정보시스템 보안

문 1. 사용자와 시스템 또는 시스템 간의 활성화된 접속을 관리하는 시스템 보안 기능은?
① 계정과 패스워드 관리
② 세션 관리
③ 파일 관리
④ 로그 관리

문 2. 쿠키(cookie)에 대한 설명으로 옳지 않은 것은?
① 쿠키에 저장되는 내용은 각각의 웹사이트 별로 다를 수 있다.
② 쇼핑몰 사이트에서 장바구니 시스템을 이용할 때 쿠키 정보를 이용한다.
③ 쿠키는 바이러스를 스스로 전파한다.
④ 쿠키를 이용하면 사용자들의 특정 사이트 방문 여부 확인이 가능하다.

문 3. 웹 애플리케이션에 대한 보안 취약점을 이용한 공격으로 옳지 않은 것은?
① Shoulder Surfing
② Cross Site Scripting
③ SQL Injection
④ Cross Site Request Forgery

문 4. FTP 서버가 데이터를 전송할 때 목적지가 어디인지 검사하지 않는 설계상의 문제점을 이용한 FTP 공격 유형은?
① FTP Bounce 공격
② Land 공격
③ TFTP 공격
④ Smurf 공격

문 5. 웹 취약점 중 디렉터리 탐색을 차단하기 위해 사용자 입력 문자열에 필터링을 적용하는 특수 문자는?
① $
② /
③ --
④ >

문 6. 리눅스 시스템에서 /etc/shadow 파일 내용에 대한 설명으로 옳지 않은 것은?

㉠	㉡	㉢	㉣
testuser:Ep6mckrOLChF:12818:0:99999:5:7:0:12842			

① ㉠ – 암호화된 패스워드
② ㉡ – 최근 패스워드 바꾼 날
③ ㉢ – 현재 패스워드의 유효기간
④ ㉣ – 패스워드 만료 전 유저에게 바꿀 것을 경고하는 기간

문 7. 사용자의 계정명, 로그인한 시간, 로그아웃한 시간, 터미널 번호나 IP주소를 출력하는 유닉스 시스템 명령어는?
① last
② lastcomm
③ acctcom
④ chown

문 8. 다음에서 설명하는 보안 공격은?

> 유닉스 시스템에서 관리자 권한으로 실행되는 프로그램 중간에 임시 파일을 만드는 프로세스가 있을 경우 임시 파일 이름의 심볼릭 링크(Symbolic link) 파일을 생성하고, 이 프로세스 실행 중에 끼어들어 그 임시 파일을 전혀 엉뚱한 파일과 연결하여 악의적인 행동을 수행하도록 하는 공격이다.

① Fingerprinting 공격
② Race Condition 공격
③ Session Hijacking 공격
④ Heartbleed 공격

문 9. <보기 1>의 리눅스 패킷 필터링 요청 정책에 따른 <보기 2>의 ㉠ ~ ㉢에 들어갈 iptables의 명령어를 바르게 연결한 것은?

<보기 1>

> INPUT 체인에 입력 인터페이스가 eth0이고, 도착지가 192.168.10.10이고, 프로토콜은 tcp이며, 도착 포트는 80인 패킷은 버리는 정책을 추가

<보기 2>

> iptables -A INPUT -i eth0 (㉠) 192.168.10.10 (㉡) tcp (㉢) 80 -j DROP

	㉠	㉡	㉢
①	--ip	-proc	-p
②	--ip	-p	--port
③	-d	-proc	--dport
④	-d	-p	--dport

문 10. 유닉스 시스템에 기록되는 로그파일에 대한 설명을 바르게 연결한 것은?

> (가) 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보를 기록
> (나) 사용자의 로그인, 로그아웃 시간과 시스템의 종료 시간, 시작 시간을 기록
> (다) FTP 접속을 기록

	(가)	(나)	(다)
①	wtmp	pacct	loginlog
②	wtmp	loginlog	xferlog
③	pacct	loginlog	wtmp
④	pacct	wtmp	xferlog

문 11. 다음에서 설명하는 공격방법은?

