1. OSI 참조모델의 각 계층에서 사용하는 프로토콜로 가장 적절하지 <u>않은</u> 것은?

① 데이터링크 계층 : X.25, DNS
② 네트워크 계층 : ARP, IGMP
③ 전송 계층 : TCP, UDP
④ 응용 계층 : HTTP, SNMP

2. 다음 빈칸 (㉠)~(㉣)에 들어갈 용어로 가장 적절한 것은?

가상 메모리 관리 기법에서 메모리의 크기를 고정 크기로 분할하여 관리하는 것은 (㉠)이고, 가변 크기로 관리하는 것은 (㉡)이다. (㉠)으로 가상 메모리를 관리하면 메모리 단편화 중에서 (㉢)가 발생하고, (㉡)으로 가상 메모리를 관리하면 (㉣)가 발생한다.

	(㉠)	(㉡)	(㉢)	(㉣)
①	페이징	세그먼테이션	내부단편화	외부단편화
②	페이징	세그먼테이션	외부단편화	내부단편화
③	세그먼테이션	페이징	내부단편화	외부단편화
④	세그먼테이션	페이징	외부단편화	내부단편화

3. 리눅스 시스템에서 슈퍼유저의 권한으로 명령을 실행하기 위한 sudo 명령의 기본 보안 정책이 저장된 파일로 가장 적절한 것은?

① /etc/passwd
② /etc/shadow
③ /etc/groups
④ /etc/sudoers

4. 다음에서 설명하는 작업 스케줄 관리 명령어로 가장 적절한 것은?

예약한 명령어를 정해진 시간에 한 번만 실행할 때 사용하는 명령어이다.

① at
② find
③ cron
④ lsattr

5. 다음에서 설명하는 ICMP 오류 보고 메시지로 가장 적절한 것은?

- 이 메시지는 IP의 흐름제어와 혼잡제어 기능과 유사한 기능을 추가하기 위하여 설계되었다.
- 라우터나 호스트가 혼잡으로 인해 데이터그램을 폐기하게 되면, 데이터그램의 송신자에게 이 메시지를 보내게 되고, 이 메시지를 받은 송신자는 전송을 잠시 중단하거나 전송률을 줄이는 등의 조치를 하여야 한다.

① Redirect 메시지
② Source Quench 메시지
③ Destination Unreachable 메시지
④ Time Exceeded 메시지

6. 다음에서 설명하고 있는 HTTP 메소드로 가장 적절한 것은?

이 요청에 대한 응답은 원본 HTTP 요청의 사본을 포함하므로 클라이언트는 중간 서버로 변경된 내용을 확인할 수 있다. 일반적으로 웹 서버에서 이 요청은 보안 허점 역할을 할 수 있기 때문에 해제하는 것이 좋다.

① HEAD
② TRACE
③ OPTIONS
④ CONNECT

7. 다음 RAID에 대한 설명으로 적절한 것은 모두 몇 개인가?

가. RAID 1은 디스크 미러링으로 여러 디스크에 데이터를 완전 이중화하여 저장하는 방식으로 비용이 많이 발생한다.
나. RAID 3은 패리티 정보를 별도 디스크에 저장하고 데이터는 블록 단위로 데이터 디스크에 분산 저장한다.
다. RAID 5는 분산 패리티를 구현하여 안정성을 향상하고 일반적으로 4개의 디스크로 구성된다.
라. RAID 6은 패리티를 다중화하여 저장하고 장애가 발생된 상황에서 추가적인 디스크 장애가 발생해도 정상 동작한다.

① 1개
② 2개
③ 3개
④ 4개

8. ICMPv6에 추가된 기능으로 가장 적절하지 <u>않은</u> 것은?

① PMTUD(Path MTU Discovery)
② DSD(Duplicate Security Detection)
③ MLD(Multicast Listener Discovery)
④ NDP(Neighbor Discovery Protocol)

9. 다음 제로트러스트 네트워크에 대한 설명 중 빈칸 (㉠)에 들어갈 용어로 가장 적절한 것은?

(㉠)은 네트워크 트래픽을 기계적으로 관리하는 계층이다. 아주 빠른 속도로 트래픽을 처리하기 때문에 일반적으로 간단한 알고리즘을 사용하고, 경우에 따라 특별 제작된 하드웨어를 사용하여 알고리즘의 동작을 가속하기도 한다.

