네트워크보안

1. 다음 중 스니핑(Sniffing) 공격에 대처하는 방법으로 가장 올바른 것은?
   ① 전용 네트워크 망에서만 통신을 수행한다.
   ② SSL, SSH를 사용한다.
   ③ VLAN 기능을 활성화한다.
   ④ 데이터 전송시에 패킷마다 다른 경로를 사용한다.

2. 다음 중 NAT(Network Address Translation)를 사용하는 가장 근본적인 이유로 올바른 것은?
   ① IP 주소 부족 문제를 해결
   ② 데이터 암호화
   ③ 네트워크 세그먼테이션
   ④ 네트워크 전송 속도 향상

3. 다음 중 OSI 계층구조와 계층별로 사용되는 보안 프로토콜의 연결이 가장 옳지 않은 것은?
   ① 데이터링크 계층 - TLS
   ② 네트워크 계층 - IPSec
   ③ 전송계층 - SSL
   ④ 응용계층 - SSH

4. 다음 중 UTM(Unified Threat Management)에 대한 설명으로 가장 옳지 않은 것은?
   ① 방화벽, VPN, IPS 등의 보안 기능을 하나로 통합하여 제공한다.
   ② 각각 다른 보안 정책을 수립하여 적용한다.
   ③ 보안 기능이 하나로 통합되어 구축시 비용이 절감된다.
   ④ 다양하고 복잡한 보안 위협에 대응하고 편의성이 향상된다.

5. 다음 중 LAN(Local Area Network) 관련 IEEE 802 표준에 대한 설명으로 가장 옳은 것은?
   ① IEEE 802.2는 Token Bus에 관한 규정이다.
   ② IEEE 802.3은 CSMA/CD에 관한 규정이다.
   ③ IEEE 802.5는 LLC 서브계층에 관한 규정이다.
   ④ IEEE 802.6은 Token Ring에 관한 규정이다.

6. 다음 중 TCP Well-Known Port 번호와 서비스의 연결이 잘못된 것은?
   ① TCP 21 - FTP
   ② TCP 22 - SSH
   ③ TCP 25 - SNMP
   ④ TCP 80 - HTTP

7. 다음 중 IPv6의 주소 유형으로 옳지 않는 것은?
   ① Unicast
   ② Anycast
   ③ Broadcast
   ④ Multicast

8. 다음 중 네트워크로 연결된 단말을 확인하는 것으로 무결성 검사, IP 주소와 MAC 주소로 접근제어를 하는 보안솔루션으로 가장 올바른 것은?
   ① IPS(Intrusion Prevention System)
   ② NAT(Network Address Translation)
   ③ NAC(Network Access Control)
   ④ DRM(Digital Rights Management)

9. netstat -s 명령으로 프로토콜별 통계정보를 확인할 수 있다. 다음 중 이에 해당되지 않는 프로토콜은 무엇인가?
   ① MAC
   ② ICMP
   ③ TCP
   ④ UDP

10. 다음 중 허니팟(Honeypot)에 대한 설명으로 가장 옳지 않은 것은?
    ① 컴퓨터 시스템에 침입한 스팸, 바이러스, 크래커를 탐지하기 위하여 의도적으로 설치한 시스템이다.
    ② 실제 공격을 당한 것처럼 보이도록 만든 함정이다.
    ③ 공격자가 허니팟으로 접근할 수 없도록 차단해야 한다.
    ④ 침입자가 오래도록 머물게 해야 한다.

11. 다음 중 지능형 지속 공격(Advanced Persistent Threat, APT)에 대한 설명 중 가장 옳지 않은 것은?
    ① 사회 공학적 방법을 사용한다.
    ② 공격 대상이 명확하다.
    ③ 불분명한 목적과 동기를 가진 해커 집단이 주로 사용한다.
    ④ 가능한 방법을 총동원한다.

12. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳은 것은?
① 망분리 기술로 USB와 같은 저장매체를 통한 악성코드 침입이 불가능하다.
② 물리적 망분리 기법에는 SBC 및 CBC 기반의 망분리 기법이 존재한다.
③ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.
④ 논리적 망분리는 VDI(Virtual Desktop Infrastructure)와 OS 커널 분리로 분류 될 수 있다.

13. 다음 중 DMZ(dimilitarized zone)에 대한 설명으로 가장 옳은 것은?
① 외부 네트워크에서는 DMZ에 접근할 수 없다.
② DMZ내에는 외부 인터넷에 서비스를 제공하기 위해 매우 높은 보안 수준을 요구하므로 주로 내부 접속용 데이터베이스 서버가 위치하고 있다.
③ 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다.
④ DMZ는 보안 조치가 취해진 네트워크 영역으로 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.

14. 다음에서 설명하고 있는 공격은?

