정보시스템 보안

- 문 1. cookie 정보를 불법적으로 활용하여 사용자의 세션을 탈취하기 위해 사용되는 공격은?
 - ① IP 스푸핑
- ② 버퍼 오버플로우
- ③ Cross Site Scripting
- 4 DoS
- 문 2. 데이터베이스의 DDL(Data Definition Language) 질의문에 포함 되지 않는 것은?
 - ① CREATE TABLE
 - ② DROP INDEX
 - ③ SELECT
 - **4** ALTER DATABASE
- 문 3. 공개된 웹 방화벽에 해당하는 것만을 모두 고른 것은?

¬. WebKnight

∟. ModSecurity

□. Snort

⊒. Nmap

① 7. ㄴ

② 7. ⊏

③ ㄴ, ㄹ

- ④ ㄷ. ㄹ
- 문 4. OSI 7계층의 응용 계층과 관련된 공격은?
 - ① Ping of Death
 - ② SYN flooding
 - 3 ARP spoofing
 - 4 DNS spoofing
- 문 5. 다음에서 설명하는 웹 공격 기술 유형은?

방화벽이 존재하는 시스템을 공격할 때 자주 사용되다. 일반적으로 웹 서버는 방화벽 내부에 존재하고, 80번 포트를 이용한 웹 서비스만을 제공하면 되기 때문에 방화벽에서의 인바운드 정책은 80번 포트와 필요한 포트만 빼고 다 막아 놓고, 아웃바운드 정책은 별다른 필터링을 수행하지 않는 경우가 많다. 이 웹 공격 기술은 바로 이런 허점을 이용한다.

- ① LAND
- ② 패킷 변조
- ③ 리버스 템넷
- ④ 인증 우회
- 문 6. ~ ○ 들어갈 리눅스 부팅 순서를 바르게 연결한 것은?

POST (Power on Self Test) 수행 → (①) → (②) → (©) → 실행 레벨에 따른 서비스 실행

 \bigcirc 부트 로더 실행 (L)

(E)

기본 부팅 관련 설정 사항 로드

MBR 로드

② 기본 부팅 관련 설정 사항 로드

MBR 로드

부트 로더 실행

(3) MBR 로드

(1)

부트 로더 실행

기본 부팅 관련 설정 사항 로드

(4) 부트 로더 실행 MBR 로드

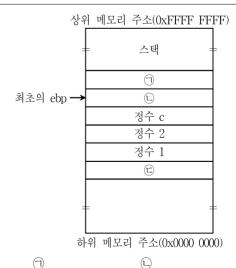
기본 부팅 관련 설정 사항 로드

문 7. 리눅스 계열 시스템에서 /bin/sh의 정보를 출력한 파일에 대한 설명으로 옳지 않은 것은?

> -r-Sr-xr-x root sys 31508 2017년 7월 21일 /bin/sh

- ① 이 파일은 모든 사용자가 실행권한을 가지고 있다.
- ② 이 파일의 소유자는 해당 파일을 읽거나 실행시킬 수 있다.
- ③ 이 파일에는 setgid가 설정되어 있다.
- ④ 이 파일을 실행 중인 일반 사용자는 root 권한을 가질 수 있다.
- 문 8. 리눅스에서 지금 어떤 프로세스가 실행 중인지를 확인하기 위해 ps라는 명령어를 사용한다. 프로세스를 실행할 때, 백그라운드 (background)와 포그라운드(foreground) 프로세스에 대한 설명 으로 옳지 않은 것은?
 - ① 백그라운드 프로세스는 현재 터미널에서 무엇을 하고 있는지와 상관없이 결과를 그대로 화면에 출력할 수 없다.
 - ② 포그라운드 프로세스는 일반적으로 한 명령어가 실행되는 동안 다른 명령어를 실행시킬 수 없다.
 - ③ 백그라운드 프로세스를 실행시키기 위해서는 명령어 뒤에 &를 붙여야 한다.
 - ④ 포그라운드 프로세스는 키보드로부터 입력을 받아서 결과를 직접 화면에 출력한다.
- 문 9. AES(Advanced Encryption Standard) 암호화 라운드 수행 시 마지막 라운드를 제외하고, 각 라운드에서 수행되는 4단계 처리 순서가 옳은 것은?
 - ① Add round key→Substitute bytes→Shift rows→Mix columns
 - ② Add round key→Substitute bytes→Mix columns→Shift rows
 - ③ Substitute bytes→Shift rows→Mix columns→Add round key
 - ④ Substitute bytes→Mix columns→Shift rows→Add round key
- 문 10. 다음은 C 프로그램 소스의 일부분이다. x86시스템에서 프로그램 내의 function 함수를 호출시 스택 프레임의 값 🗇 ~ 🖒에 들어갈 용어로 옳게 짝지은 것은?

```
void main() {
   int c;
   c=function(1.2);
int function(int a, int b) {
   a=a+b;
   return a;
```



(L)

function 함수의 반환주소 반화주소

① 저장된 프레임 포인터 ② function 함수의 반환주소

저장된 프레임 포인터

반환주소

③ 저장된 프레임 포인터 반화주소 ④ 반환주소

function 함수의 반환주소

(E)

