2017년 국가직 9급 정보시스템 보안 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
②	③	①	①	②	④	①	②	④	④
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
③	③	②	④	③	④	②	④	③	①

(정보보호직을 위한 시험과목이기 때문에, 9급 정보보호론 과목보다는 난도가 좀 높은 편이다. 시스템 보안 영역에서 좀 더 세분화된 문제가 출제가 되는데, 그 중 상당수가 정보보호론 과목에서도 난도 있는 문제로 충분히 출제가 될 수 있는 문제들이다.

이미 유닉스 리눅스의 명령어와 로그 파일 종류, 파일 권한 변경을 묻는 문제들은 여러 번 출제되었으며, XSS 공격 유형을 묻는 문제 또한 지난번 국가직 하반기 시험에 출제가 되었다.

그러므로 정보시스템 보안 과목이라도 9급 준비생들도 한 번쯤 풀어볼 만하고, 좀 지엽적이라 생각하는 문제들은 ★ 표시를 해두었으니 넘어가고 나중에 공부해도 무관하겠다.

물론 100점을 노리는 분들이나 정보보호직, 7급, 경찰간부 준비생 분들은 모두 풀어보길 권장한다.)

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

답 ②

◈ 시스템 보안 기능 종류

▷ 계정과 패스워드 관리
- 적절한 권한을 가진 사용자를 식별하기 위한 가장 기본적인 인증 수단
- 시스템에서는 계정과 패스워드 관리가 보안의 시작

▷ 세션 관리
- 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대한 관리
- 일정 시간이 지날 경우 적절히 세션을 종료하고, 비인가자에 의한 세션 가로채기를 통제

▷ 접근 제어
- 시스템이 네트워크 안에서 다른 시스템으로부터 적절히 보호될 수 있도록 네트워크 관점에서 접근을 통제

▷ 권한 관리
- 시스템의 각 사용자가 적절한 권한으로 적절한 정보 자산에 접근할 수 있도록 통제

▷ 로그 관리
- 시스템 내부 혹은 네트워크를 통한 외부에서 시스템에 어떤 영향을 미칠 경우 해당 사항을 기록

▷ 취약점 관리
- 시스템은 계정과 패스워드 관리, 세션 관리, 접근 제어, 권한 관리 등을 충분히 잘 갖추고도 보안적인 문제가 발생할 수 있음
- 이는 시스템 자체의 결함에 의한 것으로 이결함을 체계적으로 관리하는 것이 취약점 관리이다.

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.

답 ③

쿠키(Cookie)는 사용자가 방문하는 웹 사이트에 대한 설정 정보와 인증 정보를 사용자의 PC에 저장해두는 것이다.
쿠키에는 Persistent Cookie와 Session Cookie(세션 쿠키)가 있다.
Persistent Cookie(영구 쿠키)는 사용자의 하드 디스크에 저장해두며, 브라우저를 종료해도 쿠키는 디스크에 남아있다.
Session Cookie(세션 쿠키)는 브라우저 프로세스가 실행되고 있을 때까지만 유효한 쿠키로, 사용자가 브라우저를 종료하면 쿠키는 삭제된다.
③ 쿠키 역시 다른 파일과 마찬가지로 바이러스에 감염될 수 있다. 웹 브라우저을 이용할 때, 갑자기 내가 최근 방문했거나 사이트나 자주 검색하는 단어와 관련된 광고가 뜨는 것 등이 쿠키 정보를 이용한 바이러스, 악성 코드들이다.
하지만 쿠키 스스로 바이러스를 전파하지는 않는다.
<오답 체크> ① 자동 로그인을 설정 유무, 검색 기능 제공 유무, 등 웹 사이트별 제공하는 서비스에 따라 쿠키에 저장되는 내용은 다르다.

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

답 ①

① **Shoulder Surfing**(숄더 서핑)은 사회공학적 공격기법의 하나로, 어깨 너머로 훔쳐보는 행위를 의미한다.
<오답 체크> ② **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)
웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.
③ **SQL Injection**(삽입) 공격
클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격이다.
④ **CSRF**(Cross-site request forgery, 크로스사이트 요청 변조)
로그인 된 피해자의 세션 쿠키를 위조하여, 피해자가 의도 않은 요청을 웹사이트로 보내 피해입히는 공격이다.

