2022-지방직-정보보호론-A-해설

총평

2022년 지방직 정보보호론은 이전 시험(2022년 국가직, 2021년 지방직)에 비해 어렵게 출제되어 “중상”의 난이도를 가집니다. Killer 문제는 6번과 8번이고, 대부분의 문제들은 기본/심화, 기출, 단원, 모고를 충분히 회독했다면 풀 수 있는 문제들로 구성되었습니다. 그리고 생소한 문제(20번)는 소거법으로 풀 수 있었습니다.

1. 송수신자의 MAC 주소를 가로채 공격자의 MAC 주소로 변경하는 공격은?

① ARP spoofing
② Ping of Death
③ SYN Flooding
④ DDoS

정답 체크

(1) 송수신자에게 공격자의 MAC을 알려준다.

2. 스니핑 공격의 탐지 방법으로 옳지 않은 것은?

① ping을 이용한 방법
② ARP를 이용한 방법
③ DNS를 이용한 방법
④ SSID를 이용한 방법

정답 체크

(4) 해당 방법은 존재하지 않는다.

3. 공격자가 해킹을 통해 시스템에 침입하여 루트 권한을 획득한 후, 재침입할 때 권한을 쉽게 획득하기 위하여 제작된 악성 소프트웨어는?

① 랜섬웨어
② 논리폭탄
③ 슬래머 웜
④ 백도어

정답 체크

(4) 재침입을 위해 백도어를 설치한다.

4. 다음에서 설명하는 용어는?

○ 한 번의 시스템 인증을 통해 다양한 정보시스템에 재인증 절차 없이 접근할 수 있다. ○ 이 시스템의 가장 큰 약점은 일단 최초 인증 과정을 거치면, 모든 서버나 사이트에 접속할 수 있다는 것이다.

① NAC(Network Access Control)
② SSO(Single Sign On)
③ DRM(Digital Right Management)
④ DLP(Data Leak Prevention)
정답 체크
(2) 대학교 학사 시스템 등에 활용된다.

5. 보안 공격 유형에는 적극적 공격과 소극적 공격이 있다. 다음 중 공격 유형이 다른 하나는?
① 메시지 내용 공개(release of message contents)
② 신분 위장(masquerade)
③ 메시지 수정(modification of message)
④ 서비스 거부(denial of service)
정답 체크
(1) 기밀성 관련 공격이다.

6. X.509 인증서 폐기 목록(Certificate Revocation List) 형식 필드에 포함되지 않는 것은?
① 발행자 이름(Issuer name)
② 사용자 이름(Subject name)
③ 폐지된 인증서(Revoked certificate)
④ 금번 업데이트 날짜(This update date)
정답 체크
(2) X.509 CRL 형식 필드는 다음과 같다.

필드명		사용여부		설정값
기본 필드	Version	Y		V2 (1)
	Signature	Y		서명알고리즘 OID 및 파라미터
	Issuer	Y		CRL 발행 기관 DN. X.500 DN 사용
	This Update	Y		CRL 발급일 UTCTime 또는 GeneralizedTime 사용
	Next Update	Y		CRL 다음 발급일 지정날짜보다 이전에 발급함을 의미. UTCTime 또는 GeneralizedTime 사용
	Revoked Certificates	Y		인증서 일련번호 및 폐지일 포함
확장 필드		사용여부	C	
	Authority Key Identifier	Y	F	발급자 Key ID 인증서 폐지목록 검증 경로 생성 시 사용
	Issuer Alternative Name	O	F	
	CRL Number	Y	F	정수값, CRL 일련번호, 20바이트 이하
	Issuing Distribution Point	O	T	
	Delta CRL Indicator	O	F	Delta CRL 지시자, Full CRL과 동시 발급필요 cRLNumber 값과 Delta CRL 개수가 동일해야함
엔트리 확장 필드	Reason Code	O	F	폐지사유 코드 unspecified, certificateHold, privilegeWithdrawn, cACompromise 는 미사용
	Hold Instruction Code	O	F	
	Invalidity Date	O	F	
	Certificate Issuer	O	T	CRL DP 확장에 설정된 indirectCRL 지시자를 가지는 CRL에 있는 인증서의 발급기관 명칭

* 범례 : 괄호 안은 무선용 인증서 폐지목록에만 해당

사용여부	C(Criticality)
Y-사용함, 빈칸-사용하지 않음, O-Optional	T-True, F-False

7. AES 알고리즘에 대한 설명으로 옳지 않은 것은?
① 블록 암호 체제를 갖추고 있다.
② 128/192/256bit 키 길이를 제공하고 있다.
③ DES 알고리즘을 보완하기 위해 고안된 알고리즘이다.
④ 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 NOR 연산을 수행한다.
정답 체크
(4) XOR 연산을 수행한다.