> ○ 버퍼 오버플로우 공격과 유사하며 C언어가 생기면서부터 존재했지만, 발견에 많은 시간이 소요되었다.
> ○ 데이터의 형태와 길이에 대한 불명확한 정의로 인한 공격이다.

① Reverse Telnet
② Hypervisor
③ Format String
④ RootKit

문 12. 유닉스 시스템의 디렉터리별 역할에 대한 설명을 바르게 연결한 것은?

(가) 시스템의 환경 설정 및 주요 설정 파일을 담고 있다.
(나) 기본적으로 실행 가능한 파일을 담고 있다.
(다) 각 사용자의 작업 디렉터리를 담고 있다.

	(가)	(나)	(다)
①	/bin	/home	/etc
②	/home	/etc	/bin
③	/etc	/bin	/home
④	/bin	/etc	/home

문 13. 윈도우즈 시스템 명령창에서 netstat -an 명령을 수행한 결과의 일부이다. 구동 중인 서비스로 옳지 않은 것은?

프로토콜	로컬주소	외부주소	상태
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING

① FTP
② Telnet
③ SMTP
④ HTTP

문 14. OWASP(Open Web Application Security Project)에서 발표한 2013년 Mobile Security Project Top 10의 위협 요소로 옳지 않은 것은?
① 안전하지 않은 세션처리(Improper Session Handling)
② 취약한 권한 및 인증(Poor Authorization and Authentication)
③ 안전하지 않은 데이터 저장(InSecure Data Storage)
④ 서버 측 인젝션(Server Side Injection)

문 15. 리눅스 시스템의 umask 값에 따라 생성된 파일의 접근 권한이 '-rw-r-----'일 때, 기본 접근 권한을 설정하는 umask 값은?
① 200
② 260
③ 026
④ 620

문 16. 윈도우즈 시스템이 동작하기 위한 프로세스와 그에 대한 설명을 바르게 연결한 것은?

(가) Winlogon 서비스에 대한 필요한 인증 프로세스를 담당한다.
(나) 사용자 세션을 시작하는 기능을 담당한다.
(다) 사용자가 미리 지정한 시간에 작업을 실행시키는 작업 스케줄을 담당한다.

	(가)	(나)	(다)
①	smss.exe	mstask.exe	lsass.exe
②	smss.exe	lsass.exe	mstask.exe
③	lsass.exe	mstask.exe	lsass.exe
④	lsass.exe	smss.exe	mstask.exe

문 17. 버퍼 오버플로우 공격의 대응방법 중 스택에서 실행 권한을 제거해 스택에 로드된 공격자의 공격 코드가 실행될 수 없도록 하는 방법은?
① Stack Guard
② Non-Executable Stack
③ Stack Shield
④ ASLR(Address Space Layout Randomization)

문 18. 전자우편서비스 관련 프로토콜에 대한 설명으로 옳지 않은 것은?
① SMTP(Simple Mail Transfer Protocol)는 송신자의 메일 서버로부터 수신자의 메일 서버로 메시지 전송을 담당한다.
② MIME(Multipurpose Internet Mail Extension)은 SMTP를 확장하여 오디오, 비디오, 응용 프로그램, 기타 여러 종류의 데이터 파일을 주고받을 수 있다.
③ Secure/MIME은 MIME 데이터를 전자서명과 암호화 기술을 이용하여 암호화, 인증, 메시지 무결성, 송신처 부인방지 등을 제공한다.
④ IMAP(Internet Message Access Protocol)은 POP3와 다르게 SMTP 프로토콜을 의존하지 않고, 이메일의 원본을 서버에서 삭제한다.

문 19. 디지털 포렌식에서 데이터베이스에 있는 대량의 숫자 정보의 무결성 및 정확성을 확인하기 위해 수행하는 분석 방법은?
① 스니퍼 운용
② MRTG(Multi Router Traffic Grapher)
③ CAATs(Computer Assisted Auditing Techniques)
④ 네트워크 로그 서버 분석

문 20. Cross Site Scripting(XSS) 공격유형에 해당하지 않는 것은?
① Reflash XSS 공격
② Reflected XSS 공격
③ DOM(Document Object Model) 기반 XSS 공격
④ Stored XSS 공격