◈ 사회공학적 공격기법(social engineering)
▷ Pretexting : 신분을 조작하거나 거짓으로 상황을 꾸며 피해자가 특정 행동을 하도록 유도
▷ Dumpster Diving : 쓰레기통 뒤지기
▷ Piggybacking, Taligating : 권한 가진 사용자 몰래 뒤따라가기
▷ Shoulder Surfing : 어깨 넘어 훔쳐보기
▷ Quid Pro Quo : 선물이나 서비스 제공하는 척하면서 정보 빼내기
▷ Black Mail : 협박, 공갈, 갈취등의 내용이 담긴 편지
▷ Phishing : 금융기관을 사칭해서 개인정보를 불법적으로 알아내기
▷ Spear Phising : 불특정 대상이 아닌 특정 집단이나 인물을 대상으로 피싱 사기
▷ Baiting : 웹사이트에 공짜 영화나 음악 등을 걸어두고 방문을 유도한 뒤 개인정보 탈취

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

답 ①

① **FTP Bounce Attack**(FTP 바운스 공격)
FTP 프로토콜은 서버가 데이터를 전송할 때 목적지를 검사하지 않도록 설계되어 있는데, 이러한 구조상의 허점을 이용해 방화벽 내부의 다른 서버들을 스캔하고 침입하는 공격이다.

<오답 체크> ② **Land 공격**(Land Attack)
패킷의 출발지 IP 주소와 목적지 IP 주소 값을 모두 공격자의 IP 주소 값으로 만들어 전송하는 공격이다.
출발지 주소와 목적지 주소가 같기 때문에 이 패킷은 공격대상을 떠났다가 그대로 다시 공격대상에게 들어가는데, SYN Flooding 처럼 동시 사용자 수를 점유해버리며 CPU 자원을 고갈시킨다.

③ **TFTP Bruteforcing 공격**
TFTP는 인증 절차를 생략한 간소화된 FTP로, UDP를 이용하고 69번 포트를 사용한다. 주로 부팅서버나 백업용 서버에 주로 사용한다.
TFTP 서버는 인증 절차를 생략했기 때문에 파일명만 알면 다운로드가 가능한데, 공격자는 이러한 점을 이용해 BruteForce 공격(무차별 대입 공격)을 통해 서버의 파일을 획득할 수 있다.

④ **Smurf**(ICMP flooding) 공격
공격대상 호스트의 IP주소로 위장된 소스 IP주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상이 많은 양의 ICMP Echo 응답 패킷을 받아 시스템의 자원을 고갈된다.

★ **문 5. 웹 취약점 중 디렉터리 탐색을 차단하기 위해 사용자 입력 문자열에 필터링을 적용하는 특수 문자는?**

① $
② /
③ --
④ >

답 ②

② ◈ 웹 취약점을 이용한 인수조작 공격에 사용되는 특수문자

주요 특수 문자	주요 관련 공격
<	XSS
>	XSS
&	XSS
"	XSS
?	XSS
'	XSS, SQL 삽입 공격
/	XSS, 디렉터리 탐색
--	SQL 삽입 공격
=	SQL 삽입 공격
;	SQL 삽입 공격
*	SQL 삽입 공격
.	SQL 삽입 공격
..	SQL 삽입 공격

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

㉠	㉡	㉢	㉣
testuser:Ep6mckrOLChF:12818:0:99999:5:7:0:1284			

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

답 ④

㉣ '7'은 로그인을 자주 하지 않을 경우, 보안을 위해 로그인이 비활성화되는 기간을 표시하는 필드이다.
패스워드 만료 전 유저에게 바꿀 것을 경고하는 기간을 의미하는 필드는 ㉣ 앞의 '5'이다.

위의 shadow 파일은 :(콜론)으로 구분하여 9개의 필드로 구성되어 있다.

