네트워크보안

1. 다음 <보기>의 ㉠, ㉡, ㉢에 가장 적합한 것으로 짝지어진 것은?

< 보기 >

○ 이더넷은 네트워크 인터페이스 카드에 설정된 ㉠ 물리적 주소를 사용한다.
○ 네트워크 계층의 주소는 ㉡ 논리 주소를 사용한다.
○ 전송계층의 주소는 ㉢ 포트 주소를 사용한다.

① ㉠ 8Byte ㉡ 2Byte ㉢ 1Byte
② ㉠ 8Byte ㉡ 4Byte ㉢ 2Byte
③ ㉠ 6Byte ㉡ 2Byte ㉢ 1Byte
④ ㉠ 6Byte ㉡ 4Byte ㉢ 2Byte

2. 다음 <보기>는 라우터를 이용한 네트워크 보안 설정에 관련된 내용이다. 가장 옳은 내용을 모두 고르시오.

< 보기 >

㉠ egress 필터링은 라우터 내부에서 외부로 나가는 패킷의 소스 IP를 체크하여 필터링하는 것이다.
㉡ ingress 필터링은 standard 또는 extended access-list를 활용하여 라우터 내부로 유입되는 패킷의 소스 IP나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링하는 것이다.
㉢ blackhole 필터링이란 인터페이스를 통해 들어오는 패킷의 소스 IP에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인하는 것이다.
㉣ unicast RPF는 access-list나 blackhole 필터링을 이용하여 일일이 IP나, IP대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

① ㉠, ㉡, ㉢ ② ㉠, ㉣
③ ㉠, ㉡, ㉣ ④ ㉠, ㉡, ㉢, ㉣

3. TCP는 흐름 제어를 다루기 위하여 슬라이딩 윈도우(Sliding Window)를 사용한다. 수신자 호스트 B는 8500 바이트의 버퍼를 갖고 있으며, 현재 버퍼에 3150 바이트의 처리되지 않은 데이터를 갖고 있다고 가정했을 때, 호스트 A를 위한 수신자 윈도우(rwnd) 값은?

① 3150
② 5350
③ 8500
④ 11650

4. 다음 중 DDoS(Distributed Denial of Service) 공격과 툴에 대한 설명으로 가장 옳지 않은 것은?

① Teardrop은 두 번째 패킷의 Fragment Offset을 위조하여, 첫 번째 패킷 다음에 두 번째 패킷을 추가하지 않고 첫 번째 패킷의 TCP 헤더와 데이터 부분을 덮어쓰게 한다.
② Trinoo는 UDP Flood 서비스 거부 공격에 사용되는 툴이다.
③ Ghost Call은 IP Scan 이후 프리픽스로 호를 시도하여, Digest 인증을 해킹하는 공격을 의미하는 것이 아니라, 단순한 INVITE를 보내는 패턴 공격이다.
④ NetBot Attacker는 발신지와 수신지 IP를 동일하게 설정하여 라우터 및 서버의 성능장애나 시스템 다운을 유발시킨다.

5. ICMP(Internet Control Message Protocol) 프로토콜은 문제를 해결하는 기능과 전달할 수 없는 패킷에 대한 에러 정보를 알리기 위해 사용된다. 아래 대표적인 ICMP 메시지의 기능을 설명한 것 중 가장 옳지 않은 것은?

① Echo Request 메시지는 원하는 호스트로의 IP 연결을 확인하기 위해 사용된다.
② Destination Unreachable은 라우터나 목적호스트에 의해 보내지며 데이터그램이 전달되지 못한다는 것을 데이터를 보낸 호스트에 알려준다.
③ Source Quench는 데이터를 보내는 호스트에게 IP 데이터그램이 라우터의 집중현상에 의해 손실되고 있음을 알리기 위해 라우터가 보내는 메시지이다.
④ Echo Reply는 데이터를 보내는 호스트에게 목적 IP 주소에 대한 좀 더 적합한 경로가 있음을 알리기 위해 라우터가 보내는 메시지이다.

