【시스템네트워크보안】

1. 보안에 취약한 인터넷 응용 프로토콜/프로그램과 보안이 강화된 프로토콜/프로그램을 짝지은 것으로 가장 적절하지 **않은** 것은?

① TELNET – SSH　② SMTP – PGP
③ HTTP – HTTPS　④ FTP – TFTP

2. 대표적인 스마트폰 운영체제는 iOS와 Android이다. iOS가 Android에 비해 상대적으로 안전하다고 알려져 있다. <보기> 중 그 이유로 적절한 것을 모두 고른 것은?

<보 기>

㉠ iOS는 샌드박스(sandbox)를 활용하나 Android는 그렇지 않다.
㉡ 애플은 자신의 CA(Certification Authority)를 통해 응용 프로그램을 서명하여 배포한다.
㉢ iOS는 커널 무결성 확인 후, 이상이 없으면 정상 부팅된다.
㉣ iOS는 리눅스 커널을 기반으로 만들어진 운영체제이다.

① ㉠㉡　② ㉡㉢　③ ㉡㉣　④ ㉠㉣

3. 패스워드에 관한 설명 중 가장 적절하지 **않은** 것은?

① 사용자에게 부여된 권한(authorization)을 결정한다.
② 보안 강화를 위해 주기적인 패스워드 변경이 권장된다.
③ 패스워드 보안을 위해 패스워드와 솔트(salt)를 결합한 후, 그 해시 값을 저장하는 방법이 일반적으로 사용된다.
④ 사용자는 공격자의 패스워드 추측을 어렵게 하기 위해 컴퓨터 생성 패스워드를 이용할 수 있다.

4. ARP(Address Resolution Protocol)에 관한 설명 중 가장 적절한 것은?

① ARP는 MAC 주소에 대응되는 IP 주소를 구할 때 사용되는 프로토콜이다.
② ARP 요청 메시지와 ARP 응답 메시지는 LAN 상으로 브로드캐스트 된다.
③ 호스트의 ARP 테이블을 정적(static)으로 유지하면 ARP 스푸핑 공격을 막을 수 있다.
④ ARP 패킷은 IP 데이터그램의 페이로드(payload)로 전달된다.

5. <보기>에서 TCP를 이용하는 네트워크 공격에 해당하는 것들을 모두 고른 것은?

< 보 기 >

㉠ SYN flooding 공격　㉡ Ping of Death 공격
㉢ Telnet Session Hijacking 공격
㉣ HTTP GET flooding 공격
㉤ Smurf 공격　㉥ ICMP Redirecting 공격

① ㉠㉡㉢　② ㉠㉢㉣　③ ㉢㉣㉤　④ ㉢㉤㉥

6. <보기>의 주소들이 속해 있는 주소 블록들의 네트워크 주소와 브로드캐스트 주소가 올바르게 짝지어진 것은?

<보 기>

㉠ 14.12.62.8/24　㉡ 200.107.26.17/18

	㉠		㉡	
	네트워크주소	브로드캐스트 주소	네트워크주소	브로드캐스트 주소
①	14.12.62.0/24	14.12.62.255/24	200.107.0.0/18	200.107.63.255/18
②	14.12.62.1/24	14.12.62.255/24	200.107.1.0/18	200.107.1.255/18
③	14.12.62.0/24	14.12.62.255/24	200.107.26.0/18	200.107.26.255/18
④	14.12.62.1/24	14.12.62.255/24	200.107.192.0/18	200.107.192.255/18

7. <보기 1>의 용어와 <보기 2>의 설명을 연결한 것으로 가장 적절한 것은?

<보기 1>

(가) Footprinting
(나) APT(Advanced Persistent Threat) 공격
(다) Promiscuous 모드
(라) Zero Day 공격

<보기 2>

㉠ 특정 기업 또는 기관의 시스템을 목표로 한 장기적이고 정교한 공격
㉡ 컴퓨터 소프트웨어의 취약점에 대한 패치가 나오지 않은 시점에 이루어지는 공격
㉢ 해킹하기 전에 공격 대상에 대한 정보를 모으는 사전 준비 작업
㉣ 스니핑을 위해 랜카드의 필터링 기능을 해제