▷ testuser
사용자 계정(username)
▷ ㉠ Ep6mckrOLChF
패스워드를 암호화한 값(encrypted)
▷ ㉡ 12818
마지막으로 패스워드가 수정된 날(last changed)
▷ 0
패스워드가 변경되기 전 최소사용기간(일 수)(may, minlife)
0일이기 때문에 언제나 변경할 수 있다는 의미
▷ ㉢ 99999
패스워드가 변경되기 전 최대사용기간(일 수)(must, maxlife)
99999일이기 때문에 상당히 오래 사용하겠다는 의미
▷ 5
패스워드 만기일 전에 경고 메시지를 제공하는 일 수 (warn)
▷ ㉣ 7
자주 사용하지 않는 계정의 로그인 비활성화 일 수(expire, inactive)
▷ 0
계정이 만료되어 로그인 사용을 금지하는 일 수 (월/일/연도)(expire)
▷ 1284
예약 필드(reserved)

문 7. 사용자의 계정명, 로그인한 시간, 로그아웃한 시간, 터미널 번호나 IP주소를 출력하는 유닉스 시스템 명령어는?

① last
② lastcomm
③ acctcom
④ chown

답 ①

① last 명령어는 로그인과 로그아웃 기록을 보여주는 명령어로, /var/adm/wtmpx 파일의 내용을 분석해서 출력한다.
<오답 체크> ② lastcomm 명령어는 사용자들이 실행한 명령과 프로세스 기록을 보여주는 명령어이다.
③ acctcom 명령어는 사용자의 시간별 시스템 사용 정보를 보여주는 명령어이다.
④ chown 명령어는 파일 또는 폴더의 소유권을 바꾸는 명령어이다.

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

답 ②

② Race Condition(**레이스 컨디션**) 공격
두 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법이다.

<오답 체크> ① Fingerprinting(**핑거프린팅**)은 보안 공격이 아니라, 콘텐츠에 구매자의 정보를 삽입하여 불법 배포 근원지를 추적하는 기술이다.
핑거프린팅 기술을 무력화시키는 공격으로는 공모 공격이 있다.
공모 공격(Collusion Attack)은 다수가 저작물을 비교하여 핑거프린팅이 삽입된 위치를 파악한 다음 핑거프린팅을 지우거나 새로운 프린팅을 삽입하여 불법 배포하는 공격 방법이다.

③ Session Hijacking(**세션 하이재킹**) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.

④ HeartBleed(**하트블리드**) 공격
2014년 4월 OpenSSL 1.0.1 버전에서 발견된 매우 심각한 버그 OpenSSL을 구성하고 있는 TLS/DTLS의 HeartBeat 확장규격에서 발견된 취약점으로, 해당 취약점을 이용하면 서버와 클라이언트 사이에 주고받는 정보들을 탈취할 수 있다.

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

> 〈 보 기 1 〉
> INPUT 체인에 입력 인터페이스가 eth0이고, 도착지가 192.168.10.10이고, 프로토콜은 tcp이며, 도착 포트는 80인 패킷은 버리는 정책을 추가

> 〈 보 기 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

답 ④

iptables는 리눅스상에서 방화벽을 설정하는 도구이다.
㉠ 도착지 주소(192.168.10.10)를 명시하는 옵션은 '-d'이다.
㉡ 프로토콜(tcp)을 명시하는 옵션은 '-p'이다.
㉢ 도착지 포트(80)을 명시하는 옵션은 '--dport'이다.

iptables 옵션
-p : 패킷의 프로토콜 이름(또는 해당 프로토콜의 포트번호) 명시
-s : 패킷의 발신지
--sport : 패킷의 발신지 포트
-d : 패킷의 도착지를 명시한다.
--dport : 패킷의 도착지 포트
-i : 규칙을 적용할 인터페이스 이름을 명시(ex : eth0, eth1)
-j : 규칙에 맞는 패킷을 어떻게 처리할 것인가를 명시
-y : 접속 요청 패킷인 SYN 패킷을 허용하지 않음
-f : 두 번째 이후의 조각에 대해 규칙을 명시

