1. 다음에서 설명하는 윈도우 인증 구성 요소로 가장 적절한 것은?

> ○ 사용자, 그룹 계정 정보에 대한 데이터베이스를 관리한다.
> ○ 사용자의 로그인 입력 정보와 데이터베이스 정보를 비교하여 일치 여부를 확인한다.

① SAM(Security Account Manager)
② SRM(Security Reference Monitor)
③ SMB(Server Message Block)
④ LSA(Local Security Authority)

2. 다음 빈칸 (㉮)에 들어갈 용어로 가장 적절한 것은?

> (㉮)은/는 기존 운영체제에 내재된 보안상의 결함으로 인한 각종 침해로부터 시스템을 보호하기 위해 기존의 운영체제 내에 추가로 이식되어 사용자의 모든 접근 행위를 안전하게 통제하는 역할을 수행한다. (㉮)의 주요 요구조건은 보안 경계 내의 모든 주체와 객체를 통제할 수 있어야 하고, 프로세스, 파일 시스템, 메모리 관리, 입출력을 위한 자원을 제공해야 한다.

① 접근 제어
② 보안 커널
③ 침입 탐지
④ 사용자 인증

3. 보안 취약점 공격에 관한 설명으로 가장 적절한 것은?

> ○ 취약점에 대해 아직 알려지지 않았을 때 이루어지는 공격이다.
> ○ 취약점이 알려졌어도 패치가 발표되지 않은 시점에 이루어지는 공격이다.

① 제로데이(0-day) 공격
② 원데이(1-day) 공격
③ 투데이(2-day) 공격
④ 올데이(Olday) 공격

4. 리눅스 특수 권한에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① Set-UID가 부여된 파일(file-A)이 실행되는 동안에는 실행시킨 사용자의 권한이 아닌 해당 파일(file-A)의 소유자 권한으로 인식된다.
② Set-GID 권한의 표시는 그룹 허가권에 실행 권한이 없을 경우 대문자 S로 표시된다.
③ Sticky-Bit는 공유를 목적으로 파일에 설정되는 특수 권한으로서 이 권한의 표시는 other 허가권의 실행 권한 자리에 t로 표시된다.
④ 특수 권한 설정은 chmod 명령을 사용하며, 8진수 모드로 Set-UID는 4, Set-GID는 2, Sticky-Bit는 1을 갖는다.

5. 다음 중 스니핑(Sniffing)과 관련된 공격으로 가장 적절하지 <u>않은</u> 것은?

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

6. TCP에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① TCP 연결 설정의 주요 목적은 송수신 호스트간 데이터 전달 시 사용할 초기 순서 번호를 동기화하는 것이다.
② TCP SYN 플러딩(flooding)에 의한 서비스 거부 공격의 취약점이 있다.
③ 데이터가 오류 없이 목적지 호스트에 도착했는지 확인하기 위한 방법 중의 하나로 재전송타이머를 사용할 수 있다.
④ 목적지 호스트에서 TCP 세그먼트(segment)들을 재조합하는 과정의 취약점을 이용하여 Teardrop 공격이 가능하다.

7. 리눅스/유닉스의 주요 로그 파일 <보기 1>과 설명 <보기 2>를 가장 적절하게 연결한 것은?

< 보기 1 >

㉮ utmp(x)
㉯ wtmp(x)
㉰ loginlog
㉱ pacct

< 보기 2 >

㉠ 실패한 로그인 시도에 대한 정보를 저장하는 로그로서 기본으로 제공하지 않는다.
㉡ 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보를 저장하는 로그이다.
㉢ 사용자의 로그인, 로그아웃, 시스템 재부팅 정보를 저장하는 로그이다.
㉣ 현재 시스템에 로그인한 사용자 상태를 저장하는 로그이다.

	㉮	㉯	㉰	㉱
①	㉢	㉣	㉡	㉠
②	㉢	㉠	㉣	㉡
③	㉣	㉡	㉢	㉠
④	㉣	㉢	㉠	㉡

8. 스택 가드에서 CR(0x0d), LF(0X0a), EOF(0xff) 등을 조합해서 canary 값을 만드는 기술로 가장 적절한 것은?

① Null canary
② Return canary
③ Random canary
④ Terminator canary

9. 포트 포워딩(port forwarding)에 관한 설명 중 가장 적절한 것은?

