네트워크 보안

1. 공격자가 ARP 스푸핑 공격으로 위조하려는 것은?
① Port 번호 ② ICMP 에코 요청 패킷
③ MAC 주소 ④ DNS 응답 메시지

2. route 명령으로 얻은 라우팅 테이블 정보와 같은 결과물을 출력할 수 있는 것은?
① traceroute ② tcpdump
③ netstat ④ ping

3. 다음에서 설명하는 것은?

> ○ 외부 방화벽과 내부 방화벽 사이에 존재한다.
> ○ 외부에서 접속할 수 있어야 하며 보호되어야 하는 시스템(예: 회사의 웹사이트, 이메일 서버 등)을 여기에 배치한다.

① NAT(Network Address Translation)
② DMZ(Demilitarized Zone)
③ VPN(Virtual Private Network)
④ PAN(Personal Area Network)

4. 접근 제어 방식에 대한 다음 설명의 (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

> [(가)]는 사용자 ID가 아닌 시스템에서 정의한 사용자의 역할을 바탕으로 접근 권한을 정의한다. 각 사용자는 [(나)] 정적 또는 동적으로 할당될 수 있다.

(가)	(나)
① DAC	하나의 역할에만
② DAC	여러 개의 역할에
③ RBAC	하나의 역할에만
④ RBAC	여러 개의 역할에

5. HTTP 버전 1.1에서 정의된 메소드의 설명으로 옳지 않은 것은?
① POST는 서버가 클라이언트에게 문서를 전달하는 데 사용한다.
② GET은 클라이언트가 서버에게 문서를 요청할 때 사용한다.
③ HEAD는 클라이언트가 문서 자체가 아니라 문서에 대한 정보를 원할 때 사용한다.
④ TRACE는 클라이언트가 검사 목적으로 서버에게 정보 반환을 요청하는 데 사용한다.

6. DNS 스푸핑 공격의 순서를 바르게 나열한 것은?

> (가) 클라이언트는 공격자가 전송한 DNS Response를 올바른 메시지로 인식한다.
> (나) 로컬에 존재하며 DNS 서버보다 클라이언트와 가까이 위치한 공격자는 위조된 DNS Response를 클라이언트에게 전송한다.
> (다) 공격자는 스니핑 공격을 통해 클라이언트가 DNS 서버로 DNS Query를 전송하는 것을 확인한다.

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

7. 서버가 클라이언트로부터 받은 비밀키에 대하여 여러 번 해시 함수를 적용하여 얻은 해시 체인으로 일회용 비밀번호(OTP)를 생성하는 것은?
① S/KEY 방식
② 시간 동기화 방식
③ 이벤트 동기화 방식
④ 챌린지-응답 방식

8. WPA(Wi-Fi Protected Access)에 대한 설명으로 옳지 않은 것은?
① WPA는 WEP의 보안 취약점을 보완하기 위해 제안되었다.
② WPA의 TKIP는 암호 알고리즘으로 AES를 사용한다.
③ WPA-EAP는 인증을 위해서 RADIUS 서버를 이용할 수 있다.
④ WPA-PSK는 사전에 공유된 비밀키를 사용한다.

9. DoS 공격 방식에 대한 설명으로 옳지 않은 것은?
① 스머프(Smurf) 공격은 발신지 주소가 거짓으로 조작된 ICMP 패킷을 받은 네트워크의 많은 컴퓨터들이 발신지 주소로 응답을 보내게 하여 트래픽 범람을 일으키는 것이다.
② 티어드롭(Teardrop) 공격은 IP 패킷 헤더 정보를 조작해서 패킷 조각(fragment)이 중첩되도록 보내어 이를 전달받은 시스템의 IP 패킷 재조합 과정에서 오류를 발생시킨다.
③ 슬로로리스(Slowloris) 공격은 HTTP 메시지 헤더의 Content-Length 필드에 임의의 큰 값을 설정하여 웹 서버가 클라이언트에서 해당 크기의 메시지를 전송할 때까지 연결을 유지하게 함으로써 정상적인 사용자의 접속을 받아들일 수 없게 하는 것이다.
④ HTTP GET 플러딩 공격은 정상적인 TCP 세션과 함께 정상적으로 보이는 과도한 HTTP GET을 요청받은 웹 서버에 과부하가 걸리게 한다.