8. 정보기술과 보안 평가를 위한 CC(Common Criteria)의 보안 기능적 요구 조건에 해당하지 않는 것은?
① 암호 지원
② 취약점 평가

③ 사용자 데이터 보호
④ 식별과 인증
정답 체크
(2) CC의 보안 기능적 요구 조건(클래스)는 다음과 같다.

CC 2부 보안기능 클래스
FAU(Security Audit) 보안 감사
FCO(Communication) 통신
FCS(Cryptographic Support) 암호 지원
FDP(User Data Protection) 사용자 데이터 보호
FIA(Identification & Authentication) 식별 및 인증
FMT(Security Management) 보안 관련
FPR(Privacy) 프라이버시
FPT(Protection of the TSF) TSF 보호
FRU(Resource Utilisation) 자원 활용
FTA(TOE Access) TOE 접근
FTA(Trusted Path/Channel) 안전한 경로/채널

9. 커버로스(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은?
① 사용자를 인증하기 위해 사용자의 패스워드를 중앙집중식 DB에 저장하는 인증 서버를 사용한다.
② 사용자는 인증 서버에게 TGS(Ticket Granting Server)를 이용하기 위한 TGT(Ticket Granting Ticket)를 요청한다.
③ 인증 서버가 사용자에게 발급한 TGT는 유효기간 동안 재사용 할 수 있다.
④ 네트워크 기반 인증 시스템으로 비대칭 키를 이용하여 인증을 수행한다.
정답 체크
(4) 대칭키를 이용한다.

10. 다음에서 설명하는 보안 공격은?

> ○ 정상적인 HTTP GET 패킷의 헤더 부분의 마지막에 입력되는 2개의 개행 문자(\r\n\r\n) 중 하나(\r\n)를 제거한 패킷을 웹 서버에 전송할 경우, 웹 서버는 아직 HTTP 헤더 정보가 전달되지 않은 것으로 판단하여 계속 연결을 유지하게 된다.
> ○ 제한된 연결 수를 모두 소진하게 되어 결국 다른 클라이언트가 해당 웹 서버에 접속할 수 없게 된다.

① HTTP Cache Control ② Smurf
③ Slowloris ④ Replay
정답 체크
(3) Slow HTTP Header DOS라고 한다.

11. (가), (나)에 들어갈 접근통제 보안모델을 바르게 연결한 것은?

(가)은 허가되지 않은 방식의 접근을 방지하는 모델로 정보 흐름 모델 최초의 수학적 보안모델이다. (나)은 비즈니스 입장에서 직무분리 개념을 적용하고, 이해가 충돌되는 회사 간의 정보의 흐름이 일어나지 않도록 접근통제 기능을 제공하는 보안모델이다.

	(가)	(나)
①	Bell-LaPadula Model	Biba Integrity Model
②	Bell-LaPadula Model	Brewer-Nash Model
③	Clark-Wilson Model	Biba Integrity Model
④	Clark-Wilson Model	Brewer-Nash Model

정답 체크

(1) 최초의 수학적 모델은 BLP 모델이고, 이해 충돌 방지는 만리장성 모델이다.

12. 리눅스 시스템에서 umask값에 따라 새로 생성된 디렉터리의 접근 권한이 'drwxr-xr-x'일 때 기본 접근 권한을 설정하는 umask의 값은?

① 002
② 020
③ 022
④ 026

정답 체크

(3) 777-755=022

13. (가), (나)에 해당하는 침입차단시스템 동작 방식에 따른 분류를 바르게 연결한 것은?

(가) 각 서비스별로 클라이언트와 서버 사이에 프록시가 존재하며 내부 네트워크와 외부 네트워크가 직접 연결되는 것을 허용하지 않는다. (나) 서비스마다 개별 프록시를 둘 필요가 없고 프록시와 연결을 위한 전용 클라이언트 소프트웨어가 필요하다.

	(가)	(나)
①	응용 계층 게이트웨이 (application level gateway)	회선 계층 게이트웨이 (circuit level gateway)
②	응용 계층 게이트웨이 (application level gateway)	상태 검사 (stateful inspection)
③	네트워크 계층 패킷 필터링 (network level packet filtering)	상태 검사 (stateful inspection)
④	네트워크 계층 패킷 필터링 (network level packet filtering)	회선 계층 게이트웨이 (circuit level gateway)

정답 체크
(1) 응용은 개별 프록시를 사용하고, 회선은 공통 프록시를 사용한다.

