네트워크보안

1. 다음 중 SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?
   ① ChangeCipherSpec - Handshake 프로토콜에 의해 협상된 암호규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.
   ② Handshake - 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.
   ③ Alert - 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.
   ④ Record - 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용계층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

2. 다음 중 망 내 교환 장비들이 오류 상황에 대한 보고를 할 수 있게 하고, 예상하지 못한 상황이 발생한 경우 이를 알릴 수 있도록 지원하는 프로토콜은 무엇인가?
   ① ICMP ② ARP ③ RARP ④ IGMP

3. 다음 <보기> 중 제시된 Well Known Port 번호에 해당하는 프로토콜을 순서대로 가장 적합하게 제시한 것은?

< 보 기 >

㉠ 22번 포트 ㉡ 53번 포트 ㉢ 161번 포트

   ① ㉠ SSH ㉡ Gopher ㉢ NetBIOS
   ② ㉠ SSH ㉡ DNS ㉢ SNMP
   ③ ㉠ FTP ㉡ Gopher ㉢ SNMP
   ④ ㉠ FTP ㉡ DNS ㉢ NetBIOS

4. 다음 중 OSI 7계층 모델에서 동작하는 계층이 가장 다른 것은?
   ① L2TP ② PPTP
   ③ SYN 플러딩 ④ ARP 스푸핑

5. 다음 중 SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?
   ① MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.
   ② 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.
   ③ 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.
   ④ TCP/IP 프로토콜을 사용하는 네트워크에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.

6. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은 무엇인가?
   ① DoS 공격
   ② 취약한 인증 및 세션 공격
   ③ SQL 삽입 공격
   ④ CSRF 공격

7. 다음 중 SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는데 악용될 수 있는 명령어는 무엇인가?
   ① HELO ② MAIL FROM
   ③ RCPT TO ④ VRFY

8. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳지 않은 것은?
   ① 물리적 망분리와 논리적 망분리 기법이 존재한다.
   ② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.
   ③ 논리적 망분리 기법으로 SBC 및 CBC 기반의 망분리 기법이 존재한다.
   ④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.

9. 다음 중 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직으로 가장 옳은 것은?
   ① CISO ② CERT ③ CPPG ④ CPO

10. 다음 중 HTTP 응답 메시지 상태 코드의 의미가 가장 옳지 않은 것은?
① 201 – Created
② 301 – Moved Permanently
③ 401 – Unauthorized
④ 501 – Bad Request

11. 다음 중 IP Spoofing 공격 활동으로 가장 옳지 않은 것은?
① SYN Flooding 공격
② slowloris 공격
③ RST를 이용한 접속 끊기
④ 순서번호 추측(Sequence number guessing)

12. 다음 중 ESM(통합보안솔루션)의 구성요소에 대한 설명으로 가장 옳지 않은 것은?
① 보안패치 : 최근 보안취약점이 발생한 시스템에 대해서 자동으로 패치를 수행한다.
② Manager : 수집된 로그정보를 통합하고 분석한다.
③ Console : 관리자는 ESM Console을 사용해서 모니터링하고 명령어를 실행한다.
④ Agent : 시스템에 설치되어서 각종 로그정보를 수집한다.

13. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

(㉠)는 웹 페이지에 입력되는 입력 값 검증 및 필터링 등을 수행하는 방화벽이다.
(㉡)는 모바일 단말에 대해서 소프트웨어 및 펌웨어를 관리하는 솔루션이다.
(㉢)는 네트워크 패킷을 탐지하고 대응까지 수행한다.

① ㉠ WAF(Web Application Firewall) ㉡ MDM ㉢ IPS
② ㉠ WAF(Web Application Firewall) ㉡ MAM ㉢ IDS
③ ㉠ Firewall ㉡ MDM ㉢ IDS
④ ㉠ Firewall ㉡ MAM ㉢ IPS

14. 다음 중 Spoofing의 종류로 가장 옳지 않은 것은?
① ARP Spoofing ② IP Spoofing
③ DNS Spoofing ④ ULU Spoofing

15. 다음 <보기>는 VPN에 대한 설명이다. ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

· IPSEC VPN은 (㉠) 단위로 데이터를 암호화 한다.
· SSL VPN은 (㉡) 단위로 데이터를 암호화 한다.

① ㉠ 프레임 ㉡ 데이터
② ㉠ 데이터 ㉡ 프레임
③ ㉠ 패킷 ㉡ 메시지
④ ㉠ 메시지 ㉡ 메시지

16. 다음 <보기>는 VLAN(Virtual Local Area Network)에 대한 설명이다. 다음 중 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

VLAN은 여러 개의 구별되는 (㉠) 도메인을 만들기 위해서 단일 2계층 네트워크를 (㉡)으로 분할하고 한 포트에서 보이는 모든 네트워크 패킷 혹은 전체 VLAN의 모든 패킷들을 다른 모니터링 포트로 복제하는 (㉢) 기능을 제공한다.

① ㉠ 유니캐스트 ㉡ 물리적 ㉢ 허브 미러링
② ㉠ 브로드캐스트 ㉡ 논리적 ㉢ 포트 미러링
③ ㉠ 유니캐스트 ㉡ 논리적 ㉢ 포트 미러링
④ ㉠ 브로드캐스트 ㉡ 물리적 ㉢ 허브 미러링

17. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

ANTI APT 솔루션에서 악성코드를 동적으로 분석하기 위해서 악성코드를 실행한 후에 행위 로그를 분석한다. 이때 악성코드 분석은 ( ) 환경에서 수행되어야 한다.

① SCADA ② Sandbox
③ Cloud ④ CRM

18. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

Tcpdump는 네트워크에서 전송되는 패킷을 스니핑하는 도구이다. 전송되는 패킷을 특정 포트로 (㉠), 스니핑 모드를 (㉡)(으)로 설정해야 한다.

① ㉠ 포트 미러링 ㉡ 정규 모드
② ㉠ 무차별 모드 ㉡ 포트 미러링
③ ㉠ 포트 미러링 ㉡ 무차별 모드
④ ㉠ 무차별 모드 ㉡ 정규 모드

19. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

IPv6는 (㉠)비트의 주소 공간을 가지며 헤더는 총 (㉡)개의 필드를 가지고 있다. 그리고 암호화와 (㉢)기능을 지원한다.

① ㉠ 128 ㉡ 8 ㉢ 인증
② ㉠ 32 ㉡ 4 ㉢ 인증
③ ㉠ 32 ㉡ 8 ㉢ 인가
④ ㉠ 128 ㉡ 4 ㉢ 인가

20. 다음 중 리눅스 시스템의 네트워크 관리 도구 및 서비스에 대한 설명으로 가장 옳지 않은 것은?

① ifconfig - 네트워크 인터페이스의 IP 주소 설정
② traceroute - 최종 목적지 컴퓨터까지 중간에 걸치는 여러 개의 라우터에 대한 경로 및 응답 속도를 표시
③ fping - 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 정보 출력
④ tcpdump - 네트워크 모니터링 및 패킷 분석을 위해 사용되는 도구로, 패킷 필터 기능을 통해서, 특정 침입자의 침입 경로에 따라 원하는 트래픽만을 감시