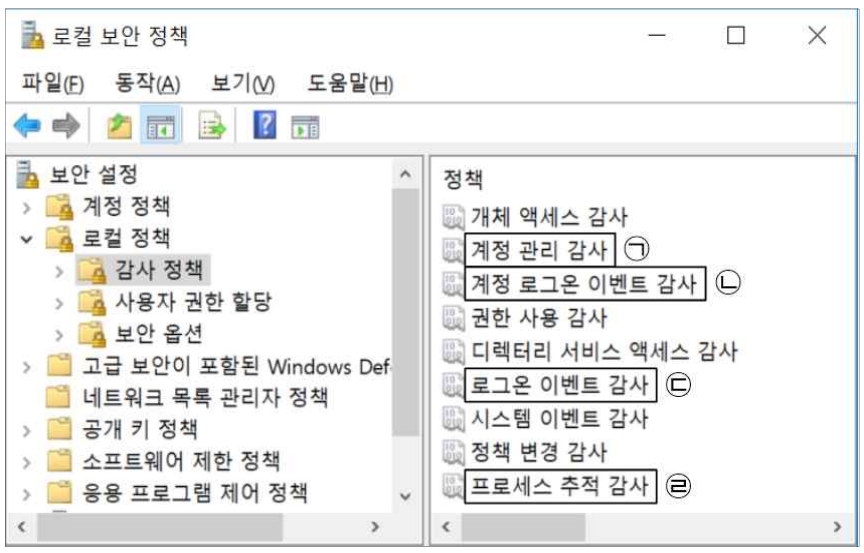
【시스템네트워크보안】

1. Linux의 i-node가 가지고 있지 **않은** 정보는?
① 파일의 이름 ② 파일의 유형
③ 파일의 링크 수 ④ 마지막으로 수정된 시간

2. IANA가 정한 사설 IP 주소로 사용하기에 옳지 **않은** 것은?
① 10.0.0.0 - 10.255.255.255
② 172.16.0.0 - 172.31.255.255
③ 192.168.0.0 - 192.168.255.255
④ 220.83.33.0 - 220.83.33.255

3. 다음 그림에서 Windows 감사 정책에 관한 설명으로 가장 적절하지 **않은** 것은?



① ㉠ 계정 관리 감사 : 사용자 계정 또는 그룹의 생성/변경/삭제, 사용자 계정의 이름 변경 및 설정 등을 감사한다.
② ㉡ 계정 로그온 이벤트 감사 : 사용자 권한 할당 정책, 감사 정책, 계정 정책 또는 트러스트 정책을 변경하려는 각 인스턴스를 감사한다.
③ ㉢ 로그온 이벤트 감사 : 각 사용자 로그온 또는 로그오프 인스턴스를 감사한다.
④ ㉣ 프로세스 추적 감사 : 프로세스 생성/종료, 핸들 복제 및 간접 개체 액세스 같은 프로세스 관련 이벤트를 감사한다.

4. NAT(Network Address Translation) 기술에 관한 설명으로 가장 적절하지 **않은** 것은?
① NAT는 사설 IP 주소와 공인 IP 주소를 서로 매핑할 수 있다.
② NAT는 IPv4 주소 고갈문제를 완화할 수 있다.
③ NAT를 사용하면 네트워크 속도가 향상된다.
④ NAT를 사용하면 내부 시스템의 네트워크 구조를 노출하지 않는 보안상 이점을 제공한다.

5. APT(Advanced Persistent Threat) 공격 행위로 가장 적절한 것은?
① 공격자는 봇넷에 명령을 전달하여 대규모의 트래픽을 유발시키거나 취약한 서버를 악용하여 공격을 수행한다.
② 공격자는 인증 작업 등이 완료되어 정상적으로 통신이 이루어지고 있는 다른 사용자의 세션을 가로채서 별도의 인증 없이 가로챈 세션으로 통신한다.
③ 공격자는 공격대상을 특정하고 네트워크에 침투하여 거점을 마련한 뒤, 제로데이 공격과 같은 기존에 알려지지 않았던 취약점을 이용하여 공격한다.
④ 공격자는 컴퓨터 시스템에 저장된 사용자 파일을 암호화하거나 컴퓨터 시스템을 잠그고 금전을 요구한다.