① 보안정책 엔진
② 트러스트 엔진
③ 컨트롤 플레인
④ 데이터 플레인

10. 리눅스 로그파일에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 현재 로그인한 사용자 정보는 로그인을 수행할 때 utmp 로그 파일에 로그인 정보가 기록된다.
② wtmp 로그는 로그인과 로그아웃 정보를 가지고 있는 로그 파일로 접속정보를 계속 기록하는 파일이다.
③ btmp 로그는 리눅스 로그인시 실패한 정보를 가지고 있는 로그파일로 텍스트 형태로 저장되어 vi 에디터를 실행하여 확인할 수 있다.
④ pacct 로그는 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보를 저장하는 로그이다.

11. 다음 빈칸 (㉠)에 들어갈 프로토콜로 가장 적절한 것은?

미국 국토안보부는 2013년 위협 정보를 전송하기 위한 위협 정보 표현 규격인 STIX와 위협 정보 전송 프로토콜인 (㉠)를 발표하였다. STIX는 사이버 위협 지능(CTI)을 교환하는데 사용되는 직렬화 형식의 언어이며, (㉠)는 이러한 사이버 위협 정보를 간단하게 확장할 수 있는 방식으로 통신하도록 해주는 프로토콜이다. (㉠)는 UTF-8로 인코딩된 JSON 형태로 데이터를 전송한다.

① BCP
② TAXII
③ PMS
④ SOAR

12. 이메일(e-mail) 요소와 설명이 가장 적절하지 <u>않은</u> 것은?

① MUA – 사용자 역할이나 사용자 응용 프로그램을 대표하며 이들을 위해 동작한다.
② MDA – MHS로부터 MS로 메시지 전달을 책임지고 수행한다.
③ MTA – 응용 프로그램 수준의 한 홉(hop)간에 메일을 중계한다.
④ MSA – 장기 메시지 저장소로 POP이나 IMAP을 이용해 원격서버에 있는 메시지를 검색한다.

13. 다음 NTFS 디스크 구조에 대한 설명으로 옳은 것을 모두 고른 것으로 가장 적절한 것은?

가. MBR은 파티션 생성시 물리적 디스크의 첫 번째 섹터에 위치하는 512 Bytes 크기의 영역이다. 나. VBR은 윈도우 부팅을 위한 기계어 코드와 볼륨 및 클러스터의 크기, MFT의 시작주소 등 설정 정보를 담고 있다. 다. MFT는 볼륨/파일시스템에 존재하는 모든 파일과 디렉토리에 대한 정보를 담고 있는 테이블이다.

① 가, 나
② 나, 다
③ 가, 다
④ 가, 나, 다

14. 다음에서 설명하는 용어로 가장 적절한 것은?

ㅇ 인터넷 사용자들이 비밀번호를 제공하지 않고 다른 웹사이트 상의 자신들의 정보에 대해 웹사이트나 애플리케이션의 접근권한을 부여할 수 있는 공통적인 수단으로 사용되는 접근 위임을 위한 개방형 표준이다. ㅇ 애플리케이션(페이스북, 구글, 엑스 등)의 사용자 비밀번호를 Third Party 앱의 제공 없이 인증, 인가할 수 있는 오픈 표준 프로토콜이다.

① OAuth
② JWT
③ SPF
④ BOOTP

15. 다음에서 설명하고 있는 취약점 진단 도구로 가장 적절한 것은?

이 취약점 진단 도구는 웹 취약점 스캐너 계열로 GPLv2 라이선스를 따르고 있어, 톰캣, 아파치, PHP 등 다양한 플랫폼의 기본 설정 파일들이 설치된 이후에 삭제되지 않고 남겨져 웹상에서 노출되고 있는지 스캔을 수행한다.

① Nikto
② Nmap
③ Arachni
④ OpenVAS

16. 다음에 출력된 내용의 밑줄 친 ㉠에 대한 설명으로 가장 적절한 것은?

```
[root@localhost~]#crontab -l
 - 생략 -
1 0 * * 2 root /home/clean.sh
          ㉠
```

① 매주 월요일 새벽 0시 1분에 /home/clean.sh 명령을 실행
② 매월 2일 새벽 0시 1분에 /home/clean.sh 명령을 실행
③ 매주 화요일 새벽 0시 1분에 /home/clean.sh 명령을 실행
④ 매일 새벽 0시 1분에 /home/clean.sh 명령을 실행

17. 다음에서 설명하는 것으로 가장 적절한 것은?