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

답 ④

(가) 사용자가 시간대별로 수행한 명령어와 프로그램에 대한 정보를 기록하는 로그파일은 pacct이다.
lastcomm이나 acctcom 명령어를 통해 내용을 볼 수 있다.
(나) 로그인/로그아웃에 대한 정보를 기록하는 로그파일은 wtmp이다.
last 명령어를 통해 wtmp 파일 내용을 볼 수 있다.
(다) FTP를 통해 송수신되는 데이터에 대한 정보를 기록하는 로그파일은 xferlog이다.

◈ 리눅스 주요 로그 정리

로그	저장 내용
utmp, utmpx	현재 로그인한 사용자들에 대한 상태 정보
wtmp, wtmpx	사용자들의 로그인/로그아웃 정보
sulog, authlog	su(switch user) 명령어 사용 정보
syslog, secure	사용자 인증에 관련된 정보
loginlog, failedlog, btmp	실패한 로그인 정보
shutdownlog	셧다운, 리부팅, 홀트 정보
access_log, error_log	웹 서버 접속, 에러 정보
lastlog	각 사용자의 최근 로그인 정보
messages	콘솔 상의 화면에 출력되는 메시지 정보
xferlog	FTP를 통해 송수신되는 데이터 정보
acct, pacct	사용자별 실행한 명령어 정보
history	사용자별 실행한 명령어, 인자 정보
sialog	Compaq Tru64 OS에서 su 명령어 사용 정보

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

답 ③

③ **Format String**(포맷 스트링) 공격
결과를 출력하기 위하여 사용되는 printf() 함수에서 지시자를 제대로 지정하지 않아 의도적으로 버그를 발생시켜, 메모리의 특정 위치의 값을 다른 것으로 변경시키는 공격이다. 해커는 이렇게 포맷 스트링의 취약점을 악용해 시스템의 권한을 획득하거나 특정 동작을 수행하게 만든다.

<오답 체크> ① **Reverse Telnet**(리버스 텔넷) 공격
보통 방화벽을 운영할 땐 인바운드 규칙(외부에서 내부로의 접속 규칙)을 설치해 통제하기 때문에, telnet(텔넷) 프로토콜을 이용한 외부에서 내부로 원격 접속은 필터링이 가능해진다.
하지만 보통 아웃바운드 규칙(내부에서 외부로의 규칙)은 허술한 경우가 대부분이다. 이러한 취약점을 이용해 방화벽 내부에서 프로그램을 실행시켜 외부에 있는 공격자 컴퓨터 쪽으로 접속하도록 조작하는 것이 리버스 텔넷 공격이다.

② **Hypervisor**(하이퍼바이저)는 하나의 컴퓨터에서 서로 다른 운영체제를 실행하는 가상화(Virtualization)을 실현하기 위한 논리적 플랫폼을 의미한다.

④ **RootKit**(루트킷)
해커들이 컴퓨터나 또는 네트웍에 침입한 사실을 숨긴 채 관리자용 접근 권한(루트 권한)을 획득하는데 사용하는 도구의 모음이다.

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

답 ③

(가) /etc 시스템 환경 설정 디렉터리
(나) /bin 기본적인 사용자 명령어 디렉터리
(다) /home 각 사용자의 홈 디렉터리

◈ 유닉스 주요 디렉터리

디렉터리	내용
/	최상위 루트 디렉터리
/boot	부팅에 필요한 핵심 실행 파일
/bin	기본적인 사용자 명령어
/dev	시스템에 연결된 장치들
/etc	시스템 환경 설정
/home	사용자 디렉터리
/lib	프로그램을 위한 다양한 공용 라이브러리
/mnt	다른 시스템에서 익스포트된 파일 시스템들을 임시로 마운트하는 디렉터리
/proc	현재 실행 프로세스들의 이미지
/sbin	시스템의 시작에 필요한 바이너라 파일
/temp	일시적으로 저장되는 임시 파일
/usr	일반 사용자를 위한 명령어와 파일
/vsr	관리자용 다양한 파일이 저장되는 디렉터리

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

답 ②

주소에서 콜론(:)뒤의 마지막 숫자는 포트 번호를 의미한다.
21번 포트는 FTP 연결 제어 정보, 25번 포트는 SMTP, 80번 포트는 HTTP의 포트 번호들이다.
② Telnet(텔넷)의 포트 번호는 23번으로 문제에 안 나와 있다.