6. 데이터 링크 계층의 프레임에서 사용되는 6bytes 크기의 주소로 제조사에 의해 할당되며, 홉에서 홉으로 갈 때마다 변경되는 주소로 가장 적절한 것은?
① 논리 주소 ② 물리 주소
③ IP 주소 ④ 포트 주소

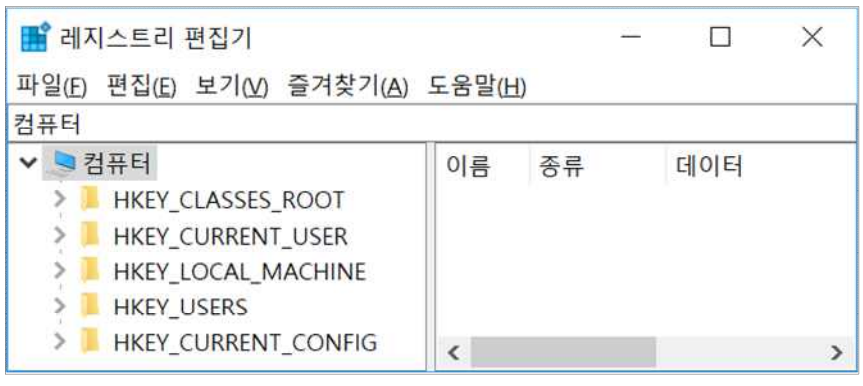
7. 다음 소스코드의 빈칸 ㉠에 들어갔을 때 버퍼 오버플로우 공격이 발생할 수 있는 함수로 가장 적절한 것은?

```
#include <stdio.h>
void main()
{
      char buffer[100];
      ㉠ (buffer);
      printf("%s\n",buffer);
}
```

① vfscanf ② strncat
③ gets ④ snprintf

8. DoS 공격에 관한 설명으로 가장 적절하지 **않은** 것은?
① SYN Flooding 공격은 다량의 SYN 패킷을 전송하여 시스템의 부하를 발생시킨다.
② Teardrop 공격은 패킷 단편화를 이용하는 공격으로 시퀀스 넘버를 조작하여 공격한다.
③ Smurf 공격은 IGMP 패킷을 사용하여 공격을 수행한다.
④ Ping of death 공격은 ping을 이용하여 패킷을 정상 크기보다 크게(최대 65,535바이트) 만들어 전송하는 공격이다.

9. Windows 레지스트리 루트키에 관한 설명으로 가장 적절한 것은?



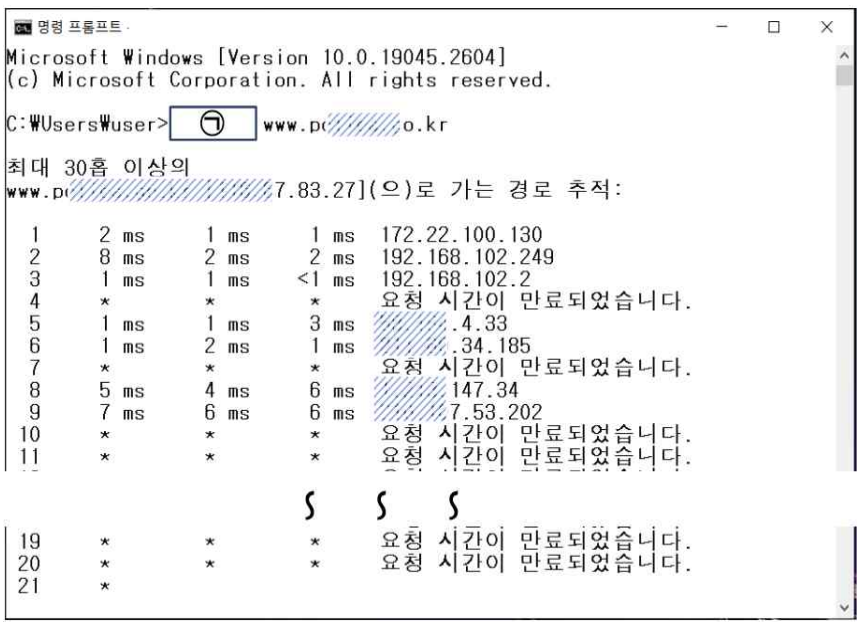
① HKEY_CLASSES_ROOT : 파일의 각 확장자에 대한 정보와 파일과 프로그램 간의 연결에 대한 정보를 저장한다.
② HKEY_CURRENT_USER : 시스템 관련 전체 정보를 저장한다.
③ HKEY_USERS : 현재 로그온 된 사용자와 관련된 데이터만 저장한다.
④ HKEY_CURRENT_CONFIG : 설치된 하드웨어와 하드웨어를 구동시키는 데 필요한 드라이버 설정에 대한 정보를 저장한다.

10. ICMP 오류 보고 메시지로 가장 적절하지 **않은** 것은?
① ICMP Parameter Problem 메시지
② ICMP Echo Request 메시지
③ ICMP Time Exceeded 메시지
④ ICMP Destination Unreachable 메시지

11. 무선랜 보안 기술에 관한 설명으로 가장 적절하지 **않은** 것은?

① WPA2는 CCMP를 사용하여 강력한 보안기능을 제공한다.
② WEP(Wired Equivalent Privacy)는 IEEE 802.11i에서 표준화한 데이터 암호화 방식이다.
③ WPA(Wi-Fi Protected Access)는 TKIP 방식을 사용한다.
④ WPA-PSK는 주로 인증서버가 설치되지 않은 소규모 네트워크에서 사용되는 방식이다.