ㅇ 원격 호스트에 로그온하거나 원격 호스트에서 명령을 실행하고, 다른 호스트로 파일을 조작할 수 있게 해주는 응용 프로그램 또는 프로토콜이다.
ㅇ 암호화 통신을 하므로 노출되더라도 안전하다.
ㅇ 버전 2에서 서버와 클라이언트는 Diffie-Hellman 키 교환 방식을 사용한다.

① rsh
② ssh
③ rlogin
④ telnet

18. 다음 윈도우 레지스트리 루트키에 대한 설명으로 적절하지 <u>않은</u> 것은 모두 몇 개인가?

가. HKEY_CLASSES_ROOT(HKCR)는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 애플리케이션에 대한 맵핑 정보와 COM 오브젝트 등록 정보를 저장하고 있다.
나. HKEY_CURRENT_USER(HKCU)는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.
다. HKEY_LOCAL_MACHINE(HKLM)은 시스템이 시작할 때 사용하는 하드웨어 프로파일 정보를 저장하고 있다.

① 0개
② 1개
③ 2개
④ 3개

19. FTP와 TFTP의 차이점에 대한 설명으로 가장 적절한 것은?

① TFTP는 FTP와 같이 TCP 포트 21번을 사용한다.
② TFTP는 자체 디스크가 없는 워크스테이션의 부팅 이미지 전달에 주로 사용한다.
③ TFTP는 사용자명/비밀번호 방식의 간단한 인증을 제공한다.
④ TFTP는 파일을 받고, 보내고, 삭제하기 등을 위한 다양한 명령을 지원한다.

20. 다음 빈칸 (㉠)에 들어갈 프로토콜로 가장 적절한 것은?

(㉠)는 MAC 주소를 기반으로 클라이언트에게 IP 주소를 할당하는데, 공격자는 이 점을 악용하여 MAC 주소를 랜덤하게 변경하여 새로운 IP 주소를 할당받는다. 결국 (㉠)가 할당할 IP 주소가 모두 고갈되어, 정상적인 클라이언트는 IP 주소를 할당받지 못하게 된다. 대응 방법으로는 특정 스위치 포트에 지정된 MAC 주소만 접속을 허용하고, 조건에 일치하지 않는 MAC 주소는 차단해야 한다.

① ARP
② RARP
③ DHCP
④ BOOTP

21. 다음에서 설명하는 스팸 메일 보안 대응을 위한 이메일 인증 기술로 가장 적절한 것은?

발신 메일 서버 정보를 사전에 발신 도메인 DNS 서버에 공개적으로 등록함으로써, 수신자가 수신한 메일의 발신자 IP 주소가 발신자 메일 주소 도메인의 실제 메일 서버 정보와 일치하는지 검사할 수 있도록 하는 이메일 인증 기술이다.

① DKIM(Domain Keys Identified Mail)
② DNSSEC(DNS Security Extensions)
③ S/MIME(Secure/Multipurpose Internet Mail Extension)
④ SPF(Sender Policy Framework)

22. 파일에 setuid와 setgid 모두가 부여된 것을 찾는 find 명령으로 가장 적절한 것은?

① find / -perm +6000
② find / -perm +4000
③ find / -mtime -1
④ find / -mtime -2

23. 다음 접근제어목록(ACL) 규칙에 대한 설명으로 옳은 것을 모두 고른 것으로 가장 적절한 것은?

가. ACL의 위에서부터 아래로 수행된다.
나. 네트워크를 넓은 범위에서 좁은 범위로 설정해야 한다.
다. ACL의 마지막 줄은 'deny any'가 생략되어 있으므로, 마지막에 'permit any'가 없을 경우 모든 IP 주소는 차단된다.
라. Named ACL의 경우에는 중간 삽입, 삭제 및 추가가 가능하다.
마. 프로토콜, 방향, 인터페이스당 1개의 ACL만 적용 가능하다.

① 가, 나, 다, 라
② 가, 나, 다, 마
③ 가, 나, 라, 마
④ 가, 다, 라, 마

24. 인터넷 전자 메일의 표준 규약인 SMTP 프로토콜을 통해 메일 서비스를 하는 샌드메일(sendmail)의 주요 파일 중 스팸메일 및 Relay 차단을 위한 설정 파일로 가장 적절한 것은?

