네트워크 보안

1. 정보보안 3대 요소 중 서비스 거부(Denial of Service) 공격의 침해 대상은?

① 가용성
② 기밀성
③ 무결성
④ 익명성

2. 네트워크에서 서버의 작동과 서버가 제공하는 서비스 존재 여부를 확인하는 것은?

① 스캐닝(scanning)
② 스미싱(SMishing)
③ 스위칭(switching)
④ 스풀링(SPOOLing)

3. 응용계층 프로토콜로 옳지 않은 것은?

① FTP(File Transfer Protocol)
② SCTP(Stream Control Transmission Protocol)
③ SMTP(Simple Mail Transfer Protocol)
④ Telnet

4. IEEE 802.11 무선 랜에서 네트워크를 식별하기 위해 사용되는 것은?

① OID(Object IDentifier)
② SSID(Service Set IDentifier)
③ RFID(Radio Frequency IDentification)
④ NIDS(Network-based Intrusion Detection System)

5. 한 번의 시스템 인증을 통하여 여러 정보 시스템에 재인증 절차 없이 접근할 수 있는 통합 로그인 기술은?

① DRM
② SSO
③ SET
④ PGP

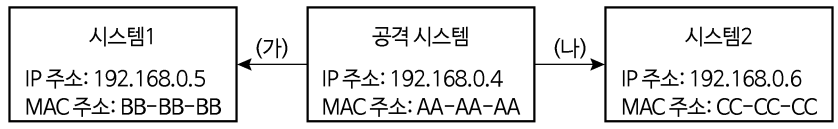
6. 스니핑(sniffing) 공격에 대한 보안 대책으로 옳지 않은 것은?

① 원격 접속 시 SSH 사용
② 웹 환경에서 HTTPS 사용
③ 스위치 대신 더미 허브 사용
④ 이메일 환경에서 S/MIME 사용

7. 블록체인에서 보유한 자산에 대한 지분율에 비례하여 의사결정 권한을 주는 합의 알고리즘은?

① PoS(Proof of Stake)
② PoW(Proof of Work)
③ PRNG(Pseudo-Random Number Generator)
④ PBFT(Practical Byzantine Fault Tolerance)

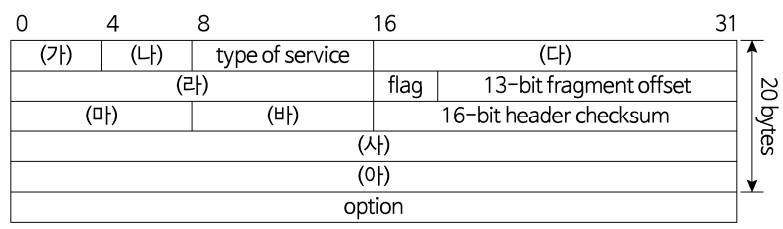
8. 다음 랜(LAN)에서 '공격시스템'이 ARP 스푸핑(spoofing) 공격을 위해 (가), (나)에서 수행하는 작업을 ㄱ ~ ㄹ에서 찾아 바르게 연결한 것은? (단, MAC 주소는 24비트로 가정한다)



ㄱ. 시스템1의 MAC 주소를 AA-AA-AA라고 알린다.
ㄴ. 시스템2의 MAC 주소를 AA-AA-AA라고 알린다.
ㄷ. 시스템1의 MAC 주소를 CC-CC-CC라고 알린다.
ㄹ. 시스템2의 MAC 주소를 BB-BB-BB라고 알린다.

	(가)	(나)
①	ㄴ	ㄱ
②	ㄴ	ㄷ
③	ㄹ	ㄱ
④	ㄹ	ㄷ

9. Land 공격을 위한 IPv4 데이터그램 헤더에서 같은 값을 저장하는 필드로만 묶인 것은?



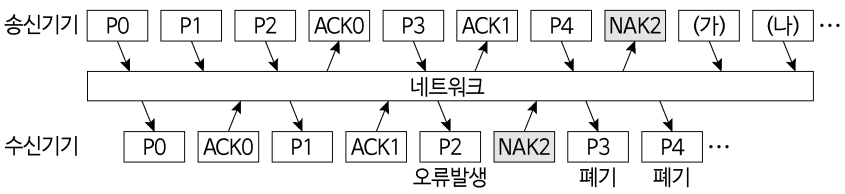
① (가), (나)
② (다), (라)
③ (마), (바)
④ (사), (아)

10. 다음에서 설명하는 취약점을 이용하는 서비스 거부 공격은?

서버는 클라이언트와 TCP 3-way 핸드셰이크(handshake) 과정을 완료하기 전에 절반-개방(half-open) 연결을 큐에 저장하는데 이 같은 큐는 한정된 용량을 가진다.

① Smurf 공격
② Teardrop 공격
③ SYN flooding 공격
④ Ping-of-death 공격

11. 다음 Go-Back-N ARQ(Automatic Repeat reQuest)를 사용하는 송신기기와 수신기기 사이에 주고받은 통신 패킷 중 (가), (나)에 들어갈 내용을 바르게 연결한 것은? (단, 윈도 크기는 3이다)



(가)	(나)
① P0	P1
② P1	P2
③ P2	P3
④ P3	P4

12. SSL/TLS 프로토콜 구조에 속하지 않는 것은?

① Record Protocol
② Handshake Protocol
③ Change Cipher Spec Protocol
④ Authentication Header Protocol

13. 암호학적 해시 함수(cryptographic hash function)의 성질 또는 특징으로 옳지 않은 것은?

① 양방향성
② 충돌 저항성(resistance)
③ 역상(preimage) 저항성
④ 제2(second) 역상 저항성

14. 다음에서 설명하는 공격을 막는 방법으로 옳지 않은 것은?

> 공격자가 몰래 보관해둔 기존의 정상적인 MAC(Message Authentication Code) 값을 재사용하여 전송하는 공격이다.

① 비표(nonce) 사용
② 리다이렉션(redirection) 사용
③ 타임스탬프(timestamp) 사용
④ 순서 번호(sequence number) 사용

15. 다음 SSH의 전송 계층 프로토콜 작업을 순서대로 나열한 것은?

> (가) 서비스 요청(service request)
> (나) 키 교환 종료(end of key exchange)
> (다) 알고리즘 협상(algorithm negotiation)
> (라) 식별 문자열 교환(identification string exchange)

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

16. CIDR(Classless Inter-Domain Routing)에 대한 설명으로 옳지 않은 것은?

① IP 주소 고갈 문제를 해결하기 위해 도입되었다.
② IP 주소를 클래스 구분 없이 지정할 수 있게 해 준다.
③ IPv4 주소체계에서만 지원하며, IPv6 주소체계에서는 지원하지 않는다.
④ 슬래시(slash, '/')를 사용하여 네트워크 프리픽스(prefix)의 길이를 표시한다.

17. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

> (가) 랜(LAN) 통신 보안을 위해, (나)는 RC4 암호화 알고리즘을 기본으로 사용하며, 암호화 과정에서 24비트의 IV(Initial Vector)를 사용한다.

(가)	(나)
① 무선	WEP(Wired Equivalent Privacy)
② 무선	WPA2(Wi-Fi Protected Access 2)
③ 유선	WEP
④ 유선	WPA2

18. VPN(Virtual Private Network)에 대한 설명으로 옳지 않은 것은?

① VPN 구현을 위해 터널링 기술을 사용한다.
② 기밀성을 제공하기 위해 암호화 기술을 사용한다.
③ VPN 구현을 위해 PPTP, L2TP 등을 사용할 수 있다.
④ SSL VPN은 SA(Security Association)를 생성하기 위해 IKE (Internet Key Exchange)를 사용한다.

19. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?

① 네트워크 관리에 필요한 정보를 주고받기 위해 사용한다.
② 하위 계층 프로토콜로 UDP를 사용한다.
③ 에이전트(agent)는 비정상적인 상황에 대한 경고 메시지를 관리자(manager)에게 보낼 수 있다.
④ 관리자는 에이전트로부터 정보를 가져올 수 있으나, 에이전트에 있는 정보를 설정할 수 없다.

20. 터널 모드로 동작하는 IPSec의 ESP(Encapsulating Security Payload) 프로토콜에서 사용하는 다음 패킷의 구조 (가) ~ (다)에 들어갈 내용을 바르게 연결한 것은? (단, 패킷의 버전은 IPv4이다)

(가)	(나)	(다)	TCP	데이터	…

(가)	(나)	(다)
① ESP 헤더	기존 IP 헤더	새 IP 헤더
② ESP 헤더	새 IP 헤더	기존 IP 헤더
③ 새 IP 헤더	기존 IP 헤더	ESP 헤더
④ 새 IP 헤더	ESP 헤더	기존 IP 헤더