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

8. 다음 표는 패킷 필터링 방화벽에 적용된 필터링 규칙의 예이다. 표에 대한 설명 중 가장 적절하지 **않은** 것은? (방화벽은 내부 네트워크와 외부 네트워크의 경계에 위치하는 것으로 가정함)

규칙	방향	발신지 IP주소	목적지 IP주소	프로토콜	목적지 포트번호	동작
A	안으로	외부	내부	TCP	25	허용
B	밖으로	내부	외부	TCP	25	허용
C	안으로	외부	내부	TCP	80	허용
D	양방향	전부	전부	TCP/UDP	전부	거절

① 방화벽 내부의 사용자들은 외부로 전자메일을 전송할 수 있다.
② 방화벽 내부의 사용자들은 외부의 FTP 서버에 접속할 수 없다.
③ 방화벽 내부의 사용자들은 외부의 웹 서버에 접속할 수 있다.
④ 방화벽 내부의 사용자들은 외부의 텔넷 서버에 접속할 수 없다.

9. <보기>의 NAT(Network Address Translation) 라우터에 대한 설명으로 옳은 것을 모두 고른 것은?

<보 기>

㉠ 사설 IP주소와 공인 IP주소의 매핑을 제공한다.
㉡ NAT 라우터는 일반적으로 IP주소와 포트 번호를 조합하여 매핑한다.
㉢ IPv4 주소 고갈 문제를 완화할 수 있으며 보안 상 이점을 갖는다.
㉣ 사설망 내부에서 웹 서버 운영 시 port forwarding을 통해 접속을 허용할 수 있다.

① ㉠㉢　② ㉠㉡㉢　③ ㉠㉢㉣　④ ㉠㉡㉢㉣

10. 리눅스 시스템의 사용자 계정 관련 파일로 가장 적절하지 **않은** 것은?

① /etc/passwd　② /etc/shadow
③ /etc/permission　④ /etc/group

11. 네트워크 진단 프로그램에 대한 설명으로 가장 적절하지 **않은** 것은?

① traceroute – 지정한 호스트까지의 경로를 조사하는 프로그램
② nslookup – DNS 서버에 도메인 네임에 관한 질의를 하는 프로그램
③ metasploit – 네트워크 토폴로지를 매핑시키는 프로그램
④ tcpdump – 네트워크 패킷 캡처 프로그램

12. 네트워크 보안 프로토콜에 대한 설명 중 가장 적절하지 **않은** 것은?

① EAP(Extensible Authentication Protocol)는 다양한 인증 방법을 지원하는 네트워크 접근 제어 프로토콜이다.
② IPsec(IP Security)은 AH(Authentication Header)를 통해 인증, 무결성, 기밀성을 제공한다.
③ TLS(Transport Layer Security)는 최근 버전 1.3으로 표준화 되었으며, 핸드셰이크(handshake) 과정을 통해 암호화에 필요한 알고리즘 및 관련 매개변수를 교환한다.
④ DNSSEC(DNS Security)은 DNS 데이터 인증과 무결성을 보장하지만, DNS 서버에 대한 DoS(Denial of Service) 공격은 막지 못한다.

13. IEEE 802.11i에 관한 설명으로 가장 적절하지 **않은** 것은?

① IEEE 802.11 무선랜의 보안 표준으로 인증, 데이터 무결성, 데이터 기밀성, 키 관리에 관한 내용을 포함한다.
② 무선단말(station)과 무선접속점(access point) 간의 안전한 통신을 제공한다.
③ 인증서버(authentication server)는 무선단말을 인증한다.
④ 무선단말과 무선접속점은 RADIUS(Remote Authentication Dial In User Service) 프로토콜을 통해 인증 정보를 교환한다.