① /etc/spool/mail
② /etc/host.conf
③ /etc/mail/access
④ /usr/bin/sendmail

25. 시스템 취약점 분석 도구에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

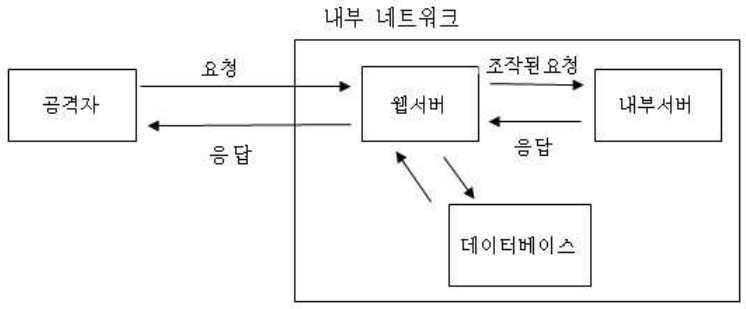
① SATAN – 해커와 동일한 방식으로 시스템에 침입하여 보안상의 약점을 찾아 보완할 수 있는 네트워크 분석용 보안 관리 도구이다.
② SARA – SATAN을 기반으로 개발된 취약점 분석 도구로 유닉스 플랫폼에서도 동작하고, HTML 형식의 보고서 기능이 있다.
③ Snort – 시스템 내부에 존재하는 취약점 점검 도구로 유닉스 시스템에서 동작하고 취약한 패스워드를 검사한다.
④ Nessus – 클라이언트/서버 구조로 취약점 검사를 수행하고, GUI 형태의 취약점 점검 설정 및 결과를 확인할 수 있다.

26. 다음 중 ping이 제공하는 정보만을 모두 고른 것으로 가장 적절한 것은?

가. 호스트의 도메인 이름을 입력하면 호스트의 IP 주소를 반환
나. 경로상의 문제점이 있는 네트워크 정보
다. 각 구간에 대한 접근성 및 네트워크 속도
라. 패킷이 돌아오는데 걸리는 시간
마. 방화벽이나 라우터에서의 필터링 여부
바. 경유 라우터의 IP 주소 및 도착 시간

① 가, 라
② 가, 나, 라
③ 가, 다, 라, 마
④ 가, 나, 다, 마, 바

27. 다음과 같이 공격자가 조작된 요청을 웹서버에 전송하여 내부 네트워크에 있는 다른 서버에 악의적인 요청을 보내는 공격으로 가장 적절한 것은?



① SQL Injection
② CSS(Cross Site Scripting)
③ CSRF(Cross Site Request Forgery)
④ SSRF(Server Side Request Forgery)

28. 다음에서 설명하는 웹 아티팩트 분석 대상으로 가장 적절한 것은?

다운로드 받은 이미지, 텍스트 파일, 아이콘 등을 가지고 있고, 다운로드 URL, 다운로드 시간, 데이터 크기 등의 정보를 가지고 있다.

① 웹 브라우저 캐시
② 히스토리 분석
③ 웹 브라우저 쿠키
④ 시스템 로그

29. LAND 공격 기법으로 가장 적절하지 <u>않은</u> 것은?

① 출발지와 목적지의 IP 주소를 동일하게 공격대상의 IP 주소로 변조하여 전송한다.
② 패킷의 시퀀스 넘버를 조작해 데이터 부분이 중첩되도록 전송함으로써, 재조립하는데 CPU 과부하를 유발한다.
③ 패킷을 수신한 시스템은 응답하기 위해 출발지 IP 주소를 참조하는데, 출발지 IP 주소가 자신의 IP 주소이기 때문에 자신에게 응답하게 되고 이 과정을 반복하게 하여 과부하를 유발한다.
④ 동시 사용자 수를 점유하고 루프 상태가 되도록 함으로써, 시스템 과부하를 유발한다.

30. 다음에서 OSI 참조모델의 물리 계층부터 응용 계층 순서로 공격을 나열한 것으로 가장 적절한 것은?

가. ARP Spoofing 공격
나. ICMP Redirect 공격
다. SQL Injection 공격
라. SYN Flooding 공격

① 가 - 나 - 다 - 라
② 가 - 나 - 라 - 다
③ 나 - 가 - 라 - 다
④ 나 - 다 - 가 - 라

31. 다음에서 설명하는 공격 방법으로 가장 적절한 것은?

ㅇ 공격대상에게 공격 트래픽을 전송할 때 라우터나 웹서버 같은 제 3자를 이용하여 출발지가 어디인지 알지 못하게 한다.
ㅇ 3 way-handshake 취약점 및 ICMP 프로토콜의 Echo Request/Echo Reply를 이용한다.
ㅇ 공격자의 IP 주소를 스푸핑하여 전송하기 때문에 대규모의 네트워크가 불필요하다.
ㅇ 경유지 서버 목록을 활용한다.