> 이 공격은 할당된 메모리 경계에 대한 검사를 하지 않은 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어 쓰는 방식이다. 만약 실행 코드가 덮어 써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다.

① Buffer Overflow 공격 ② SQL Injection 공격
③ IP Spoofing 공격 ④ Format String 공격

15. 다음은 네트워크 서비스 거부 공격으로 인한 접속 마비에 대한 현상 및 대응요령을 설명한 것이다. 다음 중 가장 옳지 않은 것은?
① 리눅스 시스템의 경우 iptables를 이용한 패킷 필터링을 설정한다.
② 이상 트래픽에 의한 네트워크 속도 저하시 서비스 거부 공격을 의심하고, 트래픽을 분석한다.
③ 서비스 거부 공격시 라우터의 패킷 필터링 기능을 설정하여 대응한다.
④ 외부에서 들어오는 패킷의 발신자를 확인하여 공격자에게 역공격을 감행한다.

16. 다음 중 웹 보안을 제공하는 방법인 SSL의 설명으로 가장 옳지 않은 것은?
① TCP/IP 프로토콜의 네트워크 계층에서 보안기능을 수행하며 전송 계층이 있는 프로토콜의 안정성을 제공한다.
② 웹사이트 접속시 http:// 대신 https://를 사용하며, 서버와 클라이언트의 상호 인증 기능이 있다.
③ 넷스케이프에서 개발된 프로토콜로써 네트워크 통신 및 인터넷 사용자에게 안전한 정보를 교환하기 위한 보안 프로토콜이다.
④ 기밀성 제공을 위한 비밀키는 핸드쉐이크 프로토콜에 의해 생성된다.

17. 다음 중 ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

> • (㉠) 기법은 정상적인 활동 데이터베이스와 비교하여 침입을 구분한다.
> • (㉡) 기법은 공격패턴, 시그니처 데이터베이스와 비교하여 침입을 구분한다.
> • (㉢) IDS(Intrusion Detection System)는 네트워크 상의 모든 패킷을 캡처한 후 이를 분석하여 침입을 탐지하는 시스템이다.
> ※ 이상탐지 : Anomaly Detection, 오용탐지 : Misuse Detection

	㉠	㉡	㉢
①	이상탐지	오용탐지	네트워크 기반
②	이상탐지	오용탐지	호스트 기반
③	오용탐지	이상탐지	네트워크 기반
④	오용탐지	이상탐지	호스트 기반

18. 컴퓨터의 네트워크 연결 상태를 점검하기 위해 netstat 명령을 사용하였다. 다음 설명 중 가장 옳지 않은 것은?
① LISTENING : 연결을 위해 접속을 대기하고 있는 상태
② CLOSE_WAIT : 연결 종료 메시지를 수신하고 그에 대한 확인메시지를 보낸 상태
③ ESTABLISHED : 완전히 종료된 상태
④ TIME_WAIT : 연결이 종료되었거나 다음 연결을 위해 대기하고 있는 상태

19. 다음 중 ESM(Enterprise Security Management) 기능으로 가장 옳지 않은 것은?

① 트래픽 조절 : 네트워크상의 트래픽 조절을 통한 연구생산성과 안정적인 성능을 지원 및 중요 트래픽의 대역폭 우선순위를 조절하여 안정적이고 신뢰성 있는 통신을 제공

② 통합관리 : 다양한 시스템에서 발생되는 이벤트를 로그화하여 관리자가 필요로 하는 모든 정보(Error, Warning, Notice, Account)를 손쉽게 검색

③ 종합관제 : 통합 관리 기능을 수행하기 위한 인터페이스를 제공하여, 다양한 보안시스템(방화벽, IDS, Scanner)에서 보내온 데이터에 의한 공격 유형, 공격자 정보, 발생 일시, 적용 필터 등을 실시간 모니터링하여 종합적으로 관리

④ 운영관리 : 관리자 관리, 권한별 접근 관리, 실시간 연결 데이터 관리 등을 통해, 관리자가 시스템을 보다 더 체계적으로 운영할 수 있도록 지원

20. 다음 중 무선랜의 보안을 강화하기 위한 대책으로 가장 안전하지 않은 것은?

① 무선랜 AP(Access Point) 접속시 데이터 암호화와 사용자 인증 기능을 제공하도록 한다.

② 무선랜 AP에 MAC(Media Access Control) 주소를 필터링하여 등록된 MAC 주소만 허용하는 정책을 설정한다.

③ 무선랜 AP에 보안을 위해 무지향성 안테나를 사용한다.

④ 무선랜 SSID(Service Set ID)를 숨김으로 설정하여 폐쇄시스템을 운영하면 SSID를 모르는 사용자의 접속시도가 현저하게 줄어든다.