① 일반적인 TCP 연결을 보안상 안전한 SSH(버전2) 연결로 변환하는 서비스
② 보안상 Well-known 포트 번호를 임시 포트 번호로 전환하는 절차
③ 한 포트에서 다른 포트로 메시지를 전달하는 데 사용되는 프로토콜
④ 공격 대상 호스트에서 서비스가 활성화되어 있는 포트를 찾아 연결하는 것

10. HTTP 요청 메소드에 대한 설명 중 가장 적절하지 <u>않은</u> 것은?

① GET : 서버가 자원을 전송해 줄 것을 요청
② PUT : 클라이언트가 서버의 URI로 자원을 전송
③ TRACE : 클라이언트와 서버간에 터널링 목적으로 사용
④ OPTIONS : 자원에 관련된 선택 사항의 정보를 요청할 때 사용

11. 다음 중 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

㉮ 인터넷의 라우터 보안을 위해 정적 라우팅(static routing)은 필수적으로 사용되어야 한다.
㉯ S/MIME은 X.509에 정의된 인증기관에 의해 서명된 공개키 인증서를 사용한다.
㉰ RTP(Real-time Transport Protocol)를 이용하여 VPN을 제공할 수 있다.
㉱ SSO(Single Sign On)는 효율적인 인증관리를 가능하게 한다.
㉲ LAN 카드의 'promiscuous' 모드 설정은 패킷 필터링 기능을 해제하는 것이다.

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

12. 레이스 컨디션 공격에 필요한 조건을 모두 고른 것으로 가장 적절한 것은?

㉮ 공격 대상 프로그램의 소유자는 root이어야 한다.
㉯ 공격 대상 프로그램은 Set-UID가 설정되어 있어야 한다.
㉰ 생성되는 임시 파일의 이름을 알고 있어야 한다.

① ㉮, ㉯
② ㉮, ㉰
③ ㉯, ㉰
④ ㉮, ㉯, ㉰

13. 다음에 출력된 리눅스의 /etc/shadow 파일에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

```
[root@localhost ~]# tail  -1 /etc/shadow

tester:$6 $1Tkc0bAR $GFtu6중략HF9tyE:16570:30:99999:7:::
       ㉮     ㉯              ㉰          ㉱
```

① ㉮ : 사용자 패스워드 암호화에 사용된 MD5 해시 알고리즘을 나타낸다.
② ㉯ : 해시 값을 생성할 때 사용된 솔트를 나타낸다.
③ ㉰ : 사용자 패스워드에 솔트를 조합하여 해시한 암호화된 패스워드를 나타낸다.
④ ㉱ : 패스워드를 바꾼 후 최소로 사용해야 되는 날짜 수를 나타낸다.

14. 스텔스 스캔 방법으로 가장 적절한 것을 모두 고른 것은?

㉮ TCP Open 스캔
㉯ NULL 스캔
㉰ XMAS 스캔
㉱ UDP 스캔

① ㉮, ㉯
② ㉮, ㉰
③ ㉯, ㉰
④ ㉯, ㉱

15. APT(Advanced Persistent Threat) 공격단계를 예를 들어 나열한 것으로 가장 적절한 것은?

① 침입(사회공학)-운영방해(권한상승)-유출(지속적인 분석)-기밀데이터 검색(은밀한 활동)
② 침입(사회공학)-기밀데이터 검색(은밀한 활동)-운영방해(권한상승)-유출(지속적인 분석)
③ 기밀데이터 검색(은밀한 활동)-침입(사회공학)-운영방해(권한상승)-유출(지속적인 분석)
④ 기밀데이터 검색(은밀한 활동)-유출(지속적인 분석)-침입(사회공학)- 운영방해(권한상승)

16. FTP에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① FTP는 명령 전달을 위한 제어 연결과 데이터 전달을 위한 데이터 연결을 분리하여 사용한다.
② FTP 클라이언트가 FTP 서버에 접속한 후 LIST 명령을 이용하여 파일 목록을 수신하고 그 중 1개의 파일을 다운로드 받으려면 1개의 데이터 연결이 필요하다.
③ FTP 응용계층과 전송계층 사이에 TLS/SSL을 추가하면 보안상 안전한 데이터 전송이 가능하다.
④ PASV 명령을 사용하면 FTP 서버가 데이터 연결을 위한 FTP 클라이언트 측 포트를 선택할 수 있다.

17. 윈도우 NTFS의 디렉터리 및 파일 접근 권한 설정 규칙을 모두 고른 것으로 가장 적절한 것은?

㉮ NTFS 접근 권한은 누적되지 않는다. ㉯ 파일 접근 권한이 디렉터리 접근 권한에 우선한다. ㉰ 거부가 허용보다 우선한다.