14. IPSec에 대한 설명으로 옳지 않은 것은?
① AH는 인증 기능을 제공한다.
② ESP는 암호화 기능을 제공한다.
③ 전송 모드는 IP 헤더를 포함한 전체 IP 패킷을 보호한다.
④ IKE는 Diffie-Hellman 키 교환 알고리즘을 기반으로 한다.
정답 체크
(3) 터널 모드에 대한 설명이다.

15. 보안 공격에 대한 설명으로 옳지 않은 것은?
① Land 공격은 패킷을 전송할 때 출발지와 목적지 IP를 동일하게 만들어서 공격 대상에게 전송한다.
② UDP Flooding 공격은 다수의 UDP 패킷을 전송하여 공격 대상 시스템을 마비시킨다.
③ ICMP Flooding 공격은 ICMP 프로토콜의 echo 패킷에 대한 응답인 reply 패킷의 폭주를 통해 공격 대상 시스템을 마비시킨다.
④ Teardrop 공격은 공격자가 자신이 전송하는 패킷을 다른 호스트의 IP 주소로 변조하여 수신자의 패킷 조립을 방해한다.
정답 체크
(4) 순서 번호를 겹치게 하는 공격이다.

16. 다음은 「지능정보화 기본법」 제6조(지능정보사회 종합계획의 수립)의 일부이다. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

> 제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획(이하 "종합계획"이라 한다)을 [(가)] 단위로 수립하여야 한다.
> ② 종합계획은 [(나)]이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 "전략위원회"라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

	(가)	(나)
①	3년	과학기술정보통신부장관
②	3년	행정안전부장관
③	5년	과학기술정보통신부장관
④	5년	행정안전부장관

정답 체크
(1) 제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획(이하 “종합계획”이라 한다)을 3년 단위로 수립하여야 한다.
② 종합계획은 과학기술정보통신부장관이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 “전략위원회”라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

17.「개인정보 영향평가에 관한 고시」상 용어의 정의로 옳지 않은 것은?
① “대상시스템”이란「개인정보 보호법 시행령」제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.
② “대상기관”이란「개인정보 보호법 시행령」제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관 및 민간기관을 말한다.
③ “개인정보 영향평가 관련 분야 수행실적”이란「개인정보 보호법 시행령」제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.
④ “개인정보 영향평가”란「개인정보 보호법」제33조제1항에 따라 공공기관의 장이「개인정보 보호법 시행령」제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
정답 체크
(2) "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관을 말한다.

18.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제23조의4(본인확인업무의 정지 및 지정취소)상 본인확인업무에 대해 전부 또는 일부의 정지를 명하거나 본인확인기관 지정을 취소할 수 있는 사유에 해당하지 않는 것은?
①「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우
② 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
③ 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
④ 지정받은 날부터 3개월 이내에 본인확인업무를 개시하지 아니하거나 3개월 이상 계속하여 본인확인업무를 휴지한 경우
정답 체크
(4) 제23조의4(본인확인업무의 정지 및 지정취소) ① 방송통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다.
1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

19. 메일 보안 기술에 대한 설명으로 옳지 않은 것은?
① PGP는 중앙 집중화된 키 인증 방식이고, PEM은 분산화된 키 인증 방식이다.
② PGP를 이용하면 수신자가 이메일을 받고서도 받지 않았다고 발뺌할 수 없다.
③ PGP는 인터넷으로 전송하는 이메일을 암호화 또는 복호화하여 제3자가 알아볼 수 없게 하는 보안 프로그램이다.
④ PEM에는 메시지를 암호화하여 통신 내용을 보호하는 기능, 메시지 위·변조, 검증 및 메시지 작성자를 인증하는 보안 기능이 있다.
정답 체크
(1) PGP는 분산화된 키 인증 방식이고, PEM은 중앙 집중화된 키 인증 방식이다.

20. (가)~(다)에 해당하는 트리형 공개키 기반 구조의 구성 기관을 바르게 연결한 것은? (단, PAA는 Policy Approval Authorities, RA는 Registration Authority, PCA는 Policy Certification Authorities를 의미한다)

(가) PKI에 대한 정책을 결정하고 하위 기관의 정책을 승인하는 기관
(나) Root CA 인증서를 발급하고 CA가 준수해야 할 기본 정책을 수립하는 기관
(다) CA를 대신하여 PKI 인증 요청을 확인하고, CA 간 인터페이스를 제공하는 기관

	(가)	(나)	(다)
①	PAA	RA	PCA
②	PAA	PCA	RA
③	PCA	RA	PAA
④	PCA	PAA	RA

정답 체크
(2) Approval(승인), Certification Authorities(CA), RA(CA를 대리함)