네트워크 보안

문 1. IPv6의 특성으로 옳지 않은 것은?

① 32Bit에서 128Bit로 확장된 주소 공간
② IP 주소의 동적 할당
③ 인증 및 보안 기능 지원
④ 헤더를 고정길이에서 가변길이로 변경

문 2. 다음에서 설명하는 통신규약은?

> ○ IETF에서 만든 공개키암호화 표준을 따름
> ○ PGP에 비해 보안성이 높지만 사용이 어려움
> ○ 전자우편 사용 시 전송하기 전에 자동으로 암호화하여 전송 도중 유출되어도 편지의 내용을 알 수 없음

① PPTP
② DNS
③ SNMP
④ PEM

문 3. 무선 LAN에서 사용하는 인증 프로토콜은?

① RIP
② EAP
③ BGP
④ SIP

문 4. Land 공격의 출발지 주소와 목적지 주소로 옳은 것은?

	출발지 주소	목적지 주소
①	192.168.0.1	192.168.0.1
②	192.168.0.1	192.168.0.200
③	192.168.0.5	192.168.0.1
④	192.168.0.5	192.168.0.200

문 5. 다음에서 설명하는 보안 기술은?

> ○ 외부 네트워크로부터의 공격 탐지에 중점을 두는 전사적 보안 관리(ESM) 기능에 내부의 정보 유출 탐지 영역까지 담당
> ○ ESM와 상호보완적인 관계로 다양한 정보시스템에 대한 로그 관리 및 분석이 강화되고 빅데이터 기술이 접목되어 정보시스템 전반에 대한 신속한 위협탐지가 가능한 지능형 로그 관리 플랫폼

① DLP
② NAC
③ SIEM
④ DRM

문 6. 포트 스캔에 대한 설명으로 옳지 않은 것은?

① TCP stealth 스캔은 정상적인 3-way handshake를 완성하지 않아 로그를 남기지 않는다.
② XMAS 스캔은 NULL 스캔과 반대로 모든 플래그를 설정하여 패킷을 전송한다.
③ NULL 스캔은 어떠한 플래그도 설정하지 않고 NULL 상태로 패킷을 전송한다.
④ UDP 포트 스캔은 3-way handshake 절차를 거쳐 수행한다.

문 7. Brute Force Attack에 대한 설명으로 옳지 않은 것은?

① 특정 단어 또는 문자 조합으로 성공할 때까지 대입을 시도해 원하는 계정 정보를 얻는다.
② 공격이 가능한 서비스는 Telnet, FTP 등이 있다.
③ 공격을 막는 방법에는 포트 변경, 패스워드 변경, 필터링 툴 사용 등이 있다.
④ 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격한다.

문 8. HMAC(Hashed MAC)에 대한 설명으로 옳지 않은 것은?

① RFC2004에서 정의된 HMAC은 수정 없이 이용 가능한 해시 함수를 사용하면 소프트웨어 구현이 어렵다.
② IP 보안을 위한 필수 구현 MAC으로 선택되어 TLS나 SET에서 사용된다.
③ 더 빠르고 안전 해시함수가 있거나 필요하다면 기존의 해시 함수를 쉽게 바꿀 수 있다.
④ 심각하게 기능 저하를 유발하지 않고 해시함수의 원래 성능을 유지하도록 한다.

문 9. 매체 접근 기법 중에서 유선망에서 사용되며, 호스트가 채널의 상태를 감지하여 충돌을 피하는 데이터 전송 방안은?

① Token Bus
② Carrier Sense Multiple Access with Collision Detection
③ Token Ring
④ Carrier Sense Multiple Access with Collision Avoidance

문 10. VLAN에 대한 설명으로 옳지 않은 것은?

① 물리적 장치의 이동이나 분리 없이 소프트웨어로 하나의 LAN으로 구현된다.
② 물리적인 세그먼트가 아닌 논리적인 세그먼트로 분할한다.
③ VLAN 멤버십 구성 정보로는 포트 번호, MAC주소, IP주소 등이 있다.
④ VLAN 표준으로 IEEE 802.3 부위원회에서 IP 태깅을 위한 IP 형식을 정의하는 802.3Q표준을 제정하였다.