6. 다음 TCP(Transport Control Protocol) 프로토콜의 타이머에 대한 설명 중 가장 옳지 않은 것은?

① RTO 값은 해당 시간까지 Acknowledge가 전송되어 오지 않는 경우, 재전송하기 위한 설정값이다.
② RTO 값은 초기 RTT값을 기준으로 항상 고정되어 있다.
③ RTO 시간이 너무 클 경우 수신측의 중복 ACK에 대한 손실 세그먼트를 재전송 하는 Fast retransmission 현상이 발생한다.
④ TCP 세그먼트가 유실되어, 해당 세그먼트를 요구하는 Acknowledge가 계속 도착하더라도 RTO 시간이 Time-out되어야 재전송이 가능하다.

7. 다음 <보기>는 TCP Session Hijacking의 공격 순서를 나열한 것이다. 순서가 가장 옳은 것은?

< 보기 >

㉠ 공격 목표를 정하고 공격 대상을 설정한다.
㉡ 시퀀스 넘버의 난이도 검사를 한다.
㉢ TCP/IP 스택 구현이나 원리를 예측하고, 이를 통하여 얻어진 데이터로부터 시퀀스 넘버를 추측한다.
㉣ 공격자가 세션을 설정하고자 하는 컴퓨터로부터 시퀀스 넘버의 추측이 끝나면 그 서버와 연결되어 있는 컴퓨터에게 DoS 공격 등을 통하여 사용자를 제거한다.
㉤ 공격 대상에 세션을 설정하여 현재 공격 목표와 연결되어있는 공격 대상의 세션을 설정한다.
㉥ 제거된 사용자로부터 추측한 시퀀스 넘버를 이용하여 Session Hijacking을 실시한다.

① ㉠-㉡-㉢-㉣-㉤-㉥
② ㉠-㉤-㉡-㉣-㉢-㉥
③ ㉠-㉢-㉣-㉡-㉤-㉥
④ ㉠-㉡-㉤-㉢-㉣-㉥

8. 다음 중 침입 방지 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 침입 방지 시스템의 검사영역은 네트워크 계층과 전송계층의 IP/Port 정보를 기반으로 동작한다.
② 침입 방지 시스템의 검사영역은 방화벽이 검사할 수 없는 전송계층 상단의 어플리케이션 계층의 데이터까지도 검사가 가능하다.
③ 침입 경고 이전에 상대의 공격을 중단시키는데 목적을 두고 있다.
④ 안티 바이러스와 같은 시그니처 기반의 기술과 방화벽과 같은 네트워크 차단기능이 결합된 방식을 침입 방지 시스템이라 한다.

9. 다음 중 무선 보안 강화 방안을 설명한 것 중 가장 옳지 않은 것은?

① SSID를 브로드캐스트 불가로 접속하면 누구도 접속할 수 없다.
② TKIP은 WEP을 적용할 수 있도록 구성된 무선랜 장비 펌웨어 업그레이드나 소프트웨어 업그레이드를 통해 사용자 레벨의 보안을 강화하기 위한 방법을 제공하고 있다.
③ WEP는 RC4 스트림 암호화 기법을 사용하고 키 스트림을 정적 키를 사용한다.
④ IEEE 802.11i는 AES 암호화 기법을 사용한다.

10. 다음 중 가상사설망(VPN) 구현에 사용되는 터널링 프로토콜(Tunneling Protocol)로 가장 옳은 것은?

① PPTP, IPSEC, MPLS
② PPTP, L2TF, WAP
③ IPSEC, SET, SSL
④ L2TF, WAP, IPSEC

11. 다음 <보기>는 오용탐지(Misuse Detection)와 이상탐지(Anomaly Detection)에 대한 설명이다. 이상탐지에 해당되는 것을 모두 고른 것은?

< 보기 >

㉠ 통계적 분석방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다.
㉡ 미리 축적한 시그니처와 일치하면 침입으로 판단한다.
㉢ 제로데이 공격탐지에 적합하다.
㉣ 임계값을 설정하기 쉽기 때문에 오탐률이 낮다.