◈ 주요 포트 목록
20 - FTP 실제 데이터 전송
21 - FTP 연결 시 인증 제어 정보 전송
22 - SSH(Secure Shell)
23 - telnet
25 - SMTP
53 - DNS
80 - HTTP
88 - 커버로스(Kerberos)
109 - POP2
110 - POP3
143 - IMAP4
161 - SNMP
220 - IMAP3
443 - HTTPS

★ **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)

답 ④

(리스트에 없는 항목을 문제에 집어넣은 게 아니고, 있는 항목을 잘못되게 변형하게 문제에 집어넣었기 때문에, 꼭 리스트를 다 암기할 필요 없이 한 번쯤 읽고 지나가면 된다.)

④ 인젠셕 공격은 서버 쪽이 하는 게 아니라, 클라이언트에서 하는 것이다. M2인 취약한 서버 측 제어(Weak Server Side Control)과 M4인 클라이언트 측 인젝션 공격(Client Side Injection)을 짜집기해 만든 함정 구문이다.

<오답 체크> ① 안전하지 않은 세션처리 ---> M6
(Improper Session Handling)
② 취약한 권한 및 인증 ---> M5
(Poor Authorization and Authentication)
③ 안전하지 않은 데이터 저장 ---> M1
(InSecure Data Storage)

OWASP Mobile Top 10 2012-2013
M1 안전하지 않은 데이터 저장
(Insecure Data Storage)
M2 취약한 서버 측 제어
(Weak Server Side Control)
M3 불충분한 전송계층의 보호
(Insufficient Transport Layer Protection)
M4 클라이언트 측면의 인젝션 공격
(Client Side Injection)
M5 취약한 권한부여 및 인증
(Poor Authorization and Authentication)
M6 부적절한 세션 처리
(Improper Session Handling)
M7 신뢰할 수 없는 입력에 대한 보안 결점
(Security Decisions Via Untrusted Inputs)
M8 주변 채널에 의한 데이터 누수
(Side Channel Data Leakage)
M9 취약한 암호화
(Broken Cryptography)
M10 중요한 정보 노출
(Sensitive Information Disclosure)

OWASP Mobile Top 10 2014
M1 취약한 서버측 제어
(Weak Server Side Control)
M2 안전하지 않은 데이터 저장
(Insecure Data Storage)
M3 불충분한 전송계층의 보호
(Insufficient Transport Layer Protection)
M4 의도하지 않은 데이터 누출
(Unintended Data Leakage)
M5 취약한 권한부여 및 인증
(Poor Authorization and Authentication)
M6 취약한 암호화
(Broken Cryptography)
M7 클라이언트 측면의 인젝션 공격
(Client Side Injection)
M8 신뢰할 수 없는 입력에 대한 보안 결점
(Security Decisions Via Untrusted Inputs)
M9 부적절한 세션 처리
(Improper Session Handling)
M10 바이너리 보호 미비
(Lack of Binary Protections)

2012년과 2014년은 목록들이 비슷했는데, 2016년에는 전체적으로 항목들을 재분류하였다.

OWASP Mobile Top 10 2016(RC)
M1 부적절한 플랫폼의 사용
(Improper Platform Usage)
M2 안전하지 않은 데이터 저장
(Insecure Data Storage)
M3 안전하지 않은 통신
(Insecure Communication)
M4 안전하지 않은 인증
(Insecure Authentication)
M5 불충분한 암호화
(Insufficient Cryptography)
M6 안전하지 않은 권한부여
(Insecure Authorization)
M7 이용자 코드 품질
(Client Code Quality)
M8 코드 변조
(Code Tampering)
M9 역공학
(Reverse Engineering)
M10 불필요한 기능
(Extraneous Functionality)

문 15. 리눅스 시스템의 umask 값에 따라 생성된 파일의 접근 권한이 '-rw-r-----' 때, 기본 접근 권한을 설정하는 umask 값은?