문 11. OSI 7계층의 응용 계층 프로토콜로 옳지 않은 것은?

① FTP
② TCP
③ HTTP
④ SMTP

문 12. L2 스위치에 대한 설명으로 옳은 것은?

① OSI 2계층에서 기능을 수행하며, 고유 MAC 정보를 사용하여 통신한다.
② 패킷의 정보를 확인하여 가장 빠른 네트워크 IP 주소 경로를 찾아내 패킷을 전달한다.
③ 서로 다른 프로토콜 통신망 간에도 프로토콜을 변환하여 정보를 주고받을 수 있다.
④ 응용 계층까지 분석해서 높은 수준의 로드밸런싱을 수행한다.

문 13. 다음에서 설명하는 네트워크 기반 유틸리티는?

○ 네트워크 모니터링 및 패킷 분석을 위해 많이 사용
○ 패킷 수집을 위해 libpcap 라이브러리를 사용
○ 유닉스 및 윈도우즈 등에서 사용

① ping
② netstat
③ tcpdump
④ traceroute

문 14. 취약점을 악용해 공격을 수행하는 프로그램뿐만 아니라 공격 수행 절차, 스크립트 등을 의미하는 것은?

① Exploit
② Bell-LaPadula
③ Biba
④ IPSec

문 15. SSH에 대한 설명으로 옳은 것은?

① SSH는 TCP 및 UDP 기반의 보안 프로토콜이다.
② SSH 전송계층 프로토콜, SSH 인증 프로토콜, SSH 연결 프로토콜을 포함한다.
③ SSH는 SSH 터널링을 지원하지 않는다.
④ SSH 전송계층 프로토콜은 다수의 기본 SSH 연결을 사용하여 통신채널을 다중화한다.

문 16. DDoS 공격기법에 해당하지 않는 것은?

① Trin00
② TFN
③ MITM
④ Stacheldraht

문 17. 다음에서 설명하는 스위치 환경에서의 스니핑은?

○ 스위치에 저장 용량 이상의 MAC 주소를 보내 스위치 기능을 잃고 더미 허브처럼 동작하게 만드는 방식
○ 일부 고가 스위치는 MAC 테이블의 캐시와 연산 장치가 쓰는 캐시가 독립적으로 나뉘어 스니핑 공격이 통하지 않는 경우도 있음

① ICMP 리다이렉트
② SPAN 포트 태핑
③ 스위치 재밍
④ ARP 리다이렉트

문 18. IDS(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은?

① IDS는 네트워크기반 및 호스트기반의 침입탐지시스템으로 분류할 수 있다.
② 침입탐지 기법 중 오용탐지기법은 시그니처기반 탐지 또는 지식기반 탐지로 불린다.
③ 네트워크기반 침입탐지시스템은 네트워크 전반에 대한 감시를 할 수 있다.
④ 호스트기반 침입탐지시스템은 시스템의 로그에 대한 탐지보다는 네트워크 패킷을 수집하여 공격을 판단한다.

문 19. Wireshark에 대한 설명으로 옳지 않은 것은?

① 윈도우즈 운영체제만을 지원한다.
② www.wireshark.org에서 구할 수 있는 프로그램이다.
③ 네트워크 분석도구이다.
④ 트래픽 수집을 위해 WinPcap을 사용한다.

문 20. 네트워크 관리기능에 대한 설명으로 옳은 것은?

① 장애 관리 – 네트워크의 동작 및 효율성을 평가하는 기능
② 구성 관리 – 상호 연결 및 네트워크의 정보를 제공하는 기능
③ 성능 관리 – 비정상적인 동작을 발견하고 대처하는 기능
④ 보안 관리 – 자원 사용량과 관련이 있는 네트워크 데이터를 수집하는 기능