf

문 15. IEEE 802.11i RSN(Robust Security Network) 동작 단계에 대한 설명으로 옳지 않은 것은?

① 발견 단계에서는 STA(Station)와 AP(Access Point)가 서로를 인지하여 일련의 보안 능력에 합의하고, 해당 보안 능력을 이용하여 향후 통신에 사용할 연관을 설정한다.
② 인증 단계에서는 STA와 AS(Authentication Server)간의 상호 인증을 위하여 EAP(Extensible Authentication Protocol)를 교환한다.
③ 키 관리 단계에서는 STA와 AP간에 사용되는 한 쌍의 쌍별 키와 멀티캐스팅 통신에 사용되는 그룹 키가 정의된다.
④ 보호 데이터 전송 단계에서는 CRC(Cyclic Redundancy Check)로 메시지 인증과 데이터 기밀성을 제공한다.

문 16. 128.23.16.0/20이 시작 주소인 IP 주소 블록을 동일한 크기의 8개 주소 블록으로 나눌 경우 얻어지는 서브넷의 시작 주소로 옳은 것은?

① 128.23.0.0/23
② 128.23.2.0/23
③ 128.23.20.0/23
④ 128.23.32.0/23

문 17. 윈도우즈 시스템에서 “route PRINT -4” 명령을 실행한 결과로 표현되는 정보가 아닌 것은?

① 네트워크 마스크
② 게이트웨이
③ TCP/UDP 포트
④ 인터페이스

문 18. UDP(User Datagram Protocol)의 헤더 포맷에 포함되어 있는 필드는?

① 시퀀스 번호(sequence number)
② 목적지 IP 주소(destination IP address)
③ 체크섬(checksum)
④ 헤더 길이(header length)

문 19. IPsec에 대한 설명으로 옳지 않은 것은?

① 전송모드에서 AH(Authentication Header)는 IP 페이로드와 IP 헤더의 선택된 부분을 인증한다.
② 전송모드에서 ESP(Encapsulating Security Payload)는 IP 헤더는 암호화하지 않고 IP 페이로드를 암호화한다.
③ 터널모드에서는 패킷 암호화를 지원하는 ESP와 인증을 제공하는 AH가 같이 사용되어야 한다.
④ IKE(Internet Key Exchange) 프로토콜을 사용하여 보안 연관(Security Association)을 설정한다.

문 20. ARP(Address Resolution Protocol)에 대한 설명으로 옳지 않은 것은?

① ARP는 논리 주소를 물리 주소로 변환해준다.
② ARP 패킷에는 발신자와 해당 수신자의 물리 주소와 논리 주소가 포함된다.
③ ARP 패킷은 데이터링크 프레임에 캡슐화된다.
④ 같은 네트워크상에서 ARP 요청 패킷과 ARP 응답 패킷은 브로드캐스트 된다.