① 200
② 260
③ 026
④ 620

답 ③

리눅스에서 폴더를 처음 생성하면 기본적으로 777의 권한이 설정되어 있고, 파일을 처음 생성하면 666의 권한이 설정되어 있다.
umask 명령어를 통해 현재 설정된 권한을 제거할 수 있다.
문제에서는 파일이기 때문에 처음 설정된 권한은 666이었을 것이다.
현재 소유자에게 rw-, 그룹에 r--, other에 --- 권한이 부여되어 있으므로 640 권한인 상태이다.
따라서 umask 026를 설정하면 된다.

변경 전 권한 110 110 110 = 666
umask -) 000 010 110 = 026

변경 후 권한 110 100 000 = 640

(이 문제는 폴더와 파일의 생성 권한을 구분하도록 umask 157을 보기에 같이 냈으면 더 어려웠을 텐데, 이번엔 운 좋게 그렇게 내지 않았으니 꼭 숙지하도록 한다.)

★ **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

답 ④

(가) lsass.exe (Local Security Authority Subsystem Service)
로그인한 유저의 인증을 담당하는 프로세스로, 로컬 보안, 도메인 인증 및 Active Directory 프로세스를 관리하기 위한 인터페이스를 제공하는 서비스 프로세스이다.
(나) smss.exe (Sesseion Manager Subsystem)
사용자 세션의 시작을 담당하는 세션 관리자 하위 시스템이다.
(다) mstask.exe (Microsoft Task Scheduler)
시스템의 백업이나 업데이트에 관련된 작업 스케줄러이다.

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)

답 ②

② Non-Executable Stack
가장 기초적인 오버플로우 방어 기법으로, 스택에서 코드가 실행되지 않도록 설정하는 것이다.(**NX-bit** 설정)

<오답 체크> ① **Stack Guard**(스택 가드)
메모리의 특정한 위치(ret 앞)에 카나리(canary)라는 특정한 값을 집어넣어, 프로그램 실행시 해당 카나리 값이 변조되었을 경우 스택 영역이 변조되었다고 판단하여 프로그램을 종료하는 방법이다.

③ **Stack Shield**(스택 쉴드)
(인터넷에 있는 많은 글에 스택 가드와 스택 쉴드가 같은 것인냥 나와있는데, 같은 것이라면 보기에 둘 다 나오진 않았을 것이다.)
스택 쉴드는 프로그램 반환 주소를 안전한 공간에 복사해두고, 함수가 종료될 때 현재 스택의 리턴 반환 주소와 복사해둔 반환 주소를 비교하여 변조되었는지 확인하는 탐지 방법이다.

④ **ASLR**(Address Space Layout Randomization)
메모리상의 공격을 어렵게 하기 위해 스택이나 힙, 라이브러리 등의 주소를 랜덤으로 프로세스 주소 공간에 배치함으로써 실행할 때 마다 데이터의 주소가 바뀌게 하는 방법이다.

◈ 버퍼 오버플로우 공격 대응책
1. 버퍼 오버플로우에 취약한 표준 라이브러리 함수를 사용하지 않는다. 버퍼의 경계 검사를 하지 않는 표준 C라이브러리의 strcpy(), strcat(), gets(), sprintf() 등이다.
2. 입력 값을 검사하여 특정 입력만 받아들이고 나머지를 차단하는 방식을 고려한다.
3. 프로그래밍 시 버퍼 경계 검사를 한다.
4. 버퍼 오버플로우에 안전한 라이브러리를 사용한다.
5. 각종 버퍼 오버플로우 방지 기법을 사용한다. Libsafe, StackGuard, StackShield 등이 있다.
6. 정적 분석 도구를 사용한다. 많은 분석도구가 이 버퍼 오버플로우 결함을 탐지해낼 수 있다.