10. (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

> ○ [(가)]은/는 네트워크 레벨에서 패킷에 대한 보안을 제공하기 위해 설계된 프로토콜의 모음이다.
> ○ [(가)]이/가 지원하는 [(나)]에서는 새로운 IP 헤더가 추가된다.

(가)	(나)
① IPSec	전송모드
② IPSec	터널모드
③ TLS	전송모드
④ TLS	터널모드

11. 무선 랜의 MAC 프레임에 대한 다음 설명의 (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

> 802.11 무선 랜 표준의 매체 접속 프로토콜은 [(가)]이고, 무선 MAC 계층 프레임 포맷에는 [(나)]개의 주소 필드가 있다.

(가)	(나)
① CSMA/CD	2
② CSMA/CD	4
③ CSMA/CA	2
④ CSMA/CA	4

12. SSL/TLS 핸드셰이크 프로토콜에서 클라이언트가 보내는 client_hello 메시지에 포함되지 않는 것은?
① 난수
② 클라이언트가 지원하는 암호 그룹(Cipher Suite) 목록
③ 클라이언트가 지원하는 압축 방식 목록
④ 인증서

13. (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

> 스위치 환경에서 공격자의 스위치 재밍을 통해 스위치의 매핑 테이블의 최대 저장 개수보다 더 많은 정보가 추가되어 스위치가 [(가)]모드로 동작하여, 같은 스위치 내에 위치한 공격자는 네트워크 인터페이스 카드를 [(나)]모드로 설정하여 스니핑이 가능하다.

	(가)	(나)
①	Broadcast	Full-duplex
②	Broadcast	Promiscuous
③	Unicast	Full-duplex
④	Unicast	Promiscuous

14. 다음은 TCP 3-Way Handshaking 과정의 예를 나타낸 것이다. (가) ~ (라)에 들어갈 숫자를 바르게 연결한 것은? (단, C: Client, S: Server, [ ]: 세그먼트 플래그, seq: 순서 번호, ack: 확인응답 번호)

> C → S, [SYN] seq = 102
> S → C, [SYN−ACK] seq = [(가)], ack = [(나)]
> C → S, [ACK] seq = [(다)], ack = [(라)]

	(가)	(나)	(다)	(라)
①	213	102	103	214
②	102	103	103	214
③	103	102	213	214
④	330	103	103	331

15. 암호 알고리즘에 대한 설명으로 옳지 않은 것은?
① SEED는 128비트의 블록 암호 알고리즘이며, SEED 128과 SEED 256의 키 길이는 각각 128비트와 256비트이다.
② HIGHT는 경량 환경 및 하드웨어의 효율성 향상을 위해 개발된 128비트의 블록 암호 알고리즘이다.
③ DES는 64비트의 블록 암호 알고리즘으로 16라운드로 구성되어 있다.
④ LEA는 국내에서 개발된 128비트의 블록 암호 알고리즘으로 128비트, 192비트, 256비트의 비밀키를 사용할 수 있다.

16. HMAC에 대한 설명으로 옳지 않은 것은?
① IP 보안에서 메시지 인증 목적으로 사용된다.
② MD5, SHA-1, RIPEMD-160과 같은 해시 함수를 내장하고 있다.
③ 비밀키를 적용한 블록 암호화와 해시 함수를 사용해서 결과를 산출한다.
④ IEEE 802.11i의 의사 난수 생성 과정에 사용된다.