① Zero Day 공격
② Ransomware 공격
③ DRDoS 공격
④ APT 공격

32. 위협 정보 표현 규격(STIX, Structured Threat Information Expression)의 구성 항목으로 가장 적절하지 <u>않은</u> 것은?

① SDO(STIX Domain Objects)
② SAO(STIX Attribute Objects)
③ SCO(STIX Cyber-observable Objects)
④ SRO(STIX Relationship Objects)

33. 취약점 점수 시스템 CVSS 3.1의 기본 측정 항목 중 공격 경로(Attack Vector)의 값으로 가장 적절하지 <u>않은</u> 것은?

① Local
② Network
③ Physical
④ System

34. 다음에서 설명하는 윈도우 암호화 기능으로 가장 적절한 것은?

ㅇ 드라이브를 암호화하는 기능으로 디스크 전체 볼륨을 암호화한다.
ㅇ 윈도우 파티션, USB 플래시 드라이브 등 파티션 전체를 암호화한다.
ㅇ PC의 모든 사용자 계정을 암호화하고 TPM 하드웨어를 사용한다.

① VSS
② EFS
③ BitLocker
④ Quotas

35. 다음에서 설명하는 것으로 가장 적절한 것은?

ㅇ 불특정 다수가 아닌 특정기관이나 기업의 내부직원을 목표로 삼아 집중적으로 공격하는 행위를 말한다.
ㅇ 정부기관이나 기업조직 등 특정목표의 내부 사용자를 은밀히 염탐하고 해당 조직의 기밀정보를 빼내기 위하여, 신뢰할 수 있는 내용처럼 위장한 악성 이메일(악성 링크나 악성 코드를 삽입)을 관련자들에게 전송하여 감염시킨다.
ㅇ 이후 원격제어 및 데이터 탈취 등을 시도하는 대표적인 지능형 공격이다.

① 랜섬웨어
② 애드웨어
③ 메신저 피싱
④ 스피어 피싱

36. HTTP 요청과 응답시 헤더정보에 공통으로 들어가는 항목으로 가장 적절한 것은?

① Authorization
② Referer
③ Connection
④ Location

37. /etc/shadow 파일 정보에 대한 설명으로 가장 적절하지 <u>않은</u> 것은?

root: 6p4Hf~중략~T9g/: <u>14923</u>: <u>0</u>: <u>99999</u>: <u>7</u>: : :
㉠ ㉡ ㉢ ㉣

① ㉠은 1970년 1월 1일부터 마지막으로 패스워드를 변경한 날까지의 일 수이다.
② ㉡은 패스워드를 변경하기 전에 최소 사용 기간의 일 수이다.
③ ㉢은 패스워드를 변경하지 않고 최대한 사용할 수 있는 기간의 일 수이다.
④ ㉣은 계정의 사용 제한을 결정하고 며칠 후에 완전히 사용을 정지할지 설정한다.

38. 스위치 환경에서의 스니핑(Sniffing)과 관련된 공격으로 가장 적절하지 <u>않은</u> 것은?

① IP Spoofing
② Switch Jamming
③ ARP Spoofing
④ ICMP Redirect

39. 다음에서 설명하는 SYN Flooding 대응 방법으로 옳은 것을 모두 고른 것으로 가장 적절한 것은?

가. IP당 SYN 요청에 대한 PPS(Packet per Second) 임계치를 단계적으로 조정한다.
나. SYN 패킷을 보낸 클라이언트의 존재 여부를 파악하여 차단한다.
다. 트래픽 유형별 임계치를 조정하여 TCP 세션 연결을 차단한다.
라. 임시적 방법으로 서버의 Queue 크기를 감소시킨다.

① 가, 나
② 가, 다
③ 가, 나, 다
④ 가, 나, 다, 라

40. 세션 하이재킹(Session Hijacking)의 탐지방법으로 가장 적절하지 <u>않은</u> 것은?

① 서버와 순서번호를 주기적으로 검사하여 비동기화 상태인지 탐지한다.
② 전송 중 윈도우 크기와 순서번호가 맞지 않는 상태가 되면 교정 패킷이 정상적으로 동작하지 못하게 되어, 무한루프에 빠지기 때문에 ACK 패킷의 비율이 감소하는지 탐지한다.
③ 공격자가 중간에 끼어있기 때문에 패킷의 유실과 재전송 발생, 서버와의 응답 시간이 증가하는지 탐지한다.
④ 접속 초기에 예상하지 못한 세션의 리셋이 발생하는지 탐지한다.