① ㉮, ㉯ ② ㉮, ㉰
③ ㉯, ㉰ ④ ㉮, ㉯, ㉰

18. 다음 설명에 관한 기술로 가장 적절한 것은?

○ 버퍼 오버플로가 일어날 가능성이 있는지, 암호화 알고리즘에 취약점이 없는지 등을 분석할 수 있다. ○ 소프트웨어에 버그가 발생했을 때 원인을 파악하기 위해 사용할 수 있다. ○ 불법적인 사용자가 소프트웨어 사용 제한 기능 등을 제거하기 위해 사용할 수 있다. ○ 공격자가 배포한 악성코드의 원리를 분석하고 대응 방안을 만들기 위해 사용할 수 있다.

① 샌드박스(Sand Box)
② 16진수 편집기
③ 리버스 쉘(Reverse Shell)
④ 리버스 엔지니어링(Reverse Engineering)

19. 다음 보안 공격들의 공통점으로 가장 적절한 것은?

SYN Flooding, Smurf, Land

① ICMP 패킷을 이용한다.
② TCP 프로토콜의 취약점을 이용한다.
③ 발신지 IP 주소를 위조한다.
④ IP 데이터그램 단편화를 이용한다.

20. 무선 네트워크 보안 취약점에 관한 설명에 부합하는 위협으로 가장 적절한 것은?

○ 공격자가 무선 네트워크를 식별하기 위한 SSID를 모니터링하여 접속한다. ○ 공격자가 인증절차가 없는 취약한 AP를 찾아 접속한다. ○ MAC 필터링 기반 인증방법을 사용하는 환경에서 정상 사용자와 AP와의 통신 간 정보를 공격자가 수집하여 무선 네트워크에 접속한다.

① 도청 ② DDoS ③ 불법 AP ④ 비인가 접근

21. 발신지 호스트(source host)에서 다른 네트워크의 목적지 호스트(destination host)로 패킷이 전달되는 과정에서 패킷 내의 각종 주소의 변화에 관한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

㉮ 2계층 스위치를 통해 전달될 때 발신지 MAC 주소와 목적지 MAC 주소는 모두 변경된다. ㉯ 라우터를 통해 전달될 때 발신지 물리주소와 목적지 물리주소는 모두 변경된다. ㉰ 라우터를 통해 전달될 때 발신지 IP 주소와 목적지 IP 주소는 그대로 유지된다. ㉱ 라우터를 통해 전달될 때 발신지 포트 주소와 목적지 포트 주소는 그대로 유지된다.

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

22. 공급망 공격(Supply Chain Attack)에 대한 설명으로 가장 적절한 것은?

① 거래처 등에 위장 E-mail을 전송하여 공격자 계좌로 금전 입금을 유도한다.
② E-mail을 통해 배포된 워드 파일에 심은 매크로로 감염시킨다.
③ 침입한 컴퓨터의 공식도구나 윈도우 표준 명령어로 공격한다.
④ 패치를 배포하는 서버에 침입하여 정식 패치 등에 맬웨어(Malware)를 심는다.

23. 80386 레지스터의 용도에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① EAX : 입출력과 산술 연산에 사용한다.
② ECX : 루프가 반복되는 횟수나 좌우 방향 시프트 비트 수 저장에 사용한다.
③ EBP : 스택 세그먼트에서 현재 호출되어 사용하는 함수의 시작 주소 값 저장에 사용한다.
④ ESP : 다음 명령어의 오프셋을 저장하며, CS 레지스터와 합쳐 다음에 수행할 명령 주소를 형성한다.

24. Codenomicon사 연구진이 발견한 OpenSSL 암호화 소프트웨어 라이브러리의 심각한 보안 취약점으로 가장 적절한 것은?

① 넷버스(Netbus)
② 스쿨버스(Schoolbus)
③ 루트킷(Rootkit)
④ 하트블리드(Heartbleed)

25. E-mail 보안 기술에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① PGP는 인증서 없이 E-mail 메시지의 인증, 기밀성, 무결성 등을 제공할 수 있다.
② 메시지 송신자는 메시지에서 사용된 암호 알고리즘이나 식별자를 메시지 내에 포함할 필요가 있다.
③ 암호화와 복호화는 대칭키 알고리즘을 사용하여 수행되며 암호화된 메시지를 복호화하기 위해 필요한 비밀키는 메시지 수신자의 공개키로 암호화되어 메시지와 함께 전송된다.
④ S/MIME은 RSA 보안 기술에 기반하여 MIME의 보안 기능을 개선한 E-mail 보안 기술이다.