12. 다음 그림은 빈칸 ㉠의 명령어를 실행한 결과의 일부이다. 빈칸 ㉠에 들어갈 명령어로 옳은 것은?



① ping ② ipconfig
③ netstat ④ tracert

13. Linux의 특수 권한에 관한 설명으로 가장 적절하지 **않은** 것은?

① Sticky bit가 설정된 디렉터리는 /tmp이다.
② SetUID를 실행 권한이 없는 파일에 설정할 경우 대문자 S로 표기된다.
③ SetGID가 부여된 파일은 소유그룹의 실행 권한이 x에서 s로 변경될 수 있다.
④ Sticky bit가 부여된 디렉터리는 소유자와 소유그룹 외 사용자의 실행권한이 x에서 s로 변경된다.

14. IPv4 패킷 헤더에 관한 설명으로 가장 적절하지 **않은** 것은?

① Version : IP 프로토콜의 버전을 의미하며 값은 $1111_{(2)}$이다.
② TTL(Time to Live) : 라우터를 하나 지날 때마다 TTL 값이 1씩 줄어들고, 그 값이 0이 되면 해당 패킷은 폐기된다.
③ Protocol : IP 계층의 서비스를 사용하는 상위계층의 프로토콜을 정의한다.
④ Header Checksum : 헤더에 대한 오류-검사용으로 사용되는 필드이다.

15. 프로세스가 사용하는 메모리 공간에 관한 설명으로 가장 적절하지 **않은** 것은?

① Text 영역 : 읽기와 쓰기가 가능한 영역이며, 프로그램 코드가 저장된다.
② Stack 영역 : 프로그램 함수 내에서 사용하는 지역변수가 저장된다.
③ Heap 영역 : 프로그램 실행 중 메모리를 동적으로 할당하는 경우에 이 영역에 할당된다.
④ Data 영역 : 전역변수를 선언하는 경우 전역변수가 저장된다.

16. 다음은 이블 트윈(evil twin) 공격에 관한 설명이다. ㉠과 ㉡에 들어갈 용어를 올바르게 짝지은 것은?

> 이블 트윈(evil twin) 공격은 공격자가 공공장소에 설치된 무선 네트워크 (㉠)의 (㉡)와/과 동일한 값을 이용하여 사용자들의 접속을 유인한 뒤, 이들의 중요 정보를 중간에서 탈취하는 공격이다.

	㉠	㉡
①	AP(Access Point)	SSID
②	AP(Access Point)	MAC
③	IP(Internet Protocol)	SSID
④	IP(Internet Protocol)	MAC

17. VPN(Virtual Private Network)에 관한 설명으로 가장 적절하지 **않은** 것은?

① SSL VPN은 별도의 장비가 없어도 웹브라우저로 구성이 가능하다.
② L2TP나 PPTP와 같은 2계층 터널링 프로토콜을 사용할 수 있다.
③ IPSec의 터널모드는 IP 헤더를 포함한 전체 IP 패킷을 암호화하여 전송한다.
④ IPSec VPN을 활용하기 위해서는 응용계층의 수정이 반드시 필요하다.

18. IDS(Intrusion Detection System) 기법에 관한 설명으로 가장 적절한 것은?

① 이상탐지(anomaly) 기법은 공격에 대한 시그니처를 데이터베이스화하여 침입자의 활동과 비교하여 동일하면 침입으로 식별한다.
② 오용탐지(misuse) 기법은 제로데이 공격에 대응이 용이하다.
③ 이상탐지(anomaly) 기법은 정상적인 상태를 기준으로 했을 때 급격한 변화를 탐지하지만, 오탐율(false positive)이 높은 문제점을 가지고 있다.
④ 오용탐지(misuse) 기법은 신경망과 통계적 분석 방법만을 사용한다.

19. 다음에서 설명하고 있는 공격 방법으로 옳지 **않은** 것은?

> 프로토콜의 오류 제어 기능을 악용하는 방식으로, TCP 패킷의 시퀀스 넘버를 조작하여 공격대상이 반복적인 재요청과 수정을 계속하도록 함으로써 시스템 자원을 고갈시키는 공격이다.

① Boink 공격 ② Land 공격
③ Bonk 공격 ④ Teardrop 공격

20. HTTP 상태코드에 관한 설명으로 가장 적절하지 **않은** 것은?

① 200 OK : 서버의 요청이 성공했다는 것을 나타낸다.
② 403 Forbidden : 클라이언트가 요청한 서버의 접근을 차단한다.
③ 404 Not Found : 클라이언트가 요청한 서버의 페이지가 존재하지 않는다.
④ 500 Internal Server Error : 서버가 클라이언트의 요청을 실행할 수 없을 때 발생한다.