저장된 프레임 포인터

function 함수의 반환주소

- 문 11. VPN(Virtual Private Network)의 터널링 모드 수립 시 사용되는 암호화 프로토콜이 아닌 것은?
 - ① NNTP
 - ② IPSec
 - ③ L2TP
 - ④ PPTP
- 문 12. 리눅스 시스템의 네트워크 관리 도구 및 서비스에 대한 설명으로 옳지 않은 것은?
 - ① tcpdump 네트워크 모니터링 및 패킷 분석을 위해 사용되는 도구로, 패킷 필터 기능을 통해서, 특정 침입자의 침입 경로에 따라 원하는 트래픽만을 감시
 - ② fping 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 정보 출력
 - ③ traceroute 최종 목적지 컴퓨터까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답속도를 표시
 - ④ ifconfig 네트워크 인터페이스의 IP 주소 설정
- 문 13. TCP 대신에 UDP 69번 포트를 사용하고, 사용자 인증 절차를 요구하지 않기 때문에 누구나 호스트로부터 파일을 가져갈 수 있도록 고안된 프로토콜은?
 - ① HTTP
 - ② FTP
 - ③ TFTP
 - ④ SOAP
- 문 14. Windows 레지스트리 키에 대한 설명으로 옳지 않은 것은?
 - ① HKEY_CLASSES_ROOT 파일의 각 확장자에 대한 정보와 파일과 프로그램 간의 연결에 대한 정보 저장
 - ② HKEY_CURRENT_USER 윈도우가 설치된 컴퓨터 환경 설정에 대한 정보 저장
 - ③ HKEY_LOCAL_MACHINE 설치된 하드웨어와 소프트웨어 설치 드라이버 설정에 대한 정보 저장
 - ④ HKEY USERS 디스플레이와 프린터에 관한 정보 저장
- 문 15. 다음 보안 운영체제에 대한 설명에서 괄호 안에 들어갈 용어는?

보안커널의 중요한 부분으로 객체에 대한 접근 통제 기능을 수행하고 감사, 식별 및 인증, 보안 매개변수 설정 등과 같은 다른 보안 메커니즘과 데이터를 교환하면서 상호작용을 한다. 주체와 객체 사이에서 비인가된 접속이나 불법적인 자료 변조를 막기 위해 ()은(는) DB로부터 주체의 접근 권한을 확인하기 위해 사용된다.

- ① 코어(Core)
- ② 로컬 프로시저 호출 관리자(Local Procedure Call Manager)
- ③ 신뢰 컴퓨팅 베이스(Trusted Computing Base)
- ④ 참조 모니터(Reference Monitor)

- 문 16. SSL(Secure Socket Layer) 핸드셰이크 프로토콜 처리에서 클라이언트와 서버 사이의 논리 연결을 설립하는 데 필요한 교환 단계를 순서대로 바르게 나열한 것은?
 - 기. 서버는 인증서, 키 교환을 보내고 클라이언트에게 인증서를 요청한다.
 - □. 프로토콜 버전, 세션 ID, 암호 조합, 압축 방법 및 초기 난수를 포함하여 보안 능력을 수립한다.
 - ㄷ. 암호 조합을 변경한다.
 - ㄹ. 클라이언트는 인증서와 키 교환을 보낸다.

 - 2 \vdash \rightarrow \lnot \rightarrow \rightleftarrows \rightarrow \vdash

 - 4 $\rightleftarrows \rightarrow \sqsubset \rightarrow \llcorner \rightarrow \urcorner$
- 문 17. 인터넷 메일 구조의 핵심요소에 대한 설명으로 옳지 않은 것은?
 - ① MUA 사용자 액터(actor)와 사용자 응용프로그램을 대신하여 동작한다.
 - ② MSA 원격서버로부터 POP3 또는 IMAP를 사용하여 메시지를 추출한다.
 - ③ MDA 메시지를 MHS에서 MS로 메시지를 전달한다.
 - ④ MTA 메시지가 목적지 MDA에 도달할 때까지 중계 역할을 한다.
- 문 18. 웹을 사용할 때 직면하는 보안위협과 그에 대한 대응수단으로 옳지 않은 것은?

보안위협

대응수단

① 정당한 사용자로 위장

암호학적인 기술

② 위조 요청으로 시스템 과부하 걸기

포트 스캔 암호화, 웹 프록시(proxy)

③ 네트워크상의 도청④ 사용자 데이터 변조

암호학적인 체크섬(checksum)

- 문 19. 괄호 안에 공통으로 들어갈 용어는?
 - ()코드는 Windows 호스트 프로그램의 권한으로 실행된다.
 - ()인젝션은 다른 프로세스의 주소 공간 내에서
 - ()를(을) 강제로 로드시킴으로써 코드를 실행시키는 기술이다.
 - ① 동적 링크 라이브러리(DLL)
 - ② 보안 식별자(Security Identifier)
 - ③ 일차 도메인 컨트롤러(Primary Domain Controller)
 - NFS(Network File System)
- 문 20. 리눅스 계열 운영체제에서 매주 금요일 오후 6시 50분에 /usr/adm/backuplog.sh에 위치한 쉘 스크립트를 실행시키기 위해 crontab에 입력할 내용은?
 - $① * 50 18 * 5 -exec {/usr/adm/backuplog.sh}$
 - ② 50 18 * * 5 /usr/adm/backuplog.sh
 - ③ 50 18 * * 5 -exec {/usr/adm/backuplog.sh}
 - 4 5 * * 18 50 /usr/adm/backuplog.sh