17. DNSSEC(DNS Security Extensions)에 대한 설명으로 옳지 않은 것은?
① DNS 응답 메시지에 대한 기밀성을 제공한다.
② DNS 데이터에 공개키 기반 전자서명을 추가하여 데이터의 무결성을 제공한다.
③ DNS 응답 수신자(resolver)는 수신한 데이터에 대한 서명을 검증한다.
④ DNSSEC는 DNS 캐시 포이즈닝 공격을 방어하도록 설계되었다.

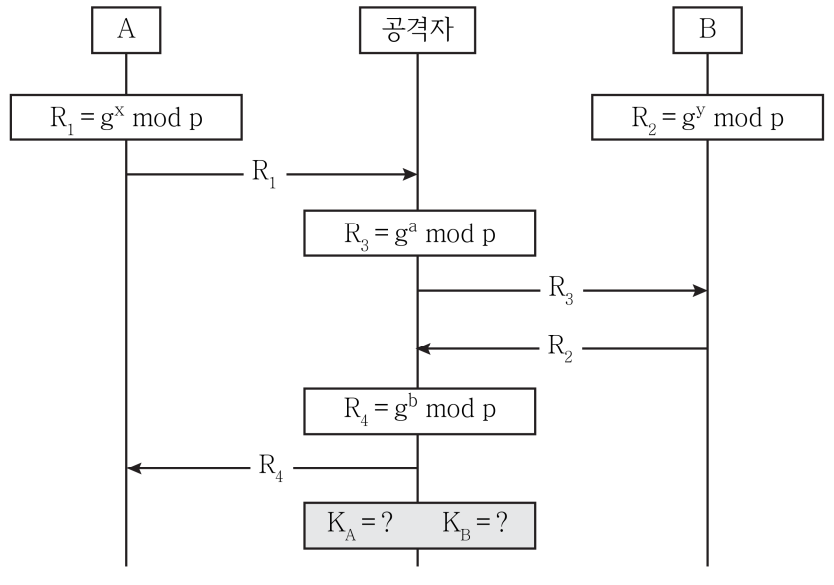
18. 하트블리드(Heartbleed)에 대한 다음 설명의 (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

> TLS를 구현하기 위한 오픈 소스인 OpenSSL에 내재된 버그로, [(가)] 프로토콜의 요청을 받은 컴퓨터에서 적절한 [(나)]이 이루어지지 않아서 피해자가 의도하지 않은 내용이 응답 패킷의 페이로드에 복사되어 공격자에게 전송될 수 있다.

	(가)	(나)
①	Handshake	페이로드 길이 확인
②	Handshake	사용자 인증
③	Heartbeat	페이로드 길이 확인
④	Heartbeat	사용자 인증

19. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?
① SSH는 안전한 원격 로그온 기능을 제공하기 위해 설계되었다.
② 사용자 인증 프로토콜을 통해 사용자가 서버에게 인증받는다.
③ 포트 전달을 통해 임의의 안전하지 않은 TCP 연결을 안전한 SSH 연결로 변환시킬 수 있다.
④ 전송 계층 프로토콜은 하나의 SSH 연결을 여러 개의 논리적 통신 채널로 다중화한다.

20. 다음은 사용자 A와 B가 Diffie-Hellman 알고리즘에 의한 키 교환을 시도하려는 도중에 발생한 중간자 공격의 개념을 도시한 것이다. 공격자가 A와의 공유비밀키 K_A와 B와의 공유비밀키 K_B를 산출하는 계산식을 바르게 연결한 것은? (단, p는 소수, g는 p의 원시근, x, y, a, b는 p보다 작은 임의의 양의 정수)



	K_A	K_B
①	$R_1^a \bmod p$	$R_2^b \bmod p$
②	$R_1^b \bmod p$	$R_2^a \bmod p$
③	$R_2^a \bmod p$	$R_1^b \bmod p$
④	$R_2^b \bmod p$	$R_1^a \bmod p$