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.

답 ④

④ IMAP는 이메일을 읽어도 원본을 서버에서 삭제하지 않는다.
읽으면 삭제가 되는 것은 POP3 프로토콜이다.

IMAP(Internet Message Access Protocol, 인터넷 메시지 접속 프로토콜)
전자메일 수신 프로토콜, 읽어도 삭제되지 않음, 다운 여부 본인이 결정

POP3(Post Office Protocol)
전자메일 수신 프로토콜, 읽으면 자동 삭제, 자동 다운

<오답 체크> ① **SMTP**(Simple Mail Transfer Protocol, 간이 전자우편 전송 프로토콜)
전자메일 송신 프로토콜

② **MIME**(Multipurpose Internet Mail Extension)
기본적으로 7비트 아스키 문자만 지원하는 SMTP의 문제를 해결하고자 SMTP를 확장하여 오디오, 비디오, 응용 프로그램, 기타 여러 종류의 데이터 파일을 주고받을 수 있도록 만든 프로토콜이다.

③ **S/MIME**(Secure/Multipurpose Internet Mail Extension)
MIME를 보호하기 위해 암호화 및 인증을 지원하는 기술로, RSA를 이용하고 인증기관 필요로 한다.

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

답 ③

③ **CAATs**(Computer Assisted Auditing Techniques)는 데이터베이스에 있는 대량의 숫자 정보의 무결성 및 정확성을 확인하기 위해 수행되는 분석 방법으로, 디지털 포렌식이나 정보시스템감사 등에 이용된다.

<오답 체크> ① 스니퍼(Sniffer)는 네트워크 패킷을 탐지하는 도구이다.

② **MRTG**(Multi Router Traffic Grapher)는 네트워크 트래픽 모니터링 및 관리를 위해서 사용되고 있는 범용의 툴이다.
주기적으로 트래픽량을 분석하여 그 결과를 gif 및 png의 그래픽 파일을 포함한 HTML파일로 생성하여 웹 브라우저를 통해서 네트워크 트래픽을 분석·관리 할 수 있다.

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

답 ①

XSS(Cross-site Scripting, 크로스 사이트 스크립팅)는 웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.
XSS 유형에는 저장 XSS, 반사 XSS, Dom 기반 XSS 공격이 있다.

① Reflash XSS 공격이란 없다.

<오답 체크> ② **반사 XSS 공격**(Reflected XSS)은 URL의 CGI 인자에 스크립트 코드를 삽입하는 공격 방법이다. 사용자에게 악성 URL을 배포하여 사용자가 클릭하도록 유도하여 바로 사용자를 공격하는 방법이다. 공격자는 공격용 악성 URL을 생성한 뒤, 이 URL을 이메일 메세지나 거짓 정보 등 다양한 경로로 사용자들에게 배포한다. 사용자는 이 URL 링크를 클릭하는 순간 바로 악성 스크립트가 사용자의 브라우저에서 실행된다.

③ DOM(Document Object Model)은 HTML 및 XML 문서 등 구조화된 문서를 표현하는 W3C 공식 표준 API이다.
DOM 기반 XSS 공격은 사용자의 브라우저가 HTML 페이지를 구문 분석하면서 DOM 객체를 실행할 때, 검증되지 않은 입력값이 자바 스크립트를 통해 삽입되면서 악성코드가 실행되는 공격 방법이다. 페이지 자체에는 변화가 없으며, 서버와 관계없이 발생한다.

④ **저장 XSS 공격**(Stroed XSS)은 웹 서버에 악성 스크립트를 영구적으로 저장해 놓는 공격 방법으로, 웹 사이트의 게시판, 사용자 프로필 및 코멘트 필드 등에 악성 스크립트를 삽입해 놓는다. 사용자가 사이트를 방문하여 저장되어 있는 페이지에 접근하면, 서버에 있던 악성 스크립트를 사용자에게 전달되어 사용자 브라우저에서 실행되어 공격한다.