26. DDoS 대응방식에 관한 설명 중 옳은 것을 모두 고른 것으로 가장 적절한 것은?

㉮ In-Line 방식은 DDoS 공격을 탐지하고 직접 차단하며 가장 많이 구축되는 방식이다.
㉯ In-Line 방식은 DDoS 대응장비에 장애가 있어도 네트워크 가용성에는 영향이 없다.
㉰ Out of Path 방식은 In-Line 방식에 비해 구축 비용이 일반적으로 많이 든다.
㉱ Out of Path 방식은 미러링 장비를 통해 복제된 패킷을 받아 DDoS 대응장비에서 분석 차단한다.

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

27. 다음 윈도우 SID 출력 내용에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

SID for WIN_2016\administrator
<u>S-1</u>-<u>5-21</u>-<u>3927844882-394592529-3216461276</u>-<u>500</u>
㉮ ㉯ ㉰ ㉱

① ㉮ : 해당 시스템이 윈도우 시스템임을 의미한다.
② ㉯ : 시스템의 사용자 계정 유형(관리자, Guest, 일반 사용자)을 나타낸다.
③ ㉰ : 시스템의 고유한 숫자로, 시스템을 설치할 때 이것의 특성을 수집하여 생성한다.
④ ㉱ : 숫자로 표현하는 각 사용자의 고유한 ID이다.

28. 사이버 킬 체인은 사이버 공격을 프로세스 기반으로 분석하여 단계별로 가해지는 위협 요소를 파악하고 공격을 완화할 목적으로 수행되는 사이버 공격 분석 모델이다. 공격단계를 순서대로 나열한 것으로 빈칸 (㉮)~(㉱)에 가장 적절한 것은?

[공격단계]
정찰 - (㉮) - (㉯) - (㉰) - (㉱) - 명령&제어 - 실행

	㉮	㉯	㉰	㉱
①	무기화	설치	전달	익스플로잇
②	무기화	전달	설치	익스플로잇
③	무기화	익스플로잇	전달	설치
④	무기화	전달	익스플로잇	설치

29. CSRF(Cross-Site Request Forgery) 공격에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① HTTP GET과 HTTP POST 서비스의 차이에 따라 CSRF 공격 방법도 차이가 있다.
② 피해자가 타겟 웹 사이트로 전송되는 사이트 간 요청을 위조할 수 있는 악성 웹 페이지를 방문하여야 한다.
③ CSRF 공격이 성공하기 위해서는 피해자가 악성 웹 페이지 방문 후 타겟 웹 사이트와 세션을 확립하여야 한다.
④ 일반적인 대응책은 HTTP 요청이 자체 웹 페이지에서 오는지 아니면 제3자의 웹 페이지에서 오는지 구별하는데 도움이 되는 비밀 토큰 등을 이용하는 것이다.

30. 리눅스 시스템에서 다음과 같은 실행 결과를 출력하는 가장 적절한 명령어는?

Filesystem	1K-blocks	Used	Avail	Use%	Mounted on
/dev/sda2	91871**	4977***	3743***	58%	/

① #mount -t
② #df -k
③ #du -k
④ #repquota -a

31. 컨테이너화된 응용프로그램의 보안에 관한 설명으로 가장 적절하지 <u>않은</u> 것은?

① 컨테이너 안에서는 호스트의 파일 시스템 전체를 볼 수 없다.
② 컨테이너는 호스트 컴퓨터의 커널을 공유한다.
③ 컨테이너 격리는 기본적으로 VM 격리보다 강하다.
④ 컨테이너 방화벽은 규칙에서 벗어난 네트워크 연결 시도를 기록하고 보고한다.

32. 단편화(fragmentation)가 수행된 IP 데이터그램의 한 조각(fragment)의 필드 값들이 다음과 같을 때의 설명으로 가장 적절한 것은?

헤더 길이=5, 전체 길이=1020, 식별자(identification)=49153 플래그의 M비트=1, 단편화 오프셋=340

① 다음 조각의 단편화 오프셋은 465이다.
② 두 번째 조각이며, 다음 조각의 식별자는 49154가 된다.
③ 중간 조각이며, 다음 조각이 마지막 조각이 된다.
④ 동일한 식별자를 갖는 단편화된 조각들은 최종 목적지의 라우터에서 재조합된다.

33. 유닉스의 traceroute에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① traceroute의 메시지는 UDP 데이터그램에 캡슐화되며 목적지 호스트에서 사용하지 않는 포트 번호를 사용한다.
② 목적지 호스트까지의 경로상에 있는 라우터들에 의해 발송되는 ICMP Time Exceeded 메시지와 ICMP Destination Unreachable 메시지를 사용한다.
③ 목적지 호스트까지의 경로상에 있는 라우터들의 개수가 n개라면 최대 (n+1)개의 ICMP 오류 보고 메시지를 수신하게 된다.
④ traceroute는 각 라우터와 목적지 호스트까지의 왕복 시간을 알기 위해 타이머를 설정한다.