14. C 언어로 개발된 소프트웨어의 메모리 오염(memory corruption)에 대한 설명으로 가장 적절하지 **않은** 것은?

① Heap Buffer Overflow – malloc() 함수를 통해 힙(heap) 영역에 할당한 변수의 메모리 경계를 검사하지 않고 사용할 때 발생할 수 있음
② Integer Overflow – 변수의 자료형보다 큰 수를 저장할 때 발생할 수 있음
③ Use-After-Free – free() 함수를 통해 이미 해제된 포인터를 사용할 때 발생할 수 있음
④ Double Free – free() 함수를 통해 포인터 해제 후, 같은 이름의 포인터를 생성하고 free() 함수로 해제할 때 발생할 수 있음

15. DEP(Data Execution Prevention)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 실행 권한이 없는 메모리 영역에서 코드가 실행되지 않도록 하는 기법을 말한다.
② CPU에서 지원하는 하드웨어 기반 DEP과 운영체제가 지원하는 소프트웨어 기반 DEP으로 구분할 수 있다.
③ ROP(Return Oriented Programming) 기법에 의해 우회가 가능하다.
④ RTL(Return To Library) 공격을 막기 위해 개발되었다.

16. 32비트 인텔 CPU 아키텍처에서 윈도우 운영체제를 사용한다고 가정할 때, 어셈블리어 명령어들에 대한 설명이다. 가장 적절하지 **않은** 것은?

① ADD ECX, 10 – 카운터 레지스터 ECX에 10을 더한 후 데이터 레지스터 EDX에 저장
② MOV ECX, 4 – 카운터 레지스터 ECX에 4를 저장
③ INC EAX – 누산기 레지스터 EAX에 저장된 값을 1 만큼 증가
④ CALL EBX – 베이스 레지스터 EBX에 저장된 주소로 이동 및 실행

17. 백도어(backdoor)에 관한 설명으로 가장 적절하지 **않은** 것은?

① 백도어는 공격자에 의해 시스템 관리자 권한이 탈취된 후 설치되거나, 백도어가 이미 탑재된 악의적인 소프트웨어 설치를 통해 시스템에 설치될 수 있다.
② 하드웨어 펌웨어에 탑재된 백도어는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 있다.
③ 운영체제 레벨의 백도어(예를 들어, 악의적인 코드가 탑재된 kernel32.dll)는 디스크 포맷 후, 정상적인 운영체제 재설치를 통해 삭제될 수 있다.
④ 응용 레벨의 백도어는 현재 동작 중인 프로세스 확인, 포트 검사, 바이러스 탐지 툴, 시스템 무결성 검사 등으로 탐지가 가능하다.

18. 암호 알고리즘에 대한 설명 중 가장 적절하지 **않은** 것은?

① AES는 기존 DES, 3DES의 취약한 암호 강도를 극복하고자 미국 NIST에서 전세계 암호학자들에게 공모를 통해 선정한 비대칭 암호 알고리즘으로 데이터에 대한 기밀성 제공 및 부인방지 기능을 제공한다.
② RC5는 미국 RSA 연구소에서 개발한 입출력, 키, 라운드 수가 가변적인 블록 암호 알고리즘으로 DES에 비해 빠른 연산 속도를 제공한다.
③ SEED는 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 블록 암호 알고리즘이며, 국제표준화기구인 ISO/IEC와 IETF로부터 암호 표준 알고리즘으로 인정받았다.
④ ARIA는 국가보안기술연구소와 국내 암호 전문가들이 경량 환경을 위해 개발한 블록 암호 알고리즘이다.

19. 다음 설명 중 가장 적절하지 **않은** 것은?

① 워터마크(watermark)는 저작권 보호를 위해 이미지나 동영상 파일에 저작권 정보를 삽입하는 기법을 말한다.
② DRM(Digital Right Management)은 문서나 동영상 파일에 보안성을 제공하기 위해 암호화 하고 인가된 사용자에 한해서 해당 파일에 접근할 수 있는 권한을 부여한다.
③ 백신 프로그램은 문서나 동영상에 접근할 수 없는 사용자로부터 해당 파일의 저작권을 보호한다.
④ 방화벽은 워터마크나 DRM이 적용된 파일을 탐지하지 못한다.

20. 다음 설명 중 가장 적절하지 **않은** 것은?

① 비트코인(Bitcoin)은 블록체인(blockchain) 기반 암호화폐(cryptocurrency)이다.
② 비트코인은 공개키 기반 주소를 사용하고 트랜잭션(transaction)을 암호화하여 전송하기 때문에 익명성이 보장된다.
③ 비트코인 블록체인의 작업증명(Proof-of-Work)은 단방향 해시 함수의 특성을 이용한다.
④ 비트코인 블록체인은 누구나 참여할 수 있는 공개형 블록체인이다.