① ㉠, ㉢ ② ㉠, ㉣ ③ ㉡, ㉢ ④ ㉡, ㉣

12. 다음 중 가상 사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은?

① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.
② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자인증의 보안 기능을 제공한다.
③ 네크워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다.
④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택근무자나 이동중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.

13. 다음 중 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명으로 가장 옳지 않은 것은?

① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원한다.
② 방화벽이나 게이트웨이 등에 구현한다.
③ IP 기반의 네트워크에서만 동작한다.
④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능하다.

14. 다음 <보기>에서 설명하는 보안 시스템은?

< 보기 >

○ 패킷을 버리거나 또는 의심이 가는 트래픽을 감지함으로써, 공격 트래픽을 방어하는 기능을 가지고 있다.
○ 모든 트래픽을 수신하는 스위치의 포트를 모니터하고, 특정 트래픽을 막기 위하여 적합한 명령어를 라우터(Router)나 침입차단시스템(Firewall)에 전송할 수 있다.
○ 호스트(Host) 기반의 이 보안 시스템은 공격을 감지하기 위하여 서명이나 비정상 감지기술을 사용한다.

① IDS ② IPS ③ DNS ④ VPN

15. 다음 중 네트워크 기반 공격기법에 대한 설명으로 가장 옳지 않은 것은?

① SYN Flooding 공격은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.
② Zero Day 공격은 시그니처(Signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.
③ APT 공격은 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.
④ Buffer Overflow 공격은 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

16. 다음 <보기>는 보안 공격 유형을 나열한 것이다. 소극적 공격을 모두 고른 것은?

< 보기 >

㉠ 신분위장(Masquerade)
㉡ 재전송(Replay)
㉢ 패킷 분석(Analysis of Packet)
㉣ 메시지 수정(Modification of Message)
㉤ 스니핑(Sniffing)
㉥ 서비스 거부(Denial of Service)

① ㉠, ㉢, ㉤ ② ㉠, ㉣
③ ㉢, ㉤ ④ ㉢, ㉣, ㉥

17. 다음 중 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보로 가장 옳은 것은?

① 수신 시스템이 처리할 수 있는 윈도우 크기
② 패킷을 송신하고 수신하는 프로세스의 포트 번호
③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
④ 송신 시스템의 TCP 패킷의 생성 시간

18. 다음 중 ACL 적용 규칙에 해당하지 않는 것으로 가장 옳은 것은?

① Named ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.
② ACL의 마지막에는 deny any가 생략되어 있다.
③ ACL은 먼저 입력한 순서대로 수행된다.
④ Numbered ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.

19. 다음 <보기>의 VPN에 대한 설명 중 가장 옳은 것을 모두 고른 것은?

< 보기 >

㉠ 터널링 기술은 VPN의 기본이 되는 기술로서 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 캡슐화하는 기술이다.
㉡ 데이터 암호화 기술은 터널이 형성된 한 쪽 호스트에서 데이터를 암호화해서 보내면 반대편 호스트에서 암호화 데이터를 복호화하여 원본 데이터를 확인하게 된다.
㉢ VPN은 데이터의 출처 즉, 출발지 IP가 확실한지에 대한 인증기술을 제공하고, 내부 자원에 대해서 허가 받지 않은 사용자의 접속을 차단하는 접근제어 기능을 제공한다.
㉣ VPN 구현에 가장 널리 사용되는 터널링 프로토콜에는 PPP, SSL, SSH 등이 있다.

① ㉠
② ㉠, ㉡
③ ㉠, ㉡, ㉢
④ ㉠, ㉡, ㉢, ㉣

20. 다음 중 무선랜 구축 시 보안을 위한 고려사항으로 가장 옳지 않은 것은?

① SSID(Service Set IDentifier)를 숨김모드로 사용
② 무선 단말기의 MAC(Media Access Control)주소 인증 수행
③ 관리자용 초기 ID/Password 변경
④ 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용