34. 안전한 소프트웨어 개발 운영을 목표로 하는 안전성 분석기법을 설명한 것으로 빈칸 (㉮)와 (㉯)에 가장 적절한 것은?

(㉮) : 인터페이스 및 함수 호출의 구조적 취약점 분석 (㉯) : 가상화 환경에서 직접 실행을 통해 이상 현상 분석

	㉮	㉯
①	소스코드 분석기법	샌드박스 분석기법
②	시멘틱 분석기법	행위탐지 분석기법
③	샌드박스 분석기법	바이너리 분석기법
④	시멘틱 분석기법	샌드박스 분석기법

35. 다음 설명에 관한 것으로 가장 적절한 것은?

○ 외부로부터의 접근이 가능하지만 어느 정도의 보호가 필요한 시스템들이 자리 잡고 있다. ○ 보통 웹 서버, E-mail 서버, DNS 서버 등을 둔다. ○ 외부 방화벽은 외부 연결의 필요성과 일치되는 수준 정도의 접근 제어와 보호를 수행한다. ○ 내부 방화벽은 내부의 서버와 워크스테이션들을 보호하기 위해 외부 방화벽보다 엄격한 필터링 규칙을 적용한다.

① 허니넷(Honey Net)
② 인트라넷(Intranet)
③ DMZ(Demilitarized Zone)
④ 응용 레벨 게이트웨이(Application-level Gateway)

36. 비즈니스 스캠(SCAM)은 E-mail을 해킹하여 거래 결제 시점에 바이어에게 결제 은행이 변경되었다는 E-mail을 송부하고 결제 대금을 가로채는 수법이다. 공격 절차를 나열한 것으로 가장 적절한 것은?

① E-mail 스푸핑 - 스팸 메일로 감염 - 유사 E-mail 생성 - MITM(중간자) 공격
② 스팸 메일로 감염 - 유사 E-mail 생성 - MITM(중간자) 공격 - E-mail 스푸핑
③ 스팸 메일로 감염 - MITM(중간자) 공격 - E-mail 스푸핑 - 유사 E-mail 생성
④ 유사 E-mail 생성 - MITM(중간자) 공격 - 스팸 메일로 감염 - E-mail 스푸핑

37. 다음에서 설명하는 DEP(Data Execution Prevention) 우회 방법으로 가장 적절한 것은?

○ DEP를 우회하기 위해 사용되는 함수들은 메모리와 관련된 함수이며, 이러한 함수를 호출하기 위해서는 쉘코드 주소, 크기 등 적절한 인자값이 필요하다. 이러한 인자값을 구성하고 함수를 호출하기 위해서 사용되는 기술이다. ○ RET로 끝나는 명령 조각들인 가젯(Gadget)의 체인(Chain)을 만들어서 원하는 코드 조각들을 여러 번 실행하게 된다.

① ROP
② RTL
③ ASLR
④ DEP 비활성화

38. iptables 명령어에서 체인에 설정된 정책정보를 모두 제거하는 옵션으로 가장 적절한 것은?

① iptables -L
② iptables -nL
③ iptables -vL
④ iptables -F

39. IPSec의 전송모드(transport mode)에 관한 설명 중 가장 적절하지 <u>않은</u> 것은?

① 일반적으로 데이터를 호스트-대-호스트로 보호할 때 사용한다.
② 전송모드의 IPSec 헤더와 트레일러는 데이터링크(이더넷) 프레임에 직접 캡슐화된다.
③ 송신 호스트는 전송계층으로부터 전달된 페이로드만 보호한다.
④ 터널 모드(tunnel mode)와는 다르게 하나의 IP 헤더만 생성하여 사용한다.

40. 사회공학적 공격 흐름에서 단계별 공격방법으로 가장 적절한 것은?

[공격흐름]
정보수집단계(㉮) - 관계형성단계(㉯) - 공격단계(㉰) - 실행단계(㉱)

	㉮	㉯	㉰	㉱
①	인터넷	인물 위장	감정에 호소	도덕적 의무감 유발
②	인터넷	인물 위장	도덕적 의무감 유발	감정에 호소
③	인물위장	감정에 호소	인터넷	도덕적 의무감 유발
④	인물위장	인터넷	도덕적 의무